U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7273

Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources:

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Washington, DC 20402-0001
   Internet: www.bookstore.gpo.gov
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22312-0002
   Internet: www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Division of Resource Management & Analysis
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
Internet: www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX),(4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and the Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of the NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7273

Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies

Manuscript Completed: July 2020
Date Published: March 2021

Prepared by:
Muhlheim, M. D. [1]
Poore, W. P. [1]
Nack, A. M. [2]
Wood, R. T. [3]
Melin, A. M. [1]
Bull Ezell, N. D. [1]
Hale, R. E. [1]
Holcomb, D. E. [1]
Huning, A. J. [1]
Halverson, D. S.

[1]Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6285

[2]Consultant

[3]University of Tennessee
Knoxville, TN 37996

D. S. Halverson, NRC Project Manager

Office of Nuclear Regulatory Research

ABSTRACT

An embedded digital device (EDD) is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, that is integrated into hardware equipment to implement one or more system safety functions.

This report provides a technical basis for developing guidance for the safe use of EDDs in commercial nuclear power plants (NPPs) in the United States (U.S.), along with relevant observations, based on their classification, functionality, configurability, consequences of failure, and potential for common-cause failures (CCFs), and it reviews how other agencies worldwide, both nuclear and nonnuclear, regulate, approve the use of, and actually use EDDs.

Areas of interest include the types of components in safety-related applications most likely to have EDDs, methods used by other industries and countries to regulate the use of EDDs, and potential issues noted in industry. This information serves to support the technical basis for a graded approach in the selection and use of EDDs. A tangential supply chain issue is the use of replacement parts or parts in upgrades that may contain an undeclared digital device, as it may not meet the requirements for the safety-related application it is being used in.

Other attributes such as reliability (the ability to perform with correct, consistent results), diagnostics, operating experience, and failure modes were reviewed because of their use in risk informing the acceptance of the use of EDDs. Emerging technologies associated with EDDs were noted during this work, and are described in this report.

International experience is similar to that acquired in the United States, and regulators around the world are evaluating the safe use of EDDs. Other industries are further along in the use of EDDs and therefore can provide useful insights into their use and regulation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Nuclear facilities are increasing their use and reliance on digital technology in systems and equipment. The first digital systems mimicked the analog systems, but as experience with digital systems increased, so did the complexity, functionality, communications, etc., of the systems. The same evolution has occurred in other industries and is likely to occur with the use of embedded digital devices (EDDs) in the nuclear industry. An EDD is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic that is integrated into equipment to implement one or more system safety functions. Equipment with EDDs can include sensors, breakers, priority logic modules, time delay relays, pumps, valve actuators, motor control centers, and uninterruptible power supplies.

In the United States and around the world, engineering and licensing activities in standards and guidance have been and continue to be developed to address the use of EDDs in safety-related systems. This report provides a technical basis for developing guidance for the safe use of EDDs, along with relevant observations.

The Oak Ridge National Laboratory (ORNL) review found that following the guidance for systems and 10 CFR 50, Appendix B, Quality Assurance, should be sufficient for the functionality of EDDs currently in use and that should be expected in the near term in safety-related applications. However, the effort in a simplistic application of all the associated criteria in these guidance documents may be more than is necessary for EDDs, as these documents were developed to support systems that may be more complex and require more application-specific code and customization than is necessary or applicable to a particular EDD.

Therefore, this report includes material to serve as a technical basis for graded approaches that the agency could apply to EDDs. Existing flexibilities within the regulations and guidance applicable to EDDs can be applied using a graded approach to the review of devices: (1) developed under 10 CFR Appendix B quality assurance program or (2) dedicated using the commercial grade dedication (CGD) process. Based on ORNL's review, the technical basis for performing such graded approaches is presented based on the classification, functionality, configurability, consequences of failure, and potential for common-cause failures (CCFs). Another possible way to apply a graded approach would be to allow the use of the four safety integrity levels (SILs) available in International Electrotechnical Commission (IEC) standards. This work identifies and describes how industry and many regulators, both foreign and domestic, use IEC SIL certifications to support the CGD process. Another means for applying a graded approach would be to allow the use of different Software Integrity Levels in Institute of Electrical and Electronics Engineers (IEEE) standards such as IEEE 1012-2004 (or similar in later versions of IEEE 1012).

Diagnostics, operating experience, and failure modes were reviewed because of their use in risk informing the acceptance of the use of EDDs. The performance objectives of the EDDs can be demonstrated by showing that they are sufficiently reliable and robust commensurate with their safety significance. EDDs should be designed for a reliability level that is commensurate with the safety significance of the function(s) to be performed. Supporting issues for achieving a given level of functional reliability and robustness include quality, awareness of what digital content is in the EDD, the use of software tools, cyber security vulnerabilities, redundancy, diversity, failure detection, periodic testing (including the use of self-diagnostic features and surveillance tests), and understanding of failure data/failure modes. Verification and validation (V&V) processes should be included at appropriate design stages to confirm that the necessary safety functions

have been identified and will operate as intended. The metrics and attributes covered in this report provide readers with information to understand the functions of the EDD.

Areas of interest include the supply chain, the types of components in safety-related applications most likely to have EDDs, methods used by other industries and countries to regulate the use of EDDs, and potential issues noted in industry. Being able to leverage the reviews of other countries could also be useful in facilitating more efficient reviews of EDDs. The processes used by Canada and the United Kingdom, which are very different from those of the United States, were reviewed and contrasted in this report.

A supply chain issue related to obsolescence is the use of replacement parts that may not meet the EDD requirements for the safety-related application or an undeclared digital device used in an upgrade to an existing device. This has led to issues in NPP safety-related equipment. This report provides information to be used as a technical basis in supporting potential guidance in this area.

In this work, the term *emerging technologies* refers to devices related to EDDs, practices, design development and assessment methods and tools, and issues associated with evolving technology and new initiatives from the industry that could be included in license amendment applications or that could impact NPP digital systems, but which are not yet widespread in the U.S. nuclear industry.

Emerging technologies were not investigated as an independent effort considering all types of emerging technologies, but this analysis served to capture those that were identified during the evaluation of EDDs and that are related to EDDs. In addition, existing literature reviewing emerging technologies in the U.S. nuclear industry was reviewed for relationships with EDDs. In many cases, these emerging technologies could also generally apply to digital instrumentation and control systems.

As noted in the report, awareness of an EDD's failure modes is important, and failure modes and effects analyses (FMEAs) have been used to identify the effects of those failures. Issues have been identified with the use of FMEAs for high complexity devices or within interacting systems. As EDDs are expected to increase in complexity and connectivity, the use of FMEAs to adequately address establishing the critical characteristics needed for dedication becomes questionable. Modern methods and tools designed to address more complex and connected systems may be needed for such EDDs as described in this report.

International experience is similar to that acquired in the United States, and regulators around the world are evaluating the safe use of EDDs. Other industries are further along in the use of EDDs and therefore can provide useful insights into their use and regulation in the U.S. nuclear power sector..

ACKNOWLEDGMENTS

The authors wish to thank the following staff of the Office of Nuclear Reactor Regulation: Norbert Carte, Samir Darbali, Greg Galletti, and Jack Zhou, for their invaluable insights and dedication throughout the project.

ABBREVIATIONS AND ACRONYMS

A2LA	American Association for Laboratory Accreditation
AC	alternating current
ACLASS	ANSI-ASQ National Accreditation Board
ACRS	Advisory Committee on Reactor Safeguards
ADAS	Additional Diverse Actuation System
A/D	analog-to-digital
AECL	Atomic Energy of Canada Limited
AERB	Atomic Energy Regulatory Board
AIAG	Automotive Industry Action Group
AIChE	American Institute of Chemical Engineers
AMI	advanced metering infrastructure
AMS	Analysis and Measurement Services
ANS	American Nuclear Society
ANSI	American National Standards Institute
API	American Petroleum Institute
API	application programming interface
AOO	anticipated operational occurrences
ARP	Aerospace Recommended Practice
ASIC	application-specific integrated circuit
ASIL	automotive safety integrity level
ASN	Autorité de sûreté nucléaire
ATEX	Canadian Standards Association, Canada
ATWS	anticipated transients without scram
AZZ/NLI	AZZ/Nuclear Logistics Inc.
BDBA	beyond design basis accident
BSEP	Brunswick Steam Electric Plant
BSI	British Standards Institute
BTP	Branch Technical Position
C&I	control and instrumentation
CAE	claims-arguments-evidence
CAMS	Containment Atmosphere Monitoring System
CANDU	Canadian-invented Deuterium-Uranium
CBSIS	computer-based systems important to safety
CCA	characteristic for acceptance
CCF	common cause failure
CCPS	Center for Chemical Process Safety
CDA	critical digital asset
CDC	condensate demineralizer controller
CDF	core damage frequency
CEA	French Alternative Energies and Atomic Energy Commission
CEAC	Control Element Assembly Calculator
CFR	U.S. Code of Federal Regulation
CGD	commercial grade dedication
CGI	commercial grade item
CGIE	commercial grade item evaluations
CIM	Common Information Model
CINIF	C&I Nuclear Industry Forum
CIP	critical infrastructure protection

CLW	co-located worker
CM	configuration management
CNCAN	National Commission for Nuclear Activities Control
CNSC	Canada is the Canadian Nuclear Safety Commission
COMAH	Control of Major Accident Hazards
COTS	commercial-off-the-shelf
CPC	core protection calculator
CPLD	complex programmable logic device
CPU	central processing unit
CRC	cyclic redundancy check
CRDC	control rod drive control system
CSA	Canadian Standards Association
CSB	Chemical Safety Board
D3	defense-in-depth
DAE	Department of Atomic Energy
DAkkS	Deutsche Akkreditierungsstelle
DAS	Diverse Actuation System
DBA	design-basis accident
DC	diagnostic coverage
DC	direct current
DCS	distributed control systems
DEC	design extension criterion
DEG	design engineering guide
DI&C	digital instrumentation and controls
DICWG	Digital Instrumentation and Control Working Group
DNBR	departure from nuclear boiling ration
DNFSB	Defense Nuclear Facilities Safety Board
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DSA	documented safety analysis
DVC	digital valve controller
ECCS	Emergency Core Cooling System
EDD	embedded digital device
EDF	Électricité de France
EDG	emergency diesel generator
EEPROM	electrically erasable programmable read only memory
EFCOG	Energy Facility Contractors Group
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPIX	Equipment Performance and Information Exchange System
EPRI	Electric Power Research Institute
EPROM	erasable programmable read only memory
ESF	engineered safety feature
ESFAS	engineered safety features actuation system
ET	emerging technology
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FERC	Federal Energy Regulatory Commission
FF	frequency of dangerous failure per year

FHA	functional hazard analysis
FMEA	failure mode and effects analysis
FMECA	failure modes, effects and criticality analysis
FMEDA	failure modes, effects and diagnostics analysis
FPGA	field programmable gate arrays
FPL	fixed programming language
FRA	Federal Railroad Administration
FSAR	final safety analysis report
FTA	fault tree analysis
FW	facility worker
GAN	Gosatomnadzor
GFE	government-furnished equipment
GOTS	government-off-the-shelf
GWR	guided wave radar
HART	highway addressable remote transducer
HCI	human-computer interaction
HDL	hardware description language
HHA	health hazard analysis
HLP	hardwired logic platform
HMI	human-machine interface
HPD	hardware description language programmed device
HR	highly recommended
HSE	Health and Safety Executive
IA	instrument air
IAEA	International Atomic Energy Agency
IAF	International Accreditation Forum
IAS	International Accreditation Service, Inc.
IC	integrated control
IC	integrated circuit
ICBM	independent confidence-building measures
IDD	intelligent digital device
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
IN	information notice
INPO	Institute of Nuclear Power Operations
IP	intellectual property
IPF	instrumented protective function
IPL	independent protection layer
IROFS	items relied on for safety
ISG	interim staff guidance
ISO	International Standards Organization
IT	information technology
IV&V	independent validation and verification
KAERI	Korea Advanced Energy Research Institute
KGS	Korea Gas Safety
KINAC	Korea Institute of Nuclear Nonproliferation and Control
KINS	Korea Institute of Nuclear Safety
KPI	key performance indicators
LAN	local area network
LAR	license amendment request

LAWPS	Low-Activity Waste Pretreatment System
LER	Licensee Event Report
LNG	liquefied natural gas
LOI	local operator interface
LOPA	layer of protection analysis
LOR	level of rigor
LRF	large release frequency
LVL	limited variability [programming] language
LWRS	LightWater Reactor Sustainability program
M&S	models and simulations
MCC	motor control center
MDEP	Multi-national Design Evaluation Programme
MEN	Mikro Elektronik
MEMS	Mirco-Electrical Mechanical Systems
MES	manufacturing execution system
MI	mechanical integrity
MIAC	model identification adaptive control
MIMO	multiple-input multiple -output
MOTS	modified-off-the-shelf
MLA	Multi-Lateral Agreement
MMIS	man-machine interface system
MOX	mixed-oxide
MPC	model predictive control
MRAC	model reference adaptive control
MS	mitigation system
MTTF	mean time to failure
N4	current generation of NPPs in France
NASA	National Aeronautics and Space Administration
NDE	nondestructive examination
NDI	non-developmental item
NE	Office of Nuclear Energy
NEA	Nuclear Energy Agency
NEET	Nuclear Energy Enabling Technologies
NEI	Nuclear Engineering International
NERC	North American Electric Reliability Corporation
NISIWG	nuclear industry working group
NIST	National Institute of Standards and Technology
NLI	Nuclear Logistics, Inc.
NNCA	National Nuclear Control Agency
NPJ	Nuclear Plant Journal
NPCIL	Nuclear Power Corporation of India Limited
NPEC	Nuclear Power Engineering Committee
NPP	nuclear power plant
NPRDS	Nuclear Plant Reliability Data System
NRA	nuclear regulation authority
NRC	U.S. Nuclear Regulatory Commission
NSC	Nuclear Safety Commission
NSSC	Nuclear Safety and Security Commission
NUOG	Nuclear Utility Obsolescence Group
NUPIC	Nuclear Procurement Issues Corporation
NVLAP	National Voluntary Laboratory Accreditation Program

O&M	operation and maintenance
OEM	original equipment manufacturer
OECD	Organisation for Economic Co-operation and Development
OLM	online monitoring
ONR	Office for Nuclear Regulation
ORNL	Oak Ridge National Laboratory
OS	operating system
OSHA	Occupational Safety and Health Administration
OT	operational technology
PAEC	Pakistan Atomic Energy Commission
PASS	primary avionics system software
PAL	programmable array logic
PDD	programmable digital device
PE	programmable electronic
PED	programmable electronic DEVICE
PES	programmable electronic system
PFD	probability of failure on demand
PFDavg	probability of failure on demand–average
PFH	probability of failure per hour
PG&E	Pacific Gas and Electric
PHA	preliminary hazard analysis
PHWR	pressurized heavy water reactor
PID	proportional–integral–derivative
PIE	postulated initiating events
PJLA	Perry Johnson Laboratory Accreditation
PLA	programmable logic array
PLC	programmable logic controller
PLM	priority logic module
PNRA	Pakistan Nuclear Regulatory Authority
PRA	probabilistic risk assessment
PROL	power reactor operating license
PROM	programmable read-only memory
PS	prevention system
PSM	process safety management
QA	quality assurance
QC	quality control
QHO	quantitative health objective
QSRM	quantitative software reliability methods
R&D	research and development
RAMS	Reliability, Availability, Maintainability, and Safety
RFT	redundant fault tolerant
RG	regulatory guide
RIL	research information letter
RIS	regulatory issue summary
RISC	risk-informed safety class
RMP	risk management plan
ROM	read-only memory
RPCB	reactor power cutback
RPS	reactor protection system
RRF	risk reduction factor
RTB	reactor trip breaker

RTCA	Radio Technical Commission for Aeronautics
RTD	resistance temperature detector
RTPC	real-time processing computer
RTNSS	regulatory treatment of non-safety system
RTOS	real-time operating system
RTPC	real-time process computing
RTS	reactor trip system
SAMS	Software Application Management System
SAP	safety assessment principle
SAR	safety analysis report
SAT	site acceptance test
SBO	station blackout
SC	safety class
SCADA	supervisory control and data acquisition
SCCF	software common cause failure
SERH	Safety Equipment Reliability Handbook
SFF	safe failure fraction
SFMEA	software FMEA
SHA	system hazard analysis
SI	safety injection
SIL	safety integrity level
SIS	safety instrumented system
SISO	single-input single-output
SoS	system of systems
SLM	safety layer matrix
SPIDR	System and Part Integrated Data Source
SPLD	simple programmable logic device
SQA	software quality assurance
SRdB	Sellafield Reliability Database
SRHA	system requirements hazard analysis
SRRP	Standard Regulatory Review Process
SRS	Savannah River Site
SS	safety significant
SSCs	structures, systems, and components
SSHA	subsystem hazard analysis
SSPS	solid state protection system
SSS	software system safety
STI	scientific and technical information
SwCI	software criticality index
TAG	technical assessment guide
TAM	technical assessment methodology
TCL	tool confidence level
TF SCS	Task Force on Safety Critical Software
TGN	technical guidance note
TMI	Three-Mile Island
TMR	triple modular redundant
TÜV	German Technical Inspectorate
UCI	United Controls International
UFSAR	Updated Final Safety Analysis Report
UPS	uninterrupted power supply

UTK	University of Tennessee, Knoxville
V&V	validation and verification
VDU	video display unit
VFD	variable frequency drive
VICWG	Vendor Inspection Cooperation Working Group
VNIIAES	Russian Research Institute for Nuclear Power Plant Operations

1 INTRODUCTION

The commercial marketplace for commercial instrumentation and control (I&C) components and systems is now dominated by digital technology designed to serve the needs of nonnuclear industries, which demand the advanced capabilities and features the digital technology supports. New nuclear power plants will employ digital technology in safety and nonsafety systems extensively. Therefore, the nuclear power industry stakeholders and U.S. Nuclear Regulatory Commission (NRC) staff must have confidence in the safety-relevant characteristics of this equipment to enable effective and efficient regulation and implementation.

Today, components come from a range of international suppliers, including many companies primarily focused on non-nuclear-industry customers. Additionally, the pool of nuclear power plant (NPP) vendor companies has decreased due to mergers and consolidation and a reduced number of plants being built. Many vendors and original equipment manufacturers (OEMs) in the nuclear industry partner with different sub-suppliers for different projects. For embedded digital devices (EDDs), these market conditions mean that such devices can be introduced through system upgrades, component replacements, and new equipment applications, from many sources.

Regulatory Issue Summary (RIS) 2016-05 [1] heightened the awareness that EDDs might exist in procured equipment used in safety-related systems without the devices having been explicitly identified in procurement documentation, and it recommends that licensees implement efforts to identify these devices. RIS 2016-05 [1] states,

> *. . . an embedded digital device is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware,[1] or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions. . . . EDDs include digital components with executable code or software-developed programmable logic that is permanently or semi-permanently installed within the device (commonly referred to as firmware). Firmware includes, but may not be limited to, devices such as programmable logic devices, field programmable gate arrays, application specific integrated circuits, erasable programmable read only memory, electrically erasable programmable read only memory, and complex programmable logic devices.*

Firmware includes programmable logic devices (PLDs), complex programmable logic devices (CPLDs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), erasable programmable read-only memory (EPROM), and electrically erasable programmable read-only memory (EEPROM). The benefits of EDDs include:

- Improvements in accuracy, performance, and reliability
- Asset management improvement through access to a wider selection of suppliers
- Easy access to device maintenance information

A disadvantage of an EDD is the increased design complexity and varied regulatory issues.

Equipment with EDDs can include sensors, breakers, priority logic modules, time delay relays, pumps, valve actuators, motor control centers, and uninterruptible power supplies.

1 *Firmware* refers to the combination of a hardware device, computer instructions, and data that reside as read-only software on that device (IEEE 100 [150], “Authoritative Dictionary of IEEE Standards Terms”).

RIS 2016-05 cites regulations, NRC guidance, and industry guidance to heighten awareness of the following key issues:

1. the need to ensure adequate quality and reliability of EDDs,

2. the need to address potential facility vulnerabilities to software common-cause failures (CCFs) of equipment with EDDs, and

3. the need to ensure sufficient procurement planning and material control to identify, review, test, and control EDDs.

Not only is equipment consisting of analog and older digital technology being replaced with commercial grade products containing EDDs, but EDDs can also be retrofitted to work in existing components. For example, valve controllers with EDDs can fit any existing rotary or sliding-stem valve; licensees can mount the instruments to pneumatic actuators to help improve performance and reliability. This significantly increases the number and types of components that may have EDDs, and it also increases the number of vendors and suppliers. Terminology differences can cause confusion because different names have the same meaning and the same names can have different meanings (which relates to functionality). Terminology differences can also make it difficult to discern if an EDD has been added to or is present in a device potentially resulting in the increased use of EDDs without the end user being aware of any changes.

1.1 Scope of Study

The objective of this research is to develop a technical basis for evaluating the safe use of EDDs and related emerging technologies. This technical basis should support both existing guidance and the development of new guidance to review (and/or commercial grade dedication of) EDDs and emerging technologies.

Key issues associated with EDDs [2] are detailed below:

- Replacement of an analog device or a solid-state component with a digital device may change the manner needed to ensure adequate quality and reliability, including qualification such as electromagnetic combability (EMC).

- Digital devices may have an increased susceptibility to radiation effects.

- There is new potential for software CCFs that did not exist in the analog components.

- Potential for cyber security vulnerabilities including supply chain as well as the use of wireless technology.

- Sufficient procurement planning, identification in procured equipment, and adequate quality and reliability including qualification (such as EMC) are necessary.

- Testing sufficiency and completeness must be ensured.

These issues can impact any sector of the nuclear community, including conversion and deconversion fuel cycle facilities, power reactors, non-power production or utilization facilities, and enrichment, fuel fabrication, or mixed-oxide (MOX) fuel fabrication fuel cycle facilities.

This report provides a technical basis for evaluating the safe use of EDDs, along with observations, based on the classification, functionality, configurability, consequences of failure, and potential for CCFs and reviews how other sectors regulate, approve the use of, and actually use EDDs. Other attributes such as reliability (the ability to perform with correct, consistent results), diagnostics, operating experience, and failure modes were reviewed because of their use in risk informing the acceptance of the use of EDDs. Although these can impact the reliability of an EDD, maintainability (the ability to be easily serviced, repaired, or corrected), availability (the ability to be accessed and operated when needed), flexibility (the ability to be easily adapted to changing requirements), portability of software (the ability to be easily modified for a new environment), reusability (the ability to be used in multiple applications), testability (the ability to be easily tested), and usability (the ability to be easily learned and used) were not reviewed because they are primarily commercial (operability) concerns.

Areas of interest include the supply chain, the types of components in safety related applications most likely to have EDDs, methods used by other industries and countries to regulate the use of EDDs, and potential issues noted in industry. This information serves to support the technical basis for a graded approach in the regulation of EDDs. A tangential supply-chain-related issue with respect to obsolescence is the use of replacement parts that may not meet the EDDs' requirements for the safety-related application. Equipment obsolescence is a concern for all nuclear plants. It affects plants with old and new systems and components, whether analog or digital. Obsolescence cannot be prevented. Replacement parts that do not meet the original design specifications could result in undeclared digital content that could be introduced through aftermarket parts, special manufacturing, repair/build, equivalency, reverse engineering, or design change. (Replacement parts from existing stock and the surplus market should meet requirements.)

1.2 Research Approach

This review used the knowledge of NPP systems and components to identify systems that could receive a digital upgrade in a safety related application as well as the types of devices and technologies that could be applied to them.

The first step was to review the use of EDDs in NPPs, the makeup of an EDD, and the supply chain for EDDs for use in NPPs. The next step was to identify the components most likely to have an EDD. Oak Ridge National Laboratory (ORNL) investigated the literature and nuclear power industry marketplace to identify specific examples and categories of devices, technologies, and systems that contain EDDs or could be upgraded to contain EDDs or emerging technologies. ORNL then solicited information from industry stakeholders on the most significant categories of devices, their functionality, quality, how they are developed, and how they meet regulation via internet searches and personal contact. This part of the analysis consisted of literature reviews with an emphasis on recent scientific and technical journals, internet searches, vendor contacts, and discussions with technology experts. Input was solicited from nuclear industry representatives such as the Nuclear Energy Institute (NEI), research teams under the U.S. Department of Energy (DOE) Nuclear Energy Enabling Technologies (NEET) program, foreign regulators, IAEA staff, IEC standards committee members, and vendors for components used at NPPs on the most significant categories of devices and technologies.

An initial survey of other other sectors and international regulatory practices was also performed to support future detailed work.

ORNL also determined the potential safety implications—new hazards, vulnerabilities, failure modes, and triggering mechanisms, and other potential safety concerns—based on the use of digital I&C systems and components in safety-related or important to safety applications at NPPs. ORNL then identified existing practices and solutions to address the safety implications from other industries or from international organizations.

The laboratory identified and reviewed NRC's current related regulatory infrastructure for EDDs and proposed categories of devices and technologies for evaluation. Direction was given to continue research with a technology neutral, general, high level approach to EDDs with a primary focus on information that could serve as a technical basis for graded approaches and the actionable results of that grading. This involved describing and evaluating EDD related processes and solutions from other nuclear regulators, other safety critical industries, and any methods and standards that are proposed or in use to address these technologies. Further decisions that could be supported in the future included grading based on IEEE Std. 1012, or the Office of Nuclear Regulation's (ONR's) technical assessment guide TAG-046, "Computer Based Safety Systems."

A secondary issue of interest that was identified was collecting the different terms and definitions used by other regulators and in other industries instead of "EDD." Based on that input ORNL performed evaluations of existing practices and solutions to addressing those issues and identified failure modes and other issues with EDDs. The results of these evaluations were then organized into "supporting issues" and attributes that would support graded approaches. Information on existing solutions and practices by other regulators, industries, and standard development organizations is also presented in their own sections as supporting information, or reference for future initiatives, as were emerging technologies related to EDDs that were identified during this work.

Summaries and observations were then developed.

2 EMBEDDED DIGITAL DEVICES

Interest in EDDs for monitoring and providing control of components is increasing as pure analog-based components continue to disappear from the industrial I&C marketplace and as the added functionality of digital systems is welcomed.

A typical EDD in an industrial system performs a defined function. EDDs are typically configurable but not programmable (i.e. fixed firmware with configurable parameters or changeable settings), and they can sometimes perform a safety role as temperature transmitters, pressure transmitters, voltage regulators, gas analyzers, boiler controllers, relays, and radiation monitors. In other cases, EDDs may be configurable and programmable.

EDDs may provide monitoring capabilities and diagnostics with human-machine interfaces (HMI), or they may provide autonomous control of a component. Technology trends seem to be moving toward EDDs with communication capabilities connected into a system arrangement. Thus, EDDs can provide more functionality independently at the component level, and could increase functionality further when coupled with other EDDs to make operational decisions based on inputs from other EDDs within the same flow loop or instrument channel or in another loop/channel.

Important trends in the development of EDDs are detailed below [6]:

1. Because of the high industrial competition and the advances in hardware and software technology, there is a continuous demand for products with more functionality.

2. The functionality is shifting from hardware to software.

3. The functionality is not limited to development by just one manufacturer but may be host to multiple parties.

4. More and more integration in networked environments that affect these devices in ways that might not have been foreseen.

2.1 What Is an EDD?

RIS 2016-05 [1] states:

> *"… an embedded digital device is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions."*

The term *EDD* is used primarily in the U.S. nuclear industry, while most other industries and countries use related terms such as *smart device*, *intelligent device*, or *device of limited functionality*.

In general, EDDs currently in NPPs operate in a manner similar to existing analog technology. However, unlike analog technology, the digital hardware and the associated software in an EDD can introduce new functionality, failure modes, operability issues, and 100% testing may not be achievable. In the emerging technology (ET) arena, increased communication capabilities and

wireless technology would increase the capabilities of the EDD significantly beyond its analog counterpart.

In the nuclear industry, EDDs currently primarily perform monitoring, diagnostics, or display functions, but an EDD can also perform control functions. However even if the primary additional functionality afforded by the use of an EDD is only diagnostics, the operation of the EDD may still be integral to the safety function of the device. In other cases the EDD may be entirely separate within the device from the portions responsible for the safety function. There have been cases where there are essentially two EDDs present, one for the safety function, and another for other functionality.

EDDs are generally considered to be installed physically within a component. However, this work identified external devices that are in almost all technical ways identical to one internal to a component. That is, the actual digital device can be bolted externally onto an existing SSCs or, for various reasons, portions of the device can be external in a manner that is in almost all technical ways identical to being internal. For example, relays may have the digital device embedded within the device with a container enclosing the component similar to the Allen-Bradley RTC-700 relay [3], whereas valves, pumps, and similar components may have the digital device attached to the outside of the component similar to the FieldVUE DVC6200 controller which is attached externally to a valve [4]. This is an example where diagnostics is actually performed by a “bolt on” device. In fact, the digital portions of devices may be located hundreds of feet from the actual component and installed on a rack similar to the devices at Pickering [5]. A rack of digital devices would easily allow information and data to be collected and transmitted as a package to a local control station or even to the control room.. Regulatorily such devices would require treatment similar to that described for an EDD.

There can be debate as to whether a particular digital device should be considered an EDD. For example some digital devices are considered to be standalone devices, not embedded or integrated as part of another equipment. This draws a distinction between smart transmitters which may be considered standalone devices, while some digital devices or components for circuit breakers, motor control centers, etc. are embedded or integrated as part of the corresponding equipment. Instances of a digital device embedded into a card used as part of a reactor protection system may or may not be considered an EDD. Again, regulatorily, these devices would require treatment similar to that described for an EDD.

In this report such technologies are sometimes described alongside EDDs.

2.1.1 Hardware

The *hardware* part of an EDD is the physical unit that consists of the digital device that may be installed in or on a component.

Firmware is software specifically designed for a piece of hardware, such as

- microprocessors/microcontrollers,
- PLDs, including CPLDs,
- FPGAs,
- ASICs,

- programmable read-only memory chips, including EPROM and EEPROM.

Of the component types of interest that were identified and reviewed, some of the vendors contacted indicated that the technologies currently used by them in EDDs were primarily ASICs for NPPs. Other vendors indicated that they would use ASICs, CPLDs, or whatever the customer wanted. In light of the potential costs for dedicating commercial software-based systems, it is possible that development of ASIC-based or FPGA-based components for nuclear power safety applications will expand in the long term. In fact, these types of components are installed in digital devices around the world. Therefore, maintaining an awareness of the technology is warranted as standard integrated circuit (IC) chips are replaced with FPGA and ASICs. Only limited use of CPLDs such as the Allen-Bradley relay, the solid state protection system (SSPS) circuit boards, and the Hagan 7300A ASIC-based circuit boards from Westinghouse used in plant protection systems was found. Other examples are provided in the subsection on undeclared digital content.

2.1.2 Software

Software includes the operating software, application software, and software tools, and can be embedded in the EDD firmware or logic. Some EDDs do not contain software during operation although software tools were used during their development.

Embedded software is software that interacts with and controls hardware. More specifically,

- The software is permanently or semi-permanently installed within the device (commonly referred to as *firmware*).

- The software is embeded in read only memory (ROM); it does not need secondary memories like the hard disk drive in a computer.

- Sensors observe the input and the software processes the data and transmits a signal to the actuators to control the actions or to an HMI.

EDD software may be manually written by coders or through the use of software tools. COTS software is usually dedicated. However, COTS software tools may or may not be dedicated. One vendor contacted indicated that they write software code and use software tools according to the customer and the application of the component.

2.2 Diverse Terminology Related to EDDs

Inside and outside the nuclear industry, different terms for EDDs may mean the same thing or may mean different things. Outside of the nuclear industry, however, the same words may refer to different functions or even to a system. A list of common terms which can apply to a component or system and which may or may not be referring to the same functionality is provided below:

- Embedded digital devices (EDDs)
- Embedded programmable device
- Embedded systems
- Programmable digital device
- Microprocessor-controlled device
- Configurable device

- Smart device
- Intelligent device
- Intelligent electronic device (IED)
- Intelligent field device
- Digital field device
- Industrial digital device of limited functionality
- Smart manufacturing systems

A single term may refer to different types of devices, or different terms may refer to the same type of device and use. For example, components with EDDs may also be referred to as *smart devices*, *intelligent devices*, *digital field devices*, *industrial digital devices of limited functionality*, etc. However these terms should not be considered synonymous. For example a particularly complex and flexible EDD may not meet the definition of an industrial digital device of limited functionality. In other uses, the term *smart device* may refer to a single component, or it may refer to its use in a system.

The difference in functionality and terminology should be carefully reviewed when considering any regulatory guidance, standard, method, or operating experience because its use could be different than thought. Based on this review, *smart device* and *intelligent device* are the most frequently used terms for components in the nuclear industry, whereas *industrial internet of things* (IIoT)[2] refers to interconnected devices used in the process industries.

Therefore, when determining how digital devices are used and regulated, the term *EDD* may be too limiting or confusing. In this report, if quoted or referenced material from industry or regulators refers to these devices using another term, then that term is maintained. However, this report otherwise uses the term EDD and the definition provided in RIS 2016-05 [1].

Some examples of the most common terms related to EDDs are provided below.

2.2.1 Smart Device

Digital commercial-off-the-shelf (COTS) devices are generally referred to as *smart devices* in process industries and outside the U.S. This is the most frequent term used. Smart devices are assimilated to computer-based safety systems (CBSSs) [7].

For some companies, the term *smart device* refers to devices that communicate with neighboring devices to optimize their own performance based on information about surrounding conditions. An example is a flow transmitter that can autonomously compensate its measured value with data from connected pressure or temperature sensors [8]. For an NPP, this would still be an emerging technology (ET) because of limitations on interconnectivity.

In Canada, a smart device is configurable but not programmable and has limited and pre-developed functionality and low complexity. Example devices are uninterruptible power supplies, transmitters, netting switches, and relays. Example configurations include set points, input/output (I/0) ranges, proportional–integral–derivative controller (PID) parameters, menu settings (event

2 *IIoT* refers to interconnected sensors, instruments, and other devices networked together with computers in industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency, as well as providing other economic benefits. The IIoT is an evolution of a distributed control system (DCS) that allows for a higher degree of automation to refine and optimize the process controls.

logging setting, trend settings, user interface, etc.), and enabling features (write protection, passwords, etc.) [9].

In many instances, a smart device is identical to an EDD, but it simply has another name. However, Sellafield[3] defines a smart instrument as one that measures or directly controls a single process variable, uses a microprocessor, and is a COTS instrument [10]. At Sellafield, the smart instruments could communicate by using highway addressable remote transducer (HART) protocols, although this feature is not currently being used.

Smart devices are not restricted to measurement devices; they also include actuators, valves, motor variable speed drives, and other control equipment. Some users of the term *smart devices* mean devices that provide control capabilities, such as smart thermostats as used in homes or business environments.

Based on guidance in technical guidance note (TGN) 032, the ONR defines a smart device as [11]:

- COTS
- Based on microprocessors/microcontrollers running software/firmware
- User configurable but not user programmable; user cannot add new functionality

Devices that are typically excluded from the definitions of smart devices are programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCSs). Also excluded are unique programmable systems—in essence, anything that contains full variability language.[4] By this definition, non-smart, "dumb" instruments do not feature a microprocessor and firmware. For example, a dumb pressure transmitter would include simple pressure switches and older transmitters based on analog operational ampliers, etc.

2.2.2 Intelligent Device of Limited Functionality

International Society of Automation (ISA)-108.1-2015 [13] defines an *intelligent device* as a "device having digital communication and supplementary functions such as diagnostics in addition to its basic purpose."

Regulators in France use the terms *intelligent device* and *intelligent device of limited functionality*.

The French define a device with limited functionality as a device that contains pre-developed software or programmed logic whose primary function is well defined and applicable to only one type of application within an I&C system [14]. Furthermore, the primary function of the device is conceptually simple, is limited in scope, and is not re-programmable after manufacturing. If the device's primary function can be tuned or configured, then this capability is restricted to parameters related to the process. Examples of a digital device with limited functionality include

3 Sellafield is a large multi-function nuclear site on the coast of Cumbria, England. As of 2019, activities at the site include nuclear fuel reprocessing, nuclear waste storage and nuclear decommissioning, and it is a former nuclear power generating site.

4 The IEEE Digital Engineering Guide (DEG) defines *full variability language* (FVL) as "language designed to be comprehensible to computer programmers and that provides the capability to implement a wide variety of functions and applications." For the EPRI DEG, FVL conveys the idea of programming an I&C system or component using languages like C, C++, assembly, etc., to achieve the application. Examples of FVL systems include general purpose computers, such as a plant process computer. However, it must be understood that FVL is also found in software embedded in an I&C system or component, but the FVL is typically hidden from the user's point of view.

sensors, actuators, electrical protection devices, etc., that are functionally simple. Since 2016, the French standard RCC-E has two possible qualification paths: via use of IEC 61508, or via IEC 62671 with provisions for accelerated qualification for devices already certified per IEC 61508.

The Multi-national Design Evaluation Programme (MDEP) and IEC 62671 use the term *industrial digital device of limited functionality* instead of EDD. MDEP CP-DICWG-07 [15] uses this same term and definition, while the International Atomic Energy Agency (IAEA) [16] uses the same terminology and a similar definition. MDEP does not consider complex devices such as those that use commercial computers (PCs, PLCs) to be an industrial digital devices of limited functionality.

IEC 62671 [17] defines a digital device with limited functionality as a device that complies with the following criteria:

a) *The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g., an [hardware description language programmed device] HPD) and is a candidate for use in an application important to safety.*

b) *The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, or controlling speed of a mechanical device, or performing an alarm function.*

c) *The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).*

d) *The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.*

e) *If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process (such as process range), performance (speed or timing), signal interface adjustment (such as selection of voltage or current range), or gains (such as adjustment of proportional band).*

IEC notes that *limited functionality* is a synonym for *dedicated functionality*, in which the device is dedicated, as it is used for one specific function that cannot be changed in the field. IEC defines *dedicated functionality* as the

> *property of devices that have been designed to accomplish only one clearly defined function or only a very narrow range of functions, such as, for example, capture and signal the value of a process parameter, or invert an alternating current power source to direct current. This function (or narrow range of functions) is inherent in the device, and not the product of programmability by the user.*

Ancillary functions such as self-monitoring, self-calibration, and data communication may also be implemented within the device, but they do not change the fundamental, narrow scope of the device's applicability.

This same document (IEC 62671) provides the following examples of devices that would not be considered to be devices of limited functionality [17]:

- *PLCs,*

- *Devices provided with a programmable language, regardless of its restricted nature (in terms of number of function blocks (or equivalent) or inputs and outputs), where such devices have been designed to allow them to be configured for more than one application (example: single loop digital controller with a function block language).*

Thus, devices of limited functionality have restricted configurability so that they can be configured in only very limited ways, with relatively few options to control the manner in which a device will function in its intended application. The primary function or singular function (or minimal set of related functions) of the candidate device is required for the system and is important to safely to perform its function, as claimed in the safety analysis, and which is relied on to operate autonomously to achieve this function.

A multi-function device may offer the possibility of using several of its main functions as a primary function, but such a device would not meet the definition of having limited functionality and would be less favored for use than a single-function device.

IAEA SSG-39 [16] states that a device of limited functionality has the following characteristics:

- It contains predeveloped software or programmed logic;
- It is autonomous and performs only one conceptually simple principal function, which is defined by the manufacturer and which is not modifiable by the user;
- It is not designed to be reprogrammable;
- If it is reconfigurable, then the configurability is limited to parameters relating to compatibility with the process being monitored or controlled or to interfaces with connected equipment.

EPRI 1002833 seems to relate limited functionality to a device that can be comprehensively tested; this update to NEI 01-01 states that “Example 4-1 describes the case of a digital “smart” transmitter that uses a relative simple digital architecture internally, drives the existing 4-20mA instrument loop, has limited functionality that can be comprehensively tested, and has extensive operating history.” [18].

Regulators in Japan identify the following devices as having limited functionality rather than defining the functionality: actuator, relay, breaker, monitoring device, recorder, and controller [19].

2.2.3 Embedded System

Another frequently used term is *embedded system*, which is used more in industry and in the internet of things (IoT) industry (see below). An embedded system is a combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function or functions *within a larger system* [20]. The global market for embedded systems has been growing because of the increase in devices that include embedded systems. The market has also witnessed vast developments owing to advancements in areas such as material sciences, manufacturing techniques, and research and development (R&D) activities. The result is an increased demand for advanced capability of the devices and product choices.

One of the largest users of embedded systems is the automotive industry that is projected to account for almost 20% of the overall market by 2021 [21].

Other key markets for embedded systems include consumer electronics, defense, and aerospace [21]. In particular, the consumer electronics industry has been gaining market share over the years as consumers increase spending on devices such as smartphones, laptops, and tablets for personal use. Adoption of smart electronics devices as a part of smart home setups also helps make the electronics industry a leading embedded systems market.

One area in which embedded systems are different from operating systems and development environments of other larger-scale computers is in the area of debugging [22]. Programmers working with desktop computer environments have systems that can run both the code being developed and separate debugger applications that monitor the actions of the development code as it is executed; however, embedded system programmers sometimes cannot do both.

Some programming languages run on microcontrollers with enough efficiency that rudimentary interactive debugging is available directly on the chip. In many instances, however, debugging of embedded systems requires attaching a separate debugging system to the target system via a serial or another port. In this scenario, the programmer can see the source code on the screen of a conventional personal computer just as would be the case in the debugging of software on a desktop computer. A separate, frequently used approach is to run software on a PC that emulates the physical chip in software, thus making it possible to debug the performance of the software as if it were running on an actual, physical chip.

2.2.4 Internet of Things

The *internet of things* (IoT) builds on the embedded system base, which is expected to continue growing rapidly, driven in large part by the IoT. Expanding IoT applications such as wearables, drones, smart homes, smart buildings, video surveillance, 3D printers, and smart transportation are expected to increase the growth of embedded systems.

Companies are incorporating smart technology such as IoT into their systems and devices by expanding network-capable sensors and equipment to observe from monitors and communications links how a plant is operating. In the past, machines only sent small packets of data to a supervisory manufacturing execution system (MES) or SCADA platform; today, more information is being sent from sensors, equipment, and the plant floor over the same backend network.

In the manufacturing arena, the use of the term *smart devices* represents the convergence of information technology (IT) with operational technology (OT). *IT/OT convergence* is the integration of IT systems used for processing and storing all forms of electronic data with OT systems traditionally associated with manufacturing and industrial environments used to monitor events, processes and devices, and allow for adjustments in industrial operations. The purpose is to maintain the availability of the production process and to inform the operators of plant status.

IT/OT convergence may also be referred to as the IoT or the Industrial Internet of Things (IIoT).

Whereas IT inherently includes communications as a part of its information scope, OT has not traditionally been networked technology [20]. Many devices for monitoring or adjustment did not contain programmable devices, and those with computational capabilities generally used closed, proprietary protocols and PLCs rather than technologies that afford full computer control.

Like IT networks, OT networks are generally made up of computers, servers, and network switches. However, unlike IT networks, OT networks are comprised of an entirely different set of

hardware components that would typically be found on a manufacturing plant floor. The OT may be referred to as the *industrial control system (ICS*) or *SCADA system*. Some components in the control system include PLCs that control manufacturing equipment or HMIs that allow operators to interface with machinery.

Companies have begun integrating their IT and OT networks by employing IoT sensors on machinery to monitor valves, pumps, gauges and other pieces of equipment. By converging these systems, companies can monitor and harness data in new ways, implementing live dashboards, anomaly detection, process automation, relevant generation of key performance indicators (KPIs), and hundreds of other features now possible with IT/OT convergence [24].

Other benefits of the IT/OT convergence is that the information on plant status can now be remotely accessed. Avanceon's Industry 4.0 [25] provides information at industrial plant levels by allowing workers to remotely access process sensors or final element information like measured value, configuration settings, etc. Among other things, this allows device- and system-performance optimization though delivery of remote services for maintenance and upgrades or repair from a remote location via the cloud.

It was estimated that by 2019, 35% of large global manufacturers with smart manufacturing initiatives had integrated IT and OT systems [21]. This percentage will likely increase as a Gartner survey reports that organizations are increasingly integrating and upgrading their systems, as advancements in technology have demonstrated that integrated systems produce optimized data results [24].

2.2.5 Programmable Digital Device

EDDs are a subset of *programmable digital devices (PDDs).* Institute of Electrical and Electronics Engineers (IEEE) 7-4.3.2-2016 [26] defines *programmable digital device* as "any device that relies on software instructions or programmable logic to accomplish a function. Examples include a computer, a programmable hardware device, or a device with firmware."

2.3 Examples of How EDDs Are Currently Being Used

The trend towards using EDDs is pervasive—from intelligent refrigerators to power plants to the IoT. EDDs are being commoditized into products and components that enhance their performance to make them easier to use. In part, this ease of use results in a move away from supplying data to that of supplying information. An EDD can process raw data into graphs or tables with alarms, indicators, or trends.

EDDs typically monitor parameter inputs, monitor components and their health, and provide an HMI. In some cases, an EDD may provide limited control capabilities. Because of the manner of their current use, EDDs may be too complex for vendors or suppliers to easily analyze and verify.

The use of EDDs in other industries was surveyed in the DOE NEET program, where the market for EDDs is focused now, but its use will migrate to the nuclear industry. Some examples from outside the nuclear industry are provided in the subsections below.

2.3.1 Personal Electronics and Appliances

Embedded digital capabilities in consumer products are making their way into industrial uses in pumps, valves, breakers, etc., with sophisticated new diagnostic, monitoring, and control

capabilities. For example, many consumer products rely on HMI to select or launch applications in appliances or cell phones. The worldwide use of these products and advancements in their capabilities is merging into the components used in the nuclear market. Thus, it is preferable to address the issue now.

Not surprisingly, home appliances are benefitting from the use of EDDs through added functionality and communication capabilities. For example, a smart oven with an EDD can communicate over Wi-Fi or Bluetooth to an application on the user's smart phone [28].

2.3.2 Industrial Sector

Embedded digital capabilities in various industrial sectors are making their way into control systems and autonomous controls.

EDDs may also transform how the component operates. ITT Industrial Process has developed a pump with an EDD that can derive pump flow for centrifugal pumps without using separate flow sensors. The EDD uses the pump flow information to protect the pumps from minimum flow, deadhead, run-out conditions, and cavitation. When multiple parallel pumps are in use, the EDDs can coordinate and balance all the pump outputs [27]; this communication capability makes the EDD more of a system than a component.

2.3.2.1 Aerospace

The aerospace industry was an early adopter of embedded systems. Specifically, guidance computers and avionics packages. These devices can perform complicated measurements and control functions that increase the safety of complex, unstable craft. For example, spacecraft use an embedded computer to take inertial measurements and absolute attitude data from a star tracker and synthesize them into altitude and heading information using Kalman filtering of the variables. These technologies would generally not be considere embedded digital devices. However some features of these early systems can now be found within EDDs, such as Kalman filtering.

2.3.2.2 Medical

Medical devices are also employing embedded digital systems, particularly in wearable devices like intelligent asthma monitors that can identify an oncoming asthma attack before the wearer notices symptoms. Another example is the SMARTdrill surgery tool that recommends where and how to drill based on resistance, bone density, and other factors while also providing surgeons real-time performance feedback.

3 IDENTIFYING DEVICES WITH EDDS

EDDs can be introduced through system upgrades, component replacements, and new equipment applications. With over 6,000 vendors that supply components or services to NPPs and thousands upon thousands of components, a strategy was developed to select types of components in safety systems or systems important to safety that would be likely to have EDDs in the near term.

The use of EDDs in components used in the market is already very prevalent and is expected to expand into the nuclear market. Some current statistics are outlined below that shows its prevelance in industrial commercial and residential use and the limited market in the nuclear industry.

- Industrial, commercial, and residential use:
  - 1.5 million valve positioners with digital field devices are currently installed around the world [30].
  - 8 million Rosemount 3051 pressure transmitters with digital field devices are currently installed around the world [31].
  - 1.5 million Rosemount 644 temperature transmitters, with an optional local operator interface (LOI) are installed around the world [31].
  - 1.8 million pressure transmitters are sold annually in the United Kingdom [32].
- Nuclear industry:
  - 540 pressure transmitters were purchased by the entire UK nuclear industry [32].

Thus, the data shows that a general market search would not indicate how EDDs are in use at NPPs. Several approaches were considered for identifying components with EDDs and their functions that would be relevant to safety-related applicatons at NPPs. One approach would be to focus a survey strictly on EDDs. DOE's Nuclear Energy Enabling Technology (NEET) program used this approach and focused their internet searches on EDDs. They identified the EDDs in use primarily for residential, business, and industry [33]. Their searches showed that the pervasive use of EDDs are outside the nuclear industry, which is supported by the data above. In terms of functionality, the research performed for this effort showed that EDDs primarily provide communications and diagnostics. However, based on the prevalence of EDDs as shown by the NEET study, it is very likely that as the use of EDDs increases, EDDs will migrate to the NPP industry, and other suppliers currently outside the nuclear industry will become NPP suppliers/vendors.

Of interest are the vendors that supply components with EDDs to NPPs. To this end, the approach was to specifically identify NPP vendors that supply selected components of interest. With over 6,000 vendors that supply components to NPPs, it was surmised that vendors that also design, build, and install I&C systems would be the most likely to first couple EDDs to their components. This lead to another choice: develop questionnaires (surveys) or perform focused surveys by directly contacting the down-selected list of vendors.

A review of studies that sent questionnaires to licensees showed unfavorable response rates. Some examples are provided below:

- EPRI developed a questionnaire (survey) about retrofits for utilities [34]. EPRI did not pursue this approach at the recommendations of the utilities themselves.

- EPRI conducted a survey of the application of advanced technologies to systems within NPPs by developing a questionnaire to identify the use of advanced I&C and control room technology [35]. The questionnaire was distributed to representatives of numerous domestic NPPs. There is no publication available that documents survey findings from this activity.

- ORNL did have some success in its survey of emerging technologies [36] when combined with literature reviews, internet searches, vendor contacts, and discussions with technology experts. The key to ORNL's success was the direct contact with vendors.

The responses to surveys and their usefulness (or lack thereof) and ORNLs success of directly contacting vendors led to a different approach. The chosen path forward was to

- identify vendors that provide I&C systems to NPPs

- identify those types of componets likely to have EDDs that are used in safaty applications

- idenfity those vendors that supply one or more of the components likely to have EDDs

- identify those vendors that provide I&C systems *and* one or more of the comonents likely to have EDDs

- contact the vendors to determine the characteristics and functionality of the EDDs

3.1 I&C Vendors for NPPs

Because it was surmised that the vendors who also design, build, and install I&C systems in NPPs would be those most likely to couple EDDs to their components supplied to NPPs, the first step was to identify those I&C vendors.

Our review identified those digital I&C systems and components that are currently used or are planned for use in domestic NPPs. The research approach involved data mining of available publications, reports, and information sources, followed by a more detailed search of operational data. The result of the review identified 42 I&C vendors who had some type of I&C system or platform approved by the NRC or that was undergoing NRC review. The I&C systems included PLCs, microprocessors, and FPGA-based systems.

3.2 Types of components in NPPs in safety applications likely to have EDDs

A typical NPP may contain ~200 pumps and over 5,000 valves [37]. That same plant may contain some 10,000 sensors and detectors,including up to 20 neutron detectors, 60 resistance temperature detectors (RTDs), as many as 100 thermocouples, and 500–2,500 pressure transmitters [38]. AZZ/Nuclear Logistics, Inc. partners with manufacturers and can offer over 10,000 prequalified components [39]. Thus, the number of components, component types, and

vendors is too large to thoroughly review, and a random collection of data would likely produce indefensible results.

In selecting a representative set of components likely to contain EDDs, a review was performed of the list of component vendors, along with information from previous studies on EDDs [47, 48]—all while overlaying the function of an EDD. Component lists were reviewed from the following sources:

- Nuclear Utility Obsolescence Group (NUOG) [40]
- Nuclear Suppliers Association (NSA) [41]
- Nuclear Plant Journal (NPJ), web site [23] and digital copy of journal [43]
- Nuclear Engineering International (NEI) [44]
- American Nuclear Society (ANS) products and services issue of Nuclear News [39]
- Nuclear Procurement Issues Corporation (NUPIC) [45]
- World Nuclear Association [46]
- Nuclear Engineering Enabling Technologies (NEET) workshop on the Qualification of Embedded Digital Devices that included government and industry, utilities, universities, and vendors [47]
- University of Tennessee Knoxville (UTK) identification of EDDs in selected components [33, 48]

Eighteen types of components were identified as likely to be used in NPPs in safety related applications (Table 3-1) (Appendix B). This list is not necessarily a complete list of components that may include EDDs, but a down-selection process was necessary to determine the scope of the problem. During the down-selection process, services (non-components), passive components (e.g., piping), and structural components (including cable trays) were removed from further review.

Table 3-1 Types of Components in NPPs in Safety Related Applications Likely to have EDDs

Chart (data) recorders	Priority logic modules
Circuit breakers	Pumps
Diesel generators	Radiation monitors
Flowmeters	Relays, time-delay relays
Gas analyzers	Temperature transmitters
Level meters	Uninterruptible power supplies (UPSs)
Motor control centers (MCCs)	Valve actuators
Power supplies	Valves
Pressure transmitters	Voltage regulators

3.3 Component Vendors for NPPs

To determine the quality and functionality of the EDDs, those vendors with approved I&C systems in NPPs that also produce a component in the list of most likely components to be installed in an NPP were identified. Thus, this review focused on those vendors that provide components to NPPs. Component vendor lists were reviewed from the same sources used to identify types of components listed above.

From the over 6,000 vendors that provide components, structures, or services to NPPs. Eliminating those vendors that provide at least 1 of the 18 component types of interest reduced the number of unique vendors to 320.

3.4 Vendors of Interest

To reduce the number of vendors to consider further, it was hypothesized that those vendors most likely to embed digital devices into their components would be those that also design, build, and install I&C systems in NPPs. Thus, the list of vendors that supply at least one of the component types of interest to NPPs likely to be used in safety related applications was reduced to those vendors that also design, build, and install I&C systems in NPPs. When the list was reduced to only include vendors that supply at least 1 of the 18 component types to NPPs *and* that also provide I&C systems, 17 vendors remained (Figure 3-1).

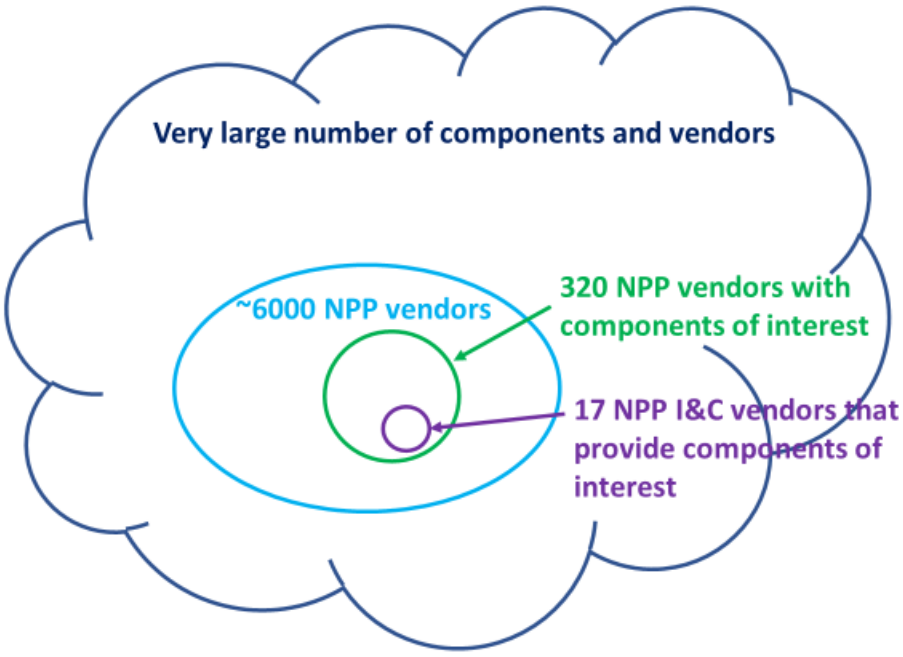


Figure 3-1 Down-Selection Process to Identify Vendors of Interest for Focused Search for EDDs in 18 Component Types.

These 17 I&C vendors were contacted for the focused vendor searches:

- Allen Bradley
- Emerson/Rosemount
- GE/GE-Hitachi
- KEPCO/KNCH
- SAIC
- Yokogawa
- Areva/Meggitt
- Areva/Miron
- Foxboro
- Honeywell
- Mitsubishi
- Siemens
- Eaton/Curtler Hammer
- Framatome
- Invensys/Schneider Electric
- Rolls-Royce
- Westinghouse

ORNL contacted these selected vendors via personal communication using the contacts provided in the products and services lists. Although surveys are typically not productive, this method of personal communication proved beneficial.

The personal contact with vendor engineers and representatives was insightful, and beneficial. In fact, the perception was that the vendors would partake in a workshop to discuss the use of EDDs and the requirements related to the use of firmware.

From discussions with vendors, it was noted that the software developer may be the licensee, the vendor, a company working on behalf of either, or a commercial software development company. For example, Allen Bradley, owned by Rockwell Automation, has PLC-based bus load sequencers, a feedwater controller, and BOP controls. For components, Allen Bradley has safety relays, solid-state pressure sensors, flow switches, solid-state temperature sensors, and temperature controllers, to name a few. For the Allen Bradley 700-RTC relay however, Texas Instruments (TI) was responsible for the design change from an IC chip to the CPLD [49]. Thomasnet.com, which provides over 500,000 detailed supplier profiles, states that TI is a "Manufacturer of analog and embedded processing devices." This shows that outsourcing does occur, although it is not readily apparent.

Other I&C vendors or component vendors not contacted may or may not develop their own EDDs. However, the information obtained from this subset of vendors will most likely remain the same regardless of the sample size. In fact, randomly contacting these other vendors did not provide additional information on the quality and functionality of the component types beyond what was already known.

A complication affecting this selection process is that over time, companies merge or are acquired. For example, Eaton, which was included in our selection process, now includes Cooper Power Systems, Cutler-Hammer, Holec, Kearney, Kyle, McGraw-Edison, Pedersen Power Production and the distribution and control business unit from Westinghouse.

3.5 Quality and Functionality

The desired output of this process involving contacting vendors was to learn about the quality and functionality of the EDDs. Not surprisingly, most of those vendors that provide I&C systems for use in NPPs have a 10 CFR 50, Appendix B program. Somewhat surprisingly (to the ORNL researchers), because not all of the internal components come from Appendix B–approved suppliers, some vendors sent the EDDs to a commercial grade dedicaiton (CGD) facility, even though the vendor's design and manufacturing were performed under an Appendix B program.

Functionality/function for EDDs can be used to categorize devices. The functionality/function(s) of these 18 component types selected for review were determined to allow the classification of the devices at the component level rather than the system level. At the device level, functionality attributes identify significant functional activities and actions performed by the EDDs. This attribute addresses the functionality provided by an EDD that enables implementation of its functions. For the 18 component types, it was determined that the EDDs perform the following functions:

Non-control functionality

- Monitor the components' inputs
  - Monitoring can be used to provide component health information or process variables; or it could be used by licensees to reduce surveillance activities and extend calibration intervals of I&C equipment.

  - The process variables monitored in the EDDs by component type is dependent upon the purchase order received by the vendor. Depending upon the type of device, the process variables include voltage (*v*), frequency (*f*), current (*i*), temperature (*T*), pressure (*P*), *flow*, etc. These variables can be transmitted to a control system such as the RPS.

  - There could be an interface between the EDD controls and the sensors or the sensor could be part of the EDD.

- Diagnostics
  - Self-diagnostics are one means that can be used to assist in detecting partial failures that can degrade the capabilities of the system but may not be immediately detectable otherwise.

  - Diagnostics are typically coupled with a monitor or a display device. The diagnostics can be separate from the control device and could even be developed and certified to different safety integrity levels (SILs).

  - A software-to-system interface provides the data necessary for diagnostic coverage and alarms.

- Display (i.e. provide an HMI)
  - HMIs used in the industrial context are mostly screens or touchscreens that connect users to machines, systems, or devices. HMIs can be simple screen displays mounted on components, advanced touchscreens, multi-touch–enabled control panels, push buttons, computers with keyboards, mobile devices or tablets.

  - In industrial facilities, factory operators use HMIs to control and automate machinery, as well as their production lines. A remote integrated HMI with a control function that has 2-way communication should follow guidance for systems rather than guidance tailored for devices.

  - The basic HMI display of the process variables monitored can display alerts if a variable is outside of expected parameters, and it can display diagnostic results.

- The HMI screen can be integrated with a control function to allow operators to turn on/off components or to allow for adjustment of parameter displays, EDD operating parameters, etc.

- There will be an interface between the EDD and the display monitor (i.e. HMI).

Control functionality

- Control
  - An example of a control function for an EDD would be to take a reference signal in the process, compare it to the setpoint, and then change the output to the control device accordingly to minimize the error (such as a voltage regulator).

  - A device with limited functionality could have a control function. That is, a device of limited functionality is a device whose primary function is well defined and applicable to only one type of application within an I&C system.

Communications functionality

- Communications

  - For this report, digital communications are not considered to be a functionality of an EDD because the communication function would be in support of a control or non-control function. If the primary purpose of a digital device were communications this would be a part of a system as opposed to an EDD. Further, while the IIoT inherently covers communications as a part of its information scope, the current use of EDDs in the nuclear power industry has not used networked technology. Once an EDD is connected and communicating (with possible voting logic), it's functionality would affect system level concerns, such as independence between redundant trains or safety/non-safety interactions, which would need to be reviewed; current regulations and guidance adequately cover this.

  - Communication capabilities may be present to allow the capability to perform diagnostics, maintenance, or software updates. These types of capabilities may not require networking.

The functionality of diagnostics allows the health of a device to be monitored continuously and remotely (through one-way communications). Devices with communication capabilities in use in industry can be configured remotely, and some devices allow firmware updates to be installed remotely. The process industry uses diagnostics to identify degradations, thus allowing corrective action to be taken and avoiding an upset condition.

As an example, the functionality of diagnostics related to a control valve is the capability to detect a variety of issues such as the following potential problems:

- Air leakage
- Valve assembly friction and dead band
- Instrument air quality
- Loose connections
- Supply pressure restriction
- Valve assembly calibration

The diagnostic capability can also facilitate characterization of the valve's performance following maintenance to increase the assurance that the valve will function properly when returned to service.

The control functionality uses onboard processing and sensor information or inputs such as from RPS or ESFAS for local open-loop and closed-loop control of process parameters. Utilizing feedback and sensor information within the EDD could be used to improve the transient response and accuracy of the controlled process parameters without resorting to centralized control.

The onboard processing ability in EDDs can be used to locally perform tasks such as:

- Self-calibration
- Continuous device diagnostics
- Statistical process information analysis
- Detection of sensor failures and switching to backup sensors
- Digital filtering
- Temperature compensation
- Known sensor error compensation
- Local data storage
- Signal analysis

EDDs with expanded communication capabilities (an ET) would enable new modes of interaction between the operator and the device and inter-device communication and coordination. Communication functions would be expected to be separate from those that allow for modification of the configuration of the EDD or for making program changes to the EDD. Once the device has a sufficiently expanded communications function it would behave more like a system rather than a simple component because of the interconnectivity between devices.

An EDD can have one or more of the functionalities—monitoring, diagnostics, display, control, and communications—during its operation. In fact, many devices have several of the functional characteristics listed above. That is, if the EDD were to provide some sort of control, then it would likely have diagnostics and monitoring capabilities. For example, low-voltage circuit breakers may incorporate embedded digital equipment to provide (1) monitoring functions or (2) monitoring and control functions.

A number of important trends can be observed in the development of embedded systems (which would apply to or include certain EDDs) and their functionalities [51]:

1. Users demand that products have more functionality.

2. The functionality provided by embedded systems is shifting from hardware to software.

3. The functionality of embedded systems is not solely developed by just one manufacturer but is common to multiple parties.

4. Embedded systems are more and more integrated into networked environments that affect plant systems in ways that were not foreseen during their construction.

At the component level, the functionalities required from the device, as well as the performance attributes associated with that functionality, include performance characteristics such as response time, memory allocation, reliability, and environmental qualification requirements. Many studies on functionality are focused at the micro level and specifically evaluate the functionality of the system.

At the system level, the functionalities required from the *device* reflect the purpose of the device. Simply stated, the software should operate as it is supposed to, and the macro level evaluation addresses the impact of its failure on the system and the device's fitness for purpose. The macro level analysis identifies the user's/product's needs that are documented as the features of the system. This is typically described by documenting the intended use of the device to be designed.

This difference between component and system level analysis is important. The functionality of new features (compared to analog) is important only for those devices providing a function required for the system level function or that could impact providing the system level function such as through timing or internal communications. That is, for those functions such as monitoring, the component may still be operable, even if the displays fails.

4 SUPPORTING ISSUES

The introduction of EDDs can affect safety by creating new hazards, vulnerabilities, failure modes, triggering mechanisms, and other potential safety concerns at both component and system levels. New vendors into the market may not be familiar with the quality requirements associated with the nuclear power industry, especially for safety related applications.

The NRC issued RIS 2016-05 [1] to clarify their technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with EDDs. RIS 2016-05, which applies to equipment, instrumentation, and controls that contain EDDs in safety-related systems, states that potential safety issues from using EDDs should adequately address the following:

1. The quality and reliability of EDDs that exist in actuation equipment

2. The potential vulnerabilities to CCFs

3. Sufficient procurement planning and material control to identify, review, test, and control EDDs

Other issues include the potential for undeclared digital content in the devices, the difficulty in obtaining information about a device's design and operating history, the use of software tools, accepting certifications (similar to dedication) from other entities, new cyber security concerns, and the possibility that a graded approach may be beneficial for approving the use of EDDs.

In addition to meeting performance requirements, the EDDs should be designed for a reliability level that is commensurate with the safety significance of the function(s) to be performed. Design attributes for achieving a given level of functional reliability and robustness include those related to quality, knowledge of the digital content in the EDD, the use of software tools, cyber security vulnerabilities, redundancy, diversity, failure detection, periodic testing (including the use of self-diagnostic features and surveillance tests), and failure data/failure modes. Verification and validation (V&V) should be included at appropriate stages of the design to confirm that the necessary safety functions have been identified and will operate as intended.

These issues, discussed below, can be used to guide regulatory judgements and recommendations when undertaking technical assessments of the use of EDDs in safety related applications. The supporting issues can be used to appropriately grade the review of the use of EDDs. In addition, the supporting issues can be used to guide assessments of components in proposed new nuclear facility designs.

4.1 Quality Assurance

The NRC has regulatory requirements to provide adequate assurance that the appropriate Quality Assurance(QA) is achieved; however, making this determination has proven to be problematic for components that contain EDDs, particularly if the presence of the EDD is not explicitly identified.

Quality Assurance is considered acceptable if the component or system is designed, manufactured, and maintained as required in 10 CFR 50, Appendix B. Some other countries and industries use International Standards Organization (ISO) 9001 to ensure adequate QA. SECY-03-0117 reviewed ISO 9001-2000 against the existing framework of Appendix B and concluded that ISO 9001 does not meet the requirements of Appendix B [52].

Two different methods of approving a component for use in safety-related applications are described in 10 CFR Part 21. The first method is to design and manufacture the component under a 10 CFR 50, Appendix B–compliant QA program. The second method is to dedicate a commercial grade item (CGI), which, if implemented correctly, is considered to be equivalent to the first method. The key in CGD is being able to identify and verify appropriate critical characteristics. Only if a safety-related component has appropriate critical characteristics that can be verified without requiring in process inspections and verifications can the component be purchased as a CGI and commercially dedicated.

Commercial grade dedication must be performed under an Appendix B QA program. In some cases, the licensees perform the CGD themselves.

The basis for a CGD program is provided in 10 CFR 21 for the reporting of defects and noncompliance. EPRI 3002002982 [53] (an update of EPRI NP-5652) provides guidelines for the CGD program, which can be used to dedicate hardware, software, and services. Software includes the operating (platform) software, application software, and software tools (compilers, assemblers, libraries) and can be embedded in programmable/configurable/fixed firmware, or it can be logic embedded in digital CGIs. The same requirements that apply to dedication of CGIs also apply to the dedication of CGD services, such as calibration [53].

The guidance in EPRI TR-106439 [54], which the NRC concluded contains an acceptable method for dedicating commercial grade digital equipment for use in NPPs, already includes provisions for flexibility in quality based on other factors, thus allowing for describing graded approaches within the existing guidance. Specifically it states:

> *The dedicator must determine which activities are appropriate for each application. In general, the choice and extent of activities undertaken to verify adequate quality, and the specific criteria applied in making the assessment, depend on the safety significance and complexity of the device.*
>
> *Safety significance depends on the function of the device and the consequences of its failure, and includes consideration of backups or other means of accomplishing the safety function. This includes consideration of the cumulative effects of upgrades to systems and equipment that provide diverse backup functions, especially in regard to preserving integrity of the intended diversity. Complexity includes the complexity of the device (e.g., overall architecture, number of functions, inputs and outputs, internal communications among processors or modules, and interfaces with other systems or devices) and complexity of the software.*

Table 4-2 in EPRI TR-106439 identifies the following activities for assessing the built-in quality for commercial digital equipment; this list is not all-inclusive [54]:

- Review of the design, its documentation, and hardware and software implementations

- Review of the design/development process and its documentation, as it was applied for the item being evaluated
- Review of qualifications and experience of personnel involved in design and verification
- Review of vendor QA program and practices, including SQA
- Review of vendor configuration control program and practices
- Failure analysis
- Review of vendor testing
- Review of product operating history

Regardless of whether the licensee used a commercial grade dedicating entity or performed testing and analyses for dedication themselves, under 10 CFR 21.21(c)(1) [55], the licensee is responsible for identifying defects and failures for dedicated items. If a commercial grade dedicating entity is used, they also have this responsibility.

EPRI TR-106439 (endorsed by NRC) identifies NUREG/CR-6421, NUREG/CR-6294, and EPRI TR-104159 (not endorsed by the NRC's endorsement of EPRI TR-106439) as documents that provide lists of attributes (not considered to be all-inclusive) related to the quality of commercial-grade digital equipment.

As noted in IEEE Std. 7-4.3.2-2016 (not currently endorsed by NRC), not every piece of commercial equipment is manufactured with the quality and design integrity necessary to be dedicated [26]. A preliminary determination of the likelihood of success should be performed to determine whether pursuit of commercial grade acceptance and dedication is likely to succeed. This should include an evaluation of how cooperative the equipment vendor will be to detailed design analysis of its equipment, as well as the degree to which compensatory actions are required and if required if they are possible, and how sufficient these compensatory measures can be for missing design, review, testing, and other essential documentation.

The safety significance and simplicity of the system also play a role in assuring quality and dependability [18]. Software development activities must be more rigorous for applications with high safety significance. Simple systems with well-defined failure modes tend to allow for more thorough testing of all I/O combinations than complex systems; complexity increases the uncertainty associated with demonstrating software quality.

Typically, evidence of QA and the manufacturer's use of appropriate development and manufacturing processes is obtained by performing a site visit, audit or inspection, or survey of the manufacturer's site and quality controls. The scope of this activity focuses on the particular device being assessed, although some procedures might be applied to a number of different devices by the same manufacturer.

Paragon, a commercial grade dedicating entity of printed circuit boards, power supplies, breakers, motor control center components, pressure gauges and switches, electrical components, mechanical components, identified the following as challenges in dedicating components [56]:

- Access to Design Information/Requirements

- Lack of Information from Utility
  - Design attributes
  - Safety function
  - Qualification requirements
  - Host component information (if required)
  - IP/Proprietary issues
  - Purchase orders have dated information, old specifications
  - Utilities are doing their own CGD vs. outsourcing

- Lack of information from OEM
  - Unwilling to provide adequate detail
  - Proprietary
  - Obsolescence; no longer supported
  - OEM Information stagnant
  - Many OEMs are now gone; obsolescence

The dedication process requires access to numerous documents, which include development process artefacts such as verification documents and results of analysis and testing performed by the manufacturer. Experience shows that it is important that manufacturers and dedicators access design documentation early in the engagement process with the manufacturer, e.g., setting up non-disclosure agreements [7]. The degree of a design's testability promotes proper operation and provides confidence that no new failure modes will be introduced. Adequacy of testability of EDDs is more likely to be successfully proven through its simplicity of design. EDDs, unlike systems, are typicaly simple devices of limited functionality with few interfaces, so their testing should be comparatively straightforward.

Nevertheless, despite a quality development process and thorough V&V and testing, complexity and other factors such as the inability to detect and eliminate errors may mean that defect-free EDDs cannot be guaranteed with reasonable assurance.

4.2 Undeclared Digital Content

Commercial off-the-shelf (COTS) devices may consist of digital components with embedded software (i.e., firmware, FPGAs), but the user or assessor may be unaware of their presence. Even for I&C devices, it may be difficult for the user or assessor to identify an embedded digital component. As digital content has become increasingly available and more cost effective to incorporate into devices, many COTS devices' analog subcomponents are being replaced with digital devices that offer more options, reduce subcomponent part counts, and provide increased configurations at a reduced cost to the manufacturer. Because the device function remains the same, the product literature and part number for the device may not be revised to reflect this change. If a digital subcomponent is not identified, then its digital/software quality would not be assessed, and the component (i.e., COTS device) may have new failure mechanisms and modes that were not considered [7]. This condition may be referred to as *COTS with undeclared content* [57].

If it is unknown if a replacement component has digital content, replacing an analog component may result in more than a minimal increase in the frequency of occurrence of an accident or the likelihood of a malfunction. The undeclared digital content may also introduce new failure modes that should be evaluated during the dedication process. The new failure modes may increase the consequences of a malfunction or failure or create the possibility for an accident type different than any previously evaluated.

The 18 types of components with EDDs identified earlier may contain digital content and could be the types of items with digital content with the end user being unaware.

One of the key issues identified in RIS 2016-05 related to the use of EDDs is that licensees include adequate procurement controls to include the identification of EDDs in procured equipment [1].

A licensee's 10 CFR 50.59 process should recognize any added digital content, and if necessary, a license amendment request (LAR) should be submitted per 10 CFR 50.90. The unique configuration of each plant, and each application within each plant, makes it imperative that each licensee analyze whether the EDDs can be installed under 10 CFR 50.59. However, if the device contains undeclared digital content it is unlikely that the 10 CFRR 50.59 process would properly evaluate the failure modes of the device or its impact on system reliability and thus plant safety. Those options that could introduce replacement parts that do not meet the original design specifications include aftermarket parts, special manufacturing, repair/build, equivalency, reverse engineering, or design change. (Replacement parts from existing stock and the surplus market should meet existing requirements.)

Undeclared digital content may result from design changes made by the manufacturer that are not communicated to the end user via notification, markings, or other indications that the device has been changed to incorporate digital content. Left undetected, undeclared digital content could find its way into, and become a de facto change to, the plant's licensing basis.

EPRI uses the term *undeclared digital content* [57] to describe digital content that is supplied as part of a CGI without the recipient's knowledge and identifies three means for identifying digital content:

1. Supplier literature (type certification, microprocessor, ASIC, FPGA, or CPLD, software version number, configurable, communication capabilities, connection ports, RCC Class in the French standard RCC-E, or Conformitè Europëenne [CE] marking, ISASecure Embedded Device Security Assurance, or IEC certification)

2. External indications (a picture or visual inspection of the item may indicate digital content or a software version number, or a "hexadecimal" data scheme may be included on the label)

3. Internal indications (a picture or visual inspection of the item showing a printed circuit board, a chip with a sticker indicating a software version number)

Because disassembling the EDD for an internal visual inspection could break seals or damage the internals, this approach should be treated as a destructive evaluation.

Other ways to identify digital content are as follows:

1. Contact the vendor / OEM

2. Include a requirement stipulating that the vendor inform the licensee of digital content, its form, pedigree, etc., in the purchase order. This would also serve as an aid for inspectors

If one is unsure on the possibility of undeclared digital component within a device, RIS 2016-05 [1], Curtiss Wright [58] and EPRI 3002008010 [57] provide guidance on identifying and assessing undeclared digital content.

4.2.1 Examples of Undeclared Digital Content

As noted in Information Notice (IN) 2014-11 [59], NRC inspections identified examples in which previous qualification testing and analysis was improperly applied, as similarity between the previously tested and the currently supplied components was not established. This is of concern for CGIs, as changes made by a commercial OEM could impact the component's qualification and dedication and could go undetected. Inadequate implementation of the CGD process might result in CGIs not being properly qualified to perform their safety functions. Particular attention to this potential concern is necessary when an item will be qualified or dedicated by an entity other than the OEM, and potential changes to the component design might impact that process. Therefore, care must be taken to ensure that replacement components are qualified and dedicated to perform their safety functions prior to installation in a nuclear power plant.

Examples of undeclared digital content are provided below.

4.2.1.1 Allen Bradley 700-RTC Relay

This is an example where the digital content is not externally visible, it was used extensively in the industry, and its failures were reported but not recognized.

In mid-2009, Texas Instruments replaced the solid state integrated circuit logic chip (i.e., old style 16 pin Motorola timing IC chip) with a complex programmable logic device (CPLD) in the Allen Bradley 700-RTC relay. This was a rolling change, with no specific manufacturing date to help distinguish between the old and new configurations [60]. Upon incorporation of the design change, Allen Bradley did not change the part number of the relay, did not issue any product update/technical service bulletin noting the change, and did not update or indicate in the 700-RTC relay technical literature that a digital CPLD device had been incorporated into the product design. Thus, the relay replaced a solid-state device with a programmable CPLD with the relay having the same make, model number, form, fit, and function. The CGD of the modified relays did not identify or address the new design or the failure mechanisms associated with the design change [61]. The change is not visible externally because the timer circuit board containing the CPLD is enclosed within the relay body, requiring disassembly to see it.

After replacing a governor and voltage regulator on an emergency diesel generator (EDG-3) at Brunswick 2 in March 2015 (6 years after the design change), the output breaker failed to remain closed during post-maintenance testing [62]. It was determined that the Allen-Bradley Timing Relay Model 700-RTC in the breaker control logic was susceptible to an inductive kick produced by the downstream relay when it deenergized. During subsequent post-maintenance testing on EDG-4 after replacing the same type relay, its output breaker attempted to close four times before finally closing. The EDG-3 relays passed a post-event site acceptance test (SAT); however, it was determined that a recorder across the relay acted as a suppression device that prevented inductive kick, which was the cause of the relay chattering and then failing. All 9 Allen-Bradley 700-RTC relays were subsequently bench tested, and all chattered.

Duke Energy reported the digital content in the Allen-Bradley 700-RTC relay per 10 CFR 21 [55]. Brunswick Steam Electric Plant (BSEP) did not appear in the affected plant's list because the relays had been obtained as commercial grade and were later dedicated for safety-related use.

Therefore, industry operating experience published via the 10 CFR 21 process was not recognized as applicable to BSEP. Brunswick had a protocol in place to perform sample inspection of incoming electrical CGD candidates for potential unauthorized digital devices [63]. This protocol applied to components likely to contain a digital device, such as transmitters, relays, timers, transducers, indicators and similar products with more complex circuitry. This process should have identified the Allen Bradley relay as having digital content [62].

In its evaluation of the cause of the event, Duke Energy indicated that the procedure for purchasing engineering products did not contain any guidance or requirement for the examination of dedicated high-risk items that may be susceptible to a manufacturer introducing a digital device such as a CPLD in the component's circuitry [62]. Thus, its CGD process did not recognize the modification of the relay.

AZZ/Nuclear Logistics Inc. (AZZ/NLI) was the supplier of the 700-RTC relays to Brunswick 2 and performed its own inspection of the internals of the timing relay in May 2015 [64]. AZZ/NLI determined that the timing relays contain a CPLD that meets the definition of a digital device under the guidance of EPRI and NEI [18]. AZZ/NLI submitted a 10 CFR 21 report indicating that 130 relays were supplied to 11 U.S. licensees since 2009. Shortly thereafter, Nutherm International, Inc. and United Controls International (UCI) submitted 10 CFR 21 reports regarding the Allen Bradley 700-RTC relays in June 2015 and July 2015, respectively. UCI indicated that four relays were sent to one plant [65], and Nutherm indicated that relays were sent to two plants [60]. Nutherm did not indicate the number of relays. A total of 5 dedication facilities dedicated nearly 700 of these 700-RTC relays that were sent to 12 different licensees that were used in safety-related applications [49].

Testing confirmed that the old-style relays—the ones with the 16-pin Motorola chip—did not experience chatter and worked properly every time [49]. Testing also confirmed that those relays with the CPLD chattered based on dc inductive kick that was produced by downstream relays de-energizing. An inductive kick occurred when the coil de-energized, and the magnetic field collapsed, generating a voltage spike of about 3,200–3,500 volts. That voltage spike was then transmitted back upstream to the relay, which basically kept resetting the timer. The breaker would reclose, and the process would start again.

4.2.1.2 Reactor Trip Breakers

This is an example of where digital content was not originally recognized.

Three-Mile Island (TMI)-1 requested a change to replace the reactor trip breakers (RTBs) in connection with the replacement of the existing control rod drive control system (CRDCS) with a digital CRDCS [66]. The licensee's original submittal dated September 29, 2008 states, "[t]he replacement of the RTBs, although included in the overall modification, is not a digital upgrade." However, the licensee's May 6, 2009, submittal informed the NRC staff that, subsequent to the September 29, 2008, submittal, NLI notified the licensee that the RTBs contained microcontrollers. In the May 6, 2009, submittal, the licensee identified the use of microcontrollers in the RTBs as a digital upgrade to a safety system. Although this was originally a device with undeclared digital content, the vendor recognized that the licensee was likely to be unaware of the change and notified them.

4.2.1.3 Smart Chart Recorder

Although the smart chart recorders were recognized to contain digital content, the extent and added functionality was not recognized.

Sellafield's overall experience with smart devices was that it was often very difficult to tell whether an instrument was "dumb" or "smart" [50]. Specifically, Sellafield found that manufacturers' data sheets never specified if microprocessors were used, operation and maintenance manuals never included this level of detail on component parts, and visual examination often proved inconclusive. However, Sellafield's experience shows that even when you recognize that the device has a digital component unnecessary software may be added that inhibits proper operation.

Several paperless chart recorders were installed in a low-SIL application at Sellafield (UK) [50]. Once installed, the recorders started to exhibit faults, mostly "going to sleep" or requiring constant rebooting. Recorders were swapped with identical spares, returned to the manufacturer, and reconfigured over a period of about 18 months, with no real improvement in reliability. It was discovered that the chart recorders contained a game called Cave Fly that was based on the film *Hunt for Red October*, and the game could not be deleted from the firmware; it could only locked-out from the operators. After the game was locked out, reliability seemed to improve, but faults were never completely eliminated. Sellafield decided to change the recorders for another make.

4.3 Software Tools

Early software development methods relied on human inspection and testing for V&V; however, with increased automation (i.e., tool use) there is a comparable reduction in human involvement. That is, there is a tendency to rely on the software tools more. Many of the software tools in use have a large user base that provides feedback, are well supported, and have been in use long enough to be well tested. However, undetected faults in the automated tools or tool-assisted engineering activities may pose serious risks to nuclear safety. In either case, having a good process and consistent method to assess the safety of the software development is important to all stakeholders in the nuclear industry from equipment vendors, utility licensees, and government regulatory organizations. The guidance and use of software tools is addressed further in Appendix C. Very generally, there are two concerns with software tools: (1) they should be evaluated to be appropriate for their manner of use (explained further below), and (2) they should be evaluated to ensure they are appropriate for the secure development and operational environment (SDOE).

IEEE Std. 603-1991 also does not specifically discuss software tools; however, IEEE Std. 7-4.3.2 specifies additional computer-specific requirements (incorporating hardware, software, firmware, and interfaces) to supplement the criteria and requirements of IEEE Std. 603. IEEE Std. 7-4.3.2 is used in conjunction with IEEE Std. 603 to assure the completeness of the safety system design when a computer is to be used as a component of a safety system.

A major change implemented in the 2016 revision of IEEE Std. 7-4.3.2 [26] (currently not endorsed by NRC) provides more specific criteria on the use of software tools used for digital devices and development of hardware, software, firmware, and programmable logic. IEEE Std. 7-4.3.2-2016 defines software tools as "a sequence of instructions and commands used in the design, development, testing, review, analysis, or maintenance of a programmable digital device or its documentation." IEEE Std. 7-4.3.2-2016 requires that software be developed, modified, or accepted in accordance with a software QA plan and that the software QA plan shall address the software tools used for system development and maintenance.

RGs 1.152 and 1.168–1.173 provide some guidance on software used in safety systems, primarily through the endorsement of various IEEE standards. RG 1.152 endorses IEEE Std. 7-4.3.2-2003 (which is addressed below) and includes a specific regulatory position on establishing and maintaining a secure operational environment and a secure development environment for system software. Because this regulatory position does not specifically address software tools, the software tools used to develop the software, as well as the development environment of the software tool, do not need to have been secure to later develop safety-related software if it is determined defects not detected by the software tool will be detected by V&V activities. However while in use on safety-related software the tools would need to be within the secure development environment. IEEE Std. 7-4.3.2 2016 includes a clause that such software tools shall be incorporated into the secure development and operational environment and controlled under configuration management.

EPRI TR-1025243, endorsed by RG 1.231, provides guidance for using a CGD process to accept safety-related, commercial-grade design and analysis tools that are used in the design and analysis of safety-related plant SSCs. EPRI TR-1025243 guidance does not apply to all software tools used to support the design and development of safety-related software.

NRC Branch Technical Position (BTP) 7-18 states that "EPRI TR-106439 and EPRI TR-107330 describe an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides additional information on the characteristics of an acceptable process for qualifying existing software and discusses the use of engineering judgment and compensating factors for purchased PLC software." EPRI TR-106439 describes the generic functional and qualification requirements for a PLC. EPRI TR-107339 (not endorsed by the NRC) contains supplemental guidance for qualifying commercial digital equipment through tailoring the guidance in EPRI TR-106439 consistent with the importance of the digital equipment to safety. The primary focus of EPRI TR-107339 is on the differences in the technical evaluation and acceptance process required for digital, software-based equipment and systems. EPRI TR-107339 provides guidance for each of the phases of the CGI dedication process—beginning with project definition, defining detailed requirements, defining critical characteristics for acceptance, formulating an acceptance strategy, and verification of critical characteristics. Regarding the supplemental guidance of EPRI TR-107339, Information Systems Laboratories, Inc. (ISL) observes [67] that it is "particularly relevant to commercial-grade software but not particularly relevant to software tools." In a review of software development tools, ISL notes that many software tools have a large user base that provides feedback, are well supported, and have been in use long enough to be well tested.

NRC's guidance in NUREG-0800 on the use of software tools [C.2] states that "The software tool should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If, however, it cannot be proven that defects not detected by software tools or introduced by software tool will be detected by V&V activities, the software tools should be designed as Appendix B quality software itself, with all the attendant regulatory requirements for software developed under an Appendix B program."

This is further elaborated on as discussed in EPRI TR-106439 [54] (referenced in RG 1.173 and RG 1.206) which states that

> *Because the output of the software tool as loaded into the PLC can be verified independently, and the tool is not connected to the PLC during operation in the plant (the PLC would be taken out of service during any re-configuration activity), the use of the tool is examined as part of dedicating the PLC but the tool itself does not require dedication.*

The PLC, its hardware and the embedded operating software (firmware) do require dedication for the ESFAS application.

ISL surveyed standards, regulatory guidance, review/approval practices, and other industry practices concerning the use of software tools upon which the reliability of a digital safety-related system depends. Conclusions from ISL are given below:

- EPRI's CGD process is similar to the aerospace industry's safety litmus test [67]. Only safety-related items need to be dedicated. Determining the critical characteristics is similar to the identification and assignment of a tool's confidence level in ISO 26262. The CGD acceptance process for EPRI is a combination of four alternative methods with similarities to methods from other industries.

- The CGD process can be applied to software tools, and many of the steps described in the dedication process specific to hardware or software dedication would be difficult to accomplish and must be adapted for software tools [67].

- The civil aviation industry software classification system is similar to the method used by the commercial nuclear power industry described in IEC 61508 and associated standards, as are the automotive industry practice described in ISO 26262, the high-speed railway industry practice described in BS EN 50128, and the method used in IEEE 1012-2004. However, the civil aviation industry practice is based on a deterministic assessment of software-related errors and their impact on aircraft, crew, and system safety compared to the probabilistic risk-based methods of IEC 61508, ISO 26262, and BS EN 50128. These software classification methods are different from the guidance in RG 1.152 (Institute of Electrical and Electronics Engineers [IEEE] 1012-2004) that assigns the highest SIL to software executed in a commercial NPP [67].

- IEC standards lack consistency, do not include a comprehensive review and approval process, and do not contain a probabilistic risk-based process to design safety-related systems and may not be appropriate for commercial nuclear power safety-related software development since software failures[5] are impossible to quantify [67].

Other industries also struggle with the use of software tools.

Atomic Energy of Canada Limited (AECL) CE-1001-STD [251] specifies requirements and a minimum set of software engineering processes for safety-critical software development for Canadian-invented Deuterium-Uranium (CANDU®) nuclear generating stations. AECL CE-1001-STD does not distinguish between different types of software tools, does not use software tool categories or classifications, and does not contain any specific software tool qualification requirements tailored to the type of tool.

NASA requires that the software tools used in developing software for safety-critical systems should be identified and the level of rigor associated with the verification, validation, and accreditation of software tools should be determined based on the tool functions and the safety classification of the systems in which the software will be used [70]. NASA also encourages the use of simulators or an in-circuit emulator (ICE) system for debugging in embedded systems; these tools allow the programmer or tester to find subtle problems more easily. However, the

5 See Appendix A for the IEC 61513 definition of the "software failure" term, which is used consistently used throughout this report.

guidebook does not discuss simulator or ICE system verification, validation, qualification, review, or approval practices.

Both the Federal Aviation Administration (FAA) and Radio Technical Commission for Aeronautics (RTCA) publish documents that address various aspects of verification, validation, certification, qualification, and use of software and software tools. The FAA requires that all software tools be identified, validated, and addressed within the software development activities and documentation. Software is classified based on how an error affects the software and system containing the software. The software classification defines the rigor necessary to demonstrate compliance with software development requirements. The primary method of tool qualification in accordance with RTCA DO-330 [71] is development, verification, and validation in accordance with a high-quality, well-organized software tool development life cycle process. Alternative tool qualification methods include using service history, exhaustive input testing, formal methods, and dissimilar tools. Unlike most other industries that superficially address COTS software tools, RTCA DO-330 provides a comprehensive qualification process for COTS tools that divides qualification responsibilities between the COTS developer and tool user. Unlike the aerospace industry, which classifies software tools separately from embedded system software, the civil aviation industry classifies software tools to the same level as the software developed with the tool.

ISO 26262 [72] is an international standard that is an automotive specific implementation of IEC 61508. ISO 26262 requires that a tool confidence level (TCL) be determined when (1) a software tool supports or enables the tailoring of activities and tasks of the safety life cycle and (2) the output of the software tool has not been examined or verified. This practice is consistent with the civil aviation industry as described in Radio Technical Commission for Aeronautics (RTCA) DO-178C; however, the ISO 26262 TCL process does not distinguish between software development tools and verification tools, and the TCL is based on a probabilistic assessment that a malfunction and its corresponding erroneous output will be prevented or detected. The TCL is used, along with the automotive safety integrity level (ASIL) to select an appropriate combination of four methods for qualifying software tools. The four qualification methods are: confidence from prior tool use, evaluation of the tool development process, tool validation, and tool development in accordance with a safety standard. Although ISO 26262 identifies four alternative software tool qualification methods, ISL concluded that they are not specific enough to ensure a consistent methodology within the automotive industry [67].

IEC 60880 and IEC 62138 identify types of software tools that require different levels of verification and assessment. IEC 60880 does not require tool qualification if the tool cannot introduce faults into the software: the tool output is always systematically verified, or tool faults are mitigated.

IAEA SSG-39 [16] requires software tools to be verified and assessed in a manner consistent with (1) tool reliability requirements, (2) the type of tool, (3) the potential for the tool to introduce fault or to fail to make the user aware of existing faults, and (4) the extent to which the tool may affect redundant elements of a system or diverse systems. Tools that can introduce faults or fail to detect faults need to be verified to a greater extent than tools less likely to introduce or detect faults; however, verification is not necessary if the tool output is systematically and independently verified.

Appendix C provides a more thorough discussion of software tools.

4.4 Credit for Other Certifications

Many countries do not use the same CGD process as the NRC but still approve components for use in NPPs. This subsection provides some insight into how others approve components for use in safety applications.

In Canada, the justification process is specifically an activity for design suitability or qualification, as opposed to having a seperate commercial grade dedication process.

For the smart device justification in the UK [7]

> *…there is generally limited reliance on certifications, especially at the higher safety classes. While the review of an independent qualified certification body can be used as evidence, its relevance depends on the scope of the certification and the availability of the supporting analyses. Often, the certifications are commissioned by a manufacturer and hence need a level of independent review (including of the supporting documents and analyses). Examples of certifications that can be credited as evidence as part of the justifications in the UK are related to quality assurance (e.g. ISO 9001) and hardware certification (e.g. environmental qualification).*
>
> *Similarly, a proven in use argument is generally a weak justification for a smart device. In fact, the relevance of the operational experience significantly depends on the quality of data collection (e.g. including the version number, the number of demands, the failure mode) and the contractual arrangement for defect notifications. Operational experience is also limited in identifying systematic failures and hence needs to be complemented, for example with additional assessment of the design process and further analyses.*

While the review of an independent qualified certification body can be used as evidence, its relevance depends on the scope of the certification and the availability of the supporting analyses. Often, the certifications are commissioned by a manufacturer and hence need a level of independent review; this review must include the assessment of supporting documents and analyses. Examples of certifications that can be credited as evidence as part of the justifications in the UK are related to QA (e.g. ISO 9001) and hardware certification (e.g. environmental qualification).

An alternative type of certification is that performed by Adelard. This method is accepted by the United Kingdom. The information needed from the device vendor to perform validation needs to be easily accessible by the third-party dedicator. Adelard, through NDAs, has obtained information from vendors but this is a long, difficult task.

Guidance on the proper dedication of CGIs to be used in safety-related applications have received industry-wide acceptance. Guidance is provided in documents such as EPRI 3002002982 [53] (an update of EPRI NP-5652 [73]; EPRI TR-102260 [74] provides supplemental guidance to EPRI NP-5652).

Similarly, industry outside the nuclear industry have certification requirements and methods for certifying products for use in different environments. Companies and testing facilities are approved for certification of these products.

The documents identified in Table 4-1 address the topic of suitability evaluations of COTS equipment. Common terms to be familiar with are CGD, proven in use, and prior use.

Table 4-1 Certification of Components in the U.S. Nuclear Industry and Other Industries

Non-Industry Specific	Process Industry	U.S. (IEEE) Nuclear	International (IEC) Nuclear	U.S. Department of Defense
• IEC 61508 Part 2 [75].	• ISA 84.00.01 Part 1 [76]	• EPRI NP-5652 R1 Guidance for CGD [73] • EPRI TR-106439 Guidance for CGD of Digital Equipment [54] • EPRI TR-107339 Guidance for CGD of Digital Equipment [77] • EPRI 1011710 Handbook for Critical Digital Reviews [78] • IEEE 7-4.3.2-2003 Criteria for Computers in Safety Systems [263]	• IEC 61513 General Requirements [79] • IEC 60987 Computer Based Hardware [80] • IEC 60880 Category A Software aspects [81] • IEC 62138 Category B or C Software aspects [82] • IEC 62671 Selection of Industrial Digital Devices of Limited Functionality [17]	• MIL-STD-882E Standard Practice for System Safety [83] • Joint Software Systems Safety Engineering Handbook [84]

Because of extensive reviews, design information made available, and testing, completion of the Adelard/Emphasis evaluation approved for use by ONR in the UK appears to be comparable to a CGD. This may be an alternative path for dedication and could provide credit for vendors that successfully complete this process.

Although there are differences in what constitutes certification, other industries recognize its need and its use is prevelant. The commercial industry has certification processes for safety systems and equipment. Examples of components certified to IEC 61508, UL 1998, and others include [85]:

- Rosemount Pressure and temperature transmitters
- Siemens AS-I limit switches, position sensors, light curtains, logic
- Green Hills RTOS
- Phoenix Contract relays
- Yokogawa ProSafe PLC, EJX pressure transmitters
- ABB Metcon PT
- Samson 3730 positioner
- Triconix Trident PLC
- Emerson Delta V logic solver, FieldVue valve controller
- Maxcon air operated valves
- ADS Tech single board computer
- Wind River RTOS

- Honeywell SafetyManager PLC
- Allen-Bradley GuardPLC
- Schmersal limit switches
- Ominfles annunciators

Allowing credit for components that have been approved by other countries or dedicators/certifiers outside the U.S. nuclear power industry may be an option to explore given a thorough review of the dedication/certification process through inspections and audits. In addition, leveraging the experience of those commercial products with a successful operating history outside the nuclear industry that may be useful in helping justify these units for use in nuclear facilities although care must be taken when using operating history as a basis for acceptability.

The World Nuclear Association (www.world-nuclear.org), in 2014 planned to have pilot audits with suppliers to develop a common consistent audit checklist and guidance linked to National Quality Standard Association (NQSA) document NSQ-100 [37]. The status of this effort is unknown to the authors.

4.5 Cyber Security

Increased communication capabilities and wireless technology would advance the capabilities of the EDD significantly beyond its analog counterparts. Cybersecurity and issues with electromagnetic propagation (electromagnetic and radio frequency interference, fading, interference abatement) are the major concerns with implementation of digital technologies. Wireless technologies, which are currently not in use in NPPs in safety-related applications, create additional cyber security concerns. Because of their availability, advantages, and extensive usage in process industries, wireless technologies will migrate into the nuclear arena in the near future.

10 CFR 73.54 [86] requires licensees to protect their critical digital assets (CDAs). NRC's RG 5.71 provides guidance for meeting 10 CFR 73.54. NEI 08-09 [87] (Addendum 3 of Revision 6 was endorsed by NRC September 8, 2017) is an alternative to RG 5.71 for meeting 10 CFR 73.54.

To avoid confusion between the coverage of the provisions of 10 CFR 73.54 and RG 1.152 with respect to cyber security, RG 1.152 defines the conditions for controlling a secure development environment and a secure operational environment. Cyber security issues are relevant throughout the entire supply chain, which includes the development and operational environments. EPRI 3002012753 [88] introduces a common supply chain model that was created with segments and transitions for describing cyber security across the supply chain that is risk-informed and that allows for a graded approach based on procurement type. It is recognized that the supply chain represents a significant cyber-attack pathway for digital assets and systems.

NEI 10-04 [89] provides guidance on the identification of digital computer and communication systems and networks subject to the requirements of 10 CFR 73.54. NEI 13-10 [90] provides guidance for addressing technical cyber security controls for CDAs. NEI 13-10 was developed to streamline the process for addressing the application of cyber security controls to the large number of CDAs identified by licensees when conducting the analysis required by 10 CFR 73.54(b). The goal is to minimize the burden on licensees for complying with their NRC-approved cyber security plan while continuing to ensure that the adequate protection criteria of 10 CFR 73.54 are met. Insights from NEI 13-10 may be helpful when assessing the risk of EDDs throughout the plant from nuclear and non-nuclear vendors.

Although it is written for the protection of critical infrastructure protection (CIP) programs [91], IEEE Std. 1686-2013 [92] defines functions and features to be provided in intelligent electronic devices (IEDs). Electronic access to IEDs (e.g., EDDs) can be locally through a control panel, locally through a communication/diagnostic port with a test set or personal computer, or remotely through communications media. This standard can help users identify which features a system should have in order to raise the security level of an IED. Access control, an audit trail, supervisory control and monitoring, and the use of cyber security features such as encryption and QA of the firmware are cyber security control features addressed in the standard.

Pacific Gas and Electric (PG&E) indicated that they have two main expectations when dealing with vendors from a cyber security perspective [93]:

1. Expectations for the vendor: This includes the requirement that the specified product is free of defects, malware, bugs, and unauthorized components and that the product is protected while in transit to PG&E.

2. Expectations of the product: PG&E expects that the product has the necessary features to enable PG&E to comply with the provisions of NEI 08-09. This includes system hardening and access control.

Because the use of EDDs at NPPs will likely increase, and more vendors of EDDs will not be from inside the nuclear industry (see the Subsection on ET in EDDs), cyber security vulnerabilities and concerns will be greater.

4.6 Common-Cause Failures (CCFs)

Understanding the likelihood of CCFs of EDDs is a real concern with respect to the ability to properly assess plant risk and protect public health and safety. These CCFs can be related to software or hardware. Recent events discussed in Subsection 4.6.6 support both of these concerns. It should be noted that this is an area of significant ongoing work and is undergoing changes concurrently with this work. This brief treatment is intended to provide some high level background and a focus on how it may relate to EDDs specifically.

The potential for CCFs exists because of common components, identical hardware, identical software, the same requirements, and the same operating environment. For cases in which such commonalities are identified, justification should be provided to demonstrate that the potential for CCF is low. Hardware and software CCFs may cause identical components to fail at the same time. If CCF vulnerabilities may be of concern as a contributor to risk, a simple estimator for its contribution would be to use the β-factor model.[6] The β-factor model is the most commonly used CCF model and is recommended by IEC 61508-6. The β-factor model is simple and easy to understand and use because it has only the one extra parameter (β). Typical implementation of the beta factor method calculates the CCF failure rate (λ_{CCF}) for a component as the β-factor times the total component failure rate (λ_T). That is, $\lambda_{CCF} = \beta \cdot \lambda_T$.

This procedure for estimating β, as described in IEC 61508-6, is based on a set of questions and a scoring system of the answers to these questions. The IEC 61508-6 checklist includes 37

6 The *β factor method* is an approximation method used for the quantitative evaluation of CCFs. In this method, the likelihood of the CCF is evaluated in relation to the random failure rate for the component. A β factor is estimated such that β% of the failure rate is attributed to the CCF and (1- β)% to the random failure rate of the component. Ideally, this factor is obtained through historical data by determining the percentage of all the component failures in which multiple similar components failed.

questions in eight groups. A slightly different approach to determine the β-factor is suggested in IEC 62601 for high-demand field machinery. The IEC 62061 checklist only has 14 questions and is less complicated than the IEC 61508-6 checklist.

The values used for β in the β-factor model can range from nearly zero to up to 25%, depending upon the device and the particular common cause issues under consideration [196]. For components with little to no data available, their failure probabilities or failure rates should be low and they are not likely to be significant contributors to core damage frequency, and a conservative generic β-factor of 0.1 is likely to be adequate [197]. This provides an estimate of the CCF as $\lambda_{CCF} = 0.1 \cdot \lambda_T$.

Software faiures are another potential cause of a CCF, commonly referred to as a software CCF (SCCF). A software design defect in an EDD can occur in the operating system (OS) (if it has one) or application system software that can cause one or more controllers to simultaneously generate erroneous outputs, or it may cause the outputs to freeze in their current state.

- The OS alone does not perform any application-specific logic that would be designed for influencing or controlled any SSC.

- An OS can be a commercially available, multi-tasking, real-time package available from a third party, or it can be a single task, once-through firmware program designed by the equipment vendor and embedded in their digital product.

- OS and application software often have different characteristics under the control of different entities.

The scope of software CCFs considered in diversity and defense-in-depth analyses include those faults and failures that could impair an automatic safety actuation or could impact the main control room instrumentation required to support operator manual action. For a software CCF to occur simultaneously in multiple EDDs, two conditions must be present:

1. An identical, latent defect must exist in the software (firmware) of multiple EDDs.

2. A triggering condition must occur almost simultaneously in multiple EDDs that exposes the latent defect.

The possibility of simultaneous failure of multiple redundant digital components exists if all of the components are executing the same program with essentially the same I/O and are more-or-less synchronous (i.e., software CCF). For a software CCF to occur in an EDD, a latent defect in the OS or the application software must exist, or the software is not suitable for a particular application.

Because of independent sensors, OS, application software, plant loop, etc., the likelihood of a software CCF occurring simultaneously at numerous EDDs because of these types of failures is likely low. This does not mean that software CCFs cannot occur, it is that the relative rankings from these failure modes are lower because of how the EDDs operate and receive sensor data.

Measures to reduce the likelihood and consequences of a CCF in an EDD include diversity, defense in depth, and no communication with other devices. The use of the EDD also needs to be considered. For example, considering the EDD as a component similar to a pump or valve, CCFs do exist, but plants may not have redundant and diverse components such as valves or

pumps in the same loop. If the EDD is an extension of the component (e.g., valve or pump), then its failure is bounded by the failure of the component to which it is attached.

Applying diversity to EDDs could be addressed through the use of EDDs from different vendors on different flow loops.

Another defensive measure to minimize the likelihood of a CCF (both in hardware and software) is through testing.

Communication independence, which is a defensive measure for a system, is a given for an EDD when it does not share data or resources.

Operating experience can be used to inform the design decisions and any review. This is a very important aspect of operating experience.

Thus, at the device level, with each device having its own sensor and operating on its own time scale, the risk of a CCF is reduced unless caused by external events, misuse of component, faulty requirements, or a software-related CCF similar to the chart recorder at Sellafield (extraneous code). Diversity on the highly redundant subsystem level may introduce maintenance problems, spare parts issues, etc. Thus, diversity at the device level may not be a practical solution.

EDDs in components in different channels/flow loops with possible software triggers may create CCF concerns. However, placing valve controllers for different valves on a rack could cause a CCF because of their physical location. Thus, while one problem may be solved the solution could create other problems.

How the NRC addresses CCFs and software CCFs is addressed below. How other agencies and IEC address CCFs is also discussed with the purpose of providing examples. Commonalities between agencies for reducing the likelihood and consequences of CCFs are the use of defense-in-depth, testing, QA, and fault tolerance. The military, however, does not address CCF per se; rather, it evaluates the consequences (hazards) of a failure. The likelihood of failure is reduced because the software system and environment are operated and tested either on a set frequency or continually.

For an EDD, the most likely contributors to CCF have been environmental effects such as EMI, DC inductive kick, temperature, seismic effects, fire, flooding, and errors in requirements or improper use of the component (i.e., use outside its critical characteristics). Likely failure modes of I&C systems are discussed below in the subsection on failure modes.

4.6.1 NRC

NRC uses the defense-in-depth approach to the design and operation of nuclear facilities in a manner that prevents and mitigates accidents that release radiation or hazardous materials. The key is to create multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is relied upon exclusively. The defense-in-depth approach includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.

Standard Review Plan (SRP) BTP 7-19, Rev. 7, Chapter 7 of NUREG-0800, and Item II.Q of SECY-93-087 note that hardware design errors, software design errors, and software programming errors are all credible sources of CCF for digital safety systems.

BTP 7-19, Revision 7, provides guidance to the NRC staff on evaluating the defense-in-depth and diversity of a DI&C ***system***. However, similar to a system, the EDD's testability could be used to eliminate consideration of CCF. In fact, compared to a system, the EDD is more likely to be simple enough that every possible combination of inputs and every possible sequence of device state can be tested, and all outputs can be verified for every case (i.e., 100% tested).

RIS 2016-05 [1] identifies NRC's regulatory requirements to address potential vulnerabilities to CCFs for safety-related equipment with EDDs. Supplement 1 to RIS 2002-22 [223] offers potential relief through qualitative assessment of the likelihood of failure. The RIS addresses two potential outcomes of the qualitative assessment:

1. Failure likelihood is sufficiently low
2. Failure likelihood is not sufficiently low

4.6.2 IEC

IEC 61513 covers the system aspects of I&C systems important to safety at NPPs, including computer-based systems. IEC 61513 states that combinations of signal and functional diversities are cited as "particularly effective methods to reduce risk of CCF due to errors in the requirements specifications or in the specification and implementation of application software" [79].

In IEC 61513 [79], the design goal for defending against CCF is specified as providing "measures against the occurrence of a CCF within I&C systems implementing different lines of defence against the same PIE [postulated initiating event]." The identified measures include the following:

- design provisions promoting tolerance of hazardous plant events (e.g., external influences and internal hazards),
- design provisions resulting in insensitivity to plant demand design (e.g., decoupling execution from plant status to avoid common triggering conditions),
- design provision to minimize the use of common elements or support systems among lines of defense,
- quality assurance and fault tolerance to minimize the potential impact of systematic faults,
- strategic design decisions to manage complexity, and
- design differences through application of diverse features.

For each design measure, requirements and recommendations are presented to guide the usage of these defensive approaches.

These measures are for I&C systems protecting against postulated IEs. The measures for tolerance can be applied to EDDs, but their application must be focused at the component level and not the system/plant level. For example, external influences such as EMI can be a significant CCF initiator to an EDD.

4.6.3 CSA N290.14-15

CSA N290.14-15 [94] is the standard used by Canadian licensed utilities to qualify commercial-grade software for use in safety-related applications.

For predeveloped software, CSA recognizes IEC SIL and other certifications. Testing can be used to support partial compliance with applicable industry standards. Testing can also be used for proof of acceptability for low complexity software. This appears to be similar to the 100% testing option for addressing CCF identified by NRC in BTP 7-19 revision 7.

4.6.4 DOE

The use of defense-in-depth design principles provides a means for addressing CCF vulnerabilities. Defense-in-depth is used to ensrue that no single function is relied upon. A digital CCF of all layers of defense would require the same digital fault to be present and concurrently actuated in each layer. A defense-in-depth analysis may reveal direct or indirect impacts on interfaces with existing plant SSCs. Defense-in-depth analysis requires assessments of the ability to prevent (reduce susceptibility) and to mitigate (cope with) a CCF.

DOE uses a much more detailed definition (9 aspects) for providing layers of protection and defense-in-depth, as shown below:

a) choose an appropriate site;

b) minimize the quantity of material-at-risk;

c) apply conservative design margins;

d) apply quality assurance;

e) use successive/multiple physical barriers for protection against radioactive releases

f) use multiple means to ensure that safety functions are met by—

    1. controlling processes,

    2. maintaining processes in safe status,

    3. providing preventive and/or mitigative controls for accidents with the potential for radiological releases, and

    4. providing means for monitoring facility conditions to support recovery from upset or accident conditions;

g) use equipment in combination with administrative controls that—

    1. restrict deviation from normal operations,

    2. monitor facility conditions during and after an event, and

    3. provide for response to accidents to achieve a safe condition;

h) provide the means to monitor accident releases as required for emergency response; and

i) establish emergency plans for minimizing the effects of an accident

The DOE NEET Advanced Sensors and Instrumentation (ASI) program is evaluating how to extend a diversity and defense-in-depth (D3) analysis method to treat EDDs. This approach involves [48] the following actions:

- Evaluate equipment to ensure awareness of the presence of an EDD.
- Determine the role and safety relevance of the digital device in the performance of safety-related functions.
- Investigate whether the implementation of relevant functions in the EDD meets either of the two criteria—internal diversity or testability—for which the CCF is considered to be resolved.
- Evaluate the performance characteristics of the equipment to determine the nature of its failure response (e.g., whether failure is detectable and whether adequate time is available to respond).
- Assess whether the component-level CCF has an unacceptable system level or safety function impact (e.g., performance of a best-estimate analysis).
- If necessary, determine the availability of diverse alternatives to mitigate the impact of CCF.

By injecting faults into the software, the DOE NEET program may be able to identify software faults, and possibly software CCFs. Its findings could support this assessment.

4.6.5 Military

The military does not address CCF per se; rather, it evaluates the consequences (hazards) of a failure. The likelihood of failure is reduced because the software system and environment are operated and tested either on a set frequency or continually.

DoD practices for software-based system development are given in the *Software System Safety Handbook* [95]. Testing is relied on to provide evidence of suitability; however, there is very limited ability to test COTS software to provide evidence that the software cannot influence system hazards. Testing in a laboratory cannot duplicate every nuance of the operational environment; nor can it duplicate every possible combination of events. During testing, COTS software is treated as a black box, and the tests measure the response of the software to input stimulus under presumably known system states.

DoD recognizes that hazards identified through black box testing are sometimes happenstance and difficult to duplicate [95]. Without detailed knowledge of the software design, the system safety and test groups can only develop limited testing to verify the safety and fail-safe features of the system. However, the DoD does perform supplemental environmental testing and additional mitigating strategies that could address CCFs.

4.6.6 Examples of CCFs

If the failure rates are comparable for analog and digital devices, then the difference between the dependability of a redundant configuration and its counterpart using conventional technology would be driven by its susceptibility to a CCF. The question then reduces to, “Are smart sensors [EDDs] more prone to CCFs than conventional devices? [121]”

Safety-related equipment with EDDs must satisfy regulatory requirements consistent with the safety significance of the equipment. Quality and reliability considerations must include potential vulnerabilities to CCFs, including software CCFs. However, 38 out of approximately 100 operating plants have reported potential and actual common-mode failures in safety-related disigal systems [96]. Some common-mode failures affected a single plant, while others affected several plants that were using the same digital system.

Operating history shows that hardware and software CCFs can occur. The examples provided are for I&C systems and not necessarily from the operating history of EDDs.

4.6.6.1 Hardware CCFs

The selection of hardware-related CCF events are discussed below. Experiences at Brunswick 2, Shearon Harris, Beaver Valley Unit 2, Waterford 3, and Browns Ferry 3 reinforce regulatory concerns regarding the quality and reliability of safety-related equipment with EDDs and also highlight the use of components in a manner not intended.

The examples were chosen to demonstrate the variety of causes or types of CCFs.

Brunswick 2

The Allen-Bradley 700-RTC breakers having undeclared digital content is discussed in the examples of undeclared digital content. Its susceptibility to CCFs is discussed here.

The introduction of the CPLD made the device susceptible to DC-inductive kick produced by the downstream relay when it de-energized. Although this was not a new failure mode for digital systems, it was a new failure mode for the 700-RTC relay.

This is a potential CCF of all four EDGs, because the Allen-Bradley relays were installed in the breaker control logic of all 4 EDGs. Although one of the primary concerns of EDDs failing is the simultaneous CCF of the embedded software or firmware, the introduction of the CPLD made the device susceptible to DC-inductive kick produced by the downstream relay when it de-energized [97].

As part of this effort, ORNL searched the 10 CFR 21 event reports for the terms “EDD,” “embedded,” “Allen-Bradley,” and “CPLD” to identify reports related to CPLDs replacing solid state or analog parts within a component. No similar events were identified using these terms. However, searches of the 10 CFR 21 event reports related to inductive kick identified this failure mechanism also occurred at Shearon Harris, Beaver Valley 2, and Waterford 3.

Both the undeclared digital content and the dc inductive kick failure mechanism are applicable to EDDs.

Shearon Harris

Both emergency load sequencers at Shearon Harris 1 were subject to a common mode failure because of improper application of the relays not accounting for dc inductive load rating [98]. The deficiency in the sequencer circuit design that existed since plant startup in 1986, failed to properly account for dc inductive loading of contacts.

There are two failure mechanisms relevant to DC inductive loading of contacts to be considered in evaluating sequencer performance. The first involves the Potter-Brumfield relays in which the tabs of the contact melt into the cam, and the second involves the microswitch contact mounted on the Agastat relays.

The contacts of the Potter-Brumfield relays do not have a specified dc rating, and testing was not performed prior to their application in the design of the sequencer by Ebasco. Previous failures of these contacts has occurred during sequencer testing, and during the special testing conducted on May 4, 1990.

The Agastat relay microswitches were installed in an inductive application where the DC current was 0.9 amps, while the contact rating was only 0.5 amps resistive. The sequencer circuit design failed to consider these ratings in the actual application.

Beaver Valley 2

In 1993, during testing of an EDG load sequencer, the load sequencer of Train A failed to automatically load safety-related equipment onto the emergency bus. After the load sequencer for Train A failed, two suspect relays were replaced, and the surveillance test was successfully repeated. Two days later, an EDG load sequencer of Train B failed to automatically load safety-related equipment onto the emergency bus [99].

The cause of both load sequencers failing was a CCF caused by voltage spiking (e.g. inductive kicks) by the auxiliary relays.

A review of these events indicated that the microprocessor-based timer/relay failed as a result of the voltage spikes that were generated by the auxiliary relay coil controlled by the timer/relay. The voltage spikes, also referred to as *inductive kicks*, were generated when the timer/relay time-delay contacts interrupted the current to the auxiliary relay coil. These spikes then arced across the timer/relay contacts. This arcing, in conjunction with the inductance and wiring capacitance, generated fast electrical noise transients called *arc showering* (electromagnetic interference). The peak voltage noise transient changes as a function of the breakdown voltage of the contact gap, which changes as the contacts move apart and/or bounce. These noise transients caused the microprocessor in the timer/relay to fail. The failure of the microprocessor-based timer/relay caused the time-delay contacts to reclose shortly after they had properly opened as part of the load sequencer operation. Closing the time-delay contact locked out (deenergized) the load sequencer master relay and prevented the load sequencer from operating. To correct the identified problem, the licensee installed diodes across the auxiliary relay coils to suppress the voltage spike that had caused the microprocessor-based timer/relay failure. This modification was confirmed to correct the problem through successful testing of the EDG load sequencer.

It was determined that the design control for the selection and review for suitability of the microprocessor timer/relays for this application was not adequate. The modification design data did not identify the potential for voltage spiking by the auxiliary relays and translate that potential

into electromagnetic interference requirements for the equipment purchase specification and the dedication testing specification. As a result of inadequate design control, a CCF mechanism was introduced into the diesel generator load sequencers.

This event highlights the need to ensure proper design control activities when replacing discrete electrical or electromechanical devices with digital microprocessor-based electronic devices. Specifically, the event shows that safety-significant, common-mode failures can occur when the design review does not ensure that the digital, microprocessor-based replacement equipment is compatible for the specific application and service environment.

Waterford 3

At Waterford 3, an inadequate design change rendered the fast bus transfer system inoperable. Modifications to the fast bus transfer circuitry in May 2017 did not properly account for the increased susceptibility to DC coil inductive kick of electronic devices and resulted in the licensee's inability to maintain offsite power to the 6.9 kilo-volt (kV) and 4.16 kV electrical buses following a trip of the main generator [100].

The direct cause of the failure of the fast dead bus transfer was the Struthers Dunn (S-D) 237 Series Direct Current (DC) Time Delay on Dropout (TDDO) relays installed in the fast dead bus transfer circuitry instantaneously timed out when they were exposed to DC coil inductive kick, which prevented automatic transfer of the safety and non-safety electrical busses from the Unit Auxiliary Transformers to the Startup Transformers.

The Root Cause of this event was that the design change procedures in effect during the development of the 1997 and 2017 modifications to the fast dead bus transfer circuitry did not include guidance that electronic devices have a greater susceptibility to DC coil inductive kick than electro-mechanical devices and did not require identification of critical characteristics for non-quality related plant changes.

The Contributing Cause of this event was the post-modification testing performed following the change of the relays from Allen Bradley to Struthers Dunn did not exercise the fast dead bus transfer timing circuitry. This contributed to this condition by delaying detection of relay failure.

Shearon Harris

Shearon Harris 1 replaced the SSPS control circuit boards with CPLD-based boards in 2013 [101]. Note that this represents a conern about a software CCF versus an actual failure event.

In this case, the licensee performed a review but erroneously concluded that the change could be implemented without performing a formal 10 CFR 50.59 evaluation and without obtaining a license amendment. Specifically, in the spring of 2012, Shearon Harris failed to perform a 10 CFR 50.59 evaluation that was sufficient to demonstrate that a license amendment was not required prior to replacing the original SSPS circuit boards with CPLD-based boards. The violation was due in part to the licensee's misinterpretation of the NEI 01-01 guidance [102]. With the replacement of the SSPS boards, the licensee implemented a change that did not adequately evaluate and document that they did not create the possibility of a software CCF in the reactor protection system (RPS) and engineered safety features actuation systems (ESFAS) had not previously been evaluated in the Updated Final Safety Analysis Report (UFSAR) [103]. The licensee failed to recognize that the software used in the replacement boards had the potential to adversely affect the design functions of the SSPS.

Unlike the original circuit boards, which used fixed logic devices, the replacement boards were CPLD-based boards that required an application-specific software (data file) to configure the board's logic functions. These data files that are placed in the board's CPLD memory perform a specified design basis safety function in the SSPS. Because potential software-related failures represent a new failure mode for the SSPS, and these failures could occur on each of the redundant SSPS safety trains, there is a potential increase in the likelihood of a software CCF of the safety function performed by the CPLDs and ultimately, the SSPS.

Browns Ferry 3

In August 2006, a manual reactor trip of Browns Ferry Unit 3 occurred following the loss of 3A and 3B reactor recirculation pumps. The pump variable frequency drive (VFD) controllers became unresponsive, and the condensate demineralizer controller (CDC) failed simultaneously with the VFD controllers. Both the CDC and VFD controllers are connected to the ethernet-based plant integrated computer system network, and due to excessive network traffic, they failed simultaneously, resulting in a manual reactor trip [104].

This event demonstrates that digital CCF can occur due to digital communications.

4.6.6.2 Software CCFs

The potential for software CCF has been recognized for many years. IEC 60800 states that "software design and coding faults" can result in the potential for CCF in software-based implementations of Category A functions. The standard states that software "by itself does not have a CCF mode. Instead, CCF is a system failure issue that arises from "faults in the functional requirements, system design, or in the software." Thus, the standard recommends that the potential effects of software CCF be considered in the application of the defense-in-depth principle, with appropriate countermeasures employed throughout the development and evaluation processes.

EPRI 1016731 [105] includes an evaluation of plant operating experience, noting that because safety systems are intentionally kept as simple as possible, they are subjected to rigorous design and quality assurance requirements, and are not often called upon to perform their safety functions; attempts to gather statistically significant data on number-of-demands and failures-to-actuate-on-demand may be futile in any relevant time frame.

A selection of software-related CCF events are discussed below. Experiences at Palo Verde 3, Turkey Pont 3 and 4, Savannah River, and Sellafield reinforce regulatory concerns regarding the quality and reliability of safety-related equipment with EDDs. EPRI also provides an example of a software CCF. The examples were chosen to demonstrate the variety of causes or types of software CCFs.

Palo Verde 3

On November 14, 1991, Palo Verde 3 tripped on low Departure from Nucleate Boiling Ratio (DNBR) signals [106]. During the post trip investigation, personnel discovered that a problem with the control element assembly calculator (CEAC) software design may have delayed the reactor trip for up to 16 seconds when a second core protection calculator (CPC) time delay was initiated. A second time delay was the result of the CEAC software design not anticipating that there would be CEA slips lasting less than 0.5 seconds.

EPRI, in its review of actual and potential software CCF events, defined this as an active CCF because a bad setting was in all 4 CEAC/CPC's, but triggered in only 1 channel (1 rod slipped faster than expected) [105]. The reactors tripped immediately on deviation/low DNBR, instead of experiencing the 16 sec trip delay. The root cause is an incorrect parameter value with a contributing factor of an inadequate requirements definition.

Turkey Point 3 and 4

In November 1994, it was discovered that although the sequencer is supposed to allow valid safety injection (SI) signals to pass through while in test mode, a logic defect inhibited a valid SI signal during testing at Turkey Point [107]. This event is the only one found by EPRI that could have resulted in an actual CCF of a 1E system under certain conditions. The root cause was determined to be inadequate software design coupled with inadequate software V&V [105].

This digital system was deployed with a selectable automatic self-test feature. It was discovered later, during surveillance testing, that 5 of 18 automatic self-test routines running in each of asynchronous sequencer channels had an error in the application logic that would have prevented an actual SI signal from passing through while in auto test mode. The licensee determined that this condition resulted in all 4 sequencers being inoperable some of the time, triggered by asynchronous yet overlapping automatic tests. These individual channel tests were set up on a set frequency, not on every processor scan cycle. The immediate corrective action was to take the system out of automatic test mode and then correct the self-test logic with a software change.

This software logic defect was introduced during the detailed logic design phase of the software development. The detailed logic designer and the independent verifier failed to recognize the interaction between some process logic inhibits and the test logic. The defect in the software logic was not detected during V&V because the response to valid inputs was not tested during all stripping and loading sequences of the automatic and manual testing logic.

EPRI stated [105],

> *it is important to note that in this case [the event at Turkey Point 3 and 4] at least one important defensive measure had apparently not been applied in developing the application software. A cyclic software design, free of conditional statements (timed, periodic tests), independent of external conditions (test switch position) might have been used to ensure that multiple channels could not be disabled simultaneously.*

EPRI also notes [105]

> *adding automated self-testing features to the relatively simple safety function logic led directly to the problem. It added complexity to the system functionality, with corresponding adverse effects on several aspects of system development that are important from a dependability perspective. For example, requirements become more complicated and more difficult to specify with high confidence that they are complete, correct, unambiguous, etc. It becomes more difficult to anticipate, specify and test all the potential abnormal and faulted conditions that the system might see…, and so on. This event reinforces the notion that safety systems in nuclear plants tend to be functionally simple (compare a signal to a setpoint and change a zero to a one if the setpoint is exceeded), and changes that increase complexity should be considered very carefully.*

Turkey Point 3

A latent design error in PLC coding prevented the two instrument air compressors from loading at Turkey Point 3. The design error was due to overreliance on the vendor to provide a complex digital modification without adequate in-house review [108].

Operations personnel in the control room at Turkey Point 3 acknowledged the instrument air (IA) low pressure annunciator and directed immediate operator action to start all available instrument air compressors. The diesel driven 3CD and 4CD IA compressors are designed to be backup sources for the electric-driven compressors. As backups, the compressors are placed in normal standby operation which bypasses all safety trip and shutdown protections to ensure that the compressors function and supply air when needed. If the diesel driven compressors experience trouble, an alarm will be activated giving operations personnel time to resolve the problem. The standby feature is unique to the diesel compressors.

As configured at the time of the event, it was expected that the 4CD and 3CD IA compressors would automatically start and load when IA system pressure dropped below the identified setpoint. Instead, system pressure continued to drop, and both the 3CD and 4CD compressors were found running unloaded in a non-responsive state. Several attempts to take local control of the compressors and load were not successful. Ultimately, operators had to employ an emergency stop and locally start them in order to load and supply IA to the system. Both diesel-driven IA compressors were restarted and loaded; however, the IA pressure decreased below 65 psig for Unit 3, which required the manual reactor trip.

A cooling fan permissive in the PLC coding but not needed for standby operation rendered the compressors in a non-responsive state, requiring an emergency stop to exit the code and allow manual operation. The vendor-supplied compressor software was not subject to a detailed technical review by in-house personnel of the operating logic of the PLC.

The root causes of the event were as follows:

- A latent design error was in PLC coding which prevented the 3CD and 4CD IA compressors from loading

- The design error was due to overreliance on the vendor to provide a complex digital modification without adequate in-house review.

Contributing causes include difficulty in reading the 3CM LCD control panel screen in direct sunlight and lack of control panel screen instructions or operator aid. During rounds, the turbine plant operator could not see the control panel display on the running electric-driven compressor, 3CM. The operator pressed what was thought to be the administrative button to get the screen to a different mode. The load button was pressed instead, causing the compressor to unload. The control panel is difficult to view in direct sunlight. In addition, instructions for operating the IA compressor control panels were not readily available during the operator rounds.

Savannah River

In July 2010, the Savannah River Site (SRS) experienced a failure in a safety-significant PLC processor module for a tritium air monitor in the Metallography Test Facility. The triple modular redundant (TMR) T8110B PLC processor module—with firmware version build (b)115, designed to provide visual/audible alarms to alert workers of increased tritium activity—was displaying only

a visual alarm in the process room. Investigation revealed that the processor had unexpectedly gone offline, and the system, as designed, went into a safe configuration to energize the visual alarm [109].

The vendor ICS Triplex (a Rockwell Automation Company) had earlier issued a product notice in June 2010 that indicated that TMR T8110 processors with firmware versions b115–b127 were defective. Because the installed system had a processor model TMR T8110B (with firmware version b115), no further action was taken because the product notice did not include model TMR T8110B.

Diagnostic information obtained from the processor was relayed to the vendor to assist with the failure analysis. At that time, the vendor informed SRS that the product notice also applied to the TMR T8110B processor with firmware version b115. The vendor attributed the problem to a defect in the processor module firmware for versions b115–b127. It therefore affected both TMR processor modules T8110 and T8110B with the same firmware version b115. The vendor provided an updated copy of the firmware (version b128) to SRS, which corrected the problem.

Sellafield (UK)

Sellafield (UK) installed vacuum transmitters to monitor ventilation depressions in gloveboxes [50]. Commissioning tests revealed that a vacuum transmitter worked correctly between atmospheric pressure and -6mB. If the transmitter were pressurized it again worked correctly to about +6mB overpressure. However, at about +6mB pressurization, the electrical output would increase, and in effect, the transmitter would work in reverse (i.e., +7mB would read -1mB, +8mB would read -2mB, +9=-3, etc.). This was clearly an unrevealed dangerous condition because the glovebox could be dangerously pressurized but the indicators would show that the pressure was within limits.

Discussions with the manufacturer revealed a poor approach to quality. The fault was “a well-known software bug,” but the manufacturer had not contacted any of the customers to inform them of the fault. The manufacturer was not clear which of the serial numbered transmitters were affected with this problem. These transmitters have been removed, a search was completed for any others at Sellafield, and steps were taken to forbid all future purchases from this manufacturer.

Sellafield (UK)

The Sellafield experience with digital recorders is discussed in the subsection on undeclared digital content [50]. Addressed here is the CCF vulnerability of those recorders.

The event at Sellafield shows that software CCF can actually occur, but not in the usual way, making this a new software failure mode to be considered. The added software caused the chart recorders to “go to sleep.” Although this occurred in a noncontrol-capable device, this shows why guidance calls for no added, unnecessary software.

One of the regulatory positions in RG 1.152 includes a Regulatory Position prohibiting unwanted software. The case of the Sellafield chart recorders, which had gaming software installed, demonstrated that any safety-related device, even one with a high level of simplicity and low functionality, should still have some level of review.

EPRI example

EPRI provides the following example of a redundant system failing because of inadequate configuration controls [110]:

> *A redundant system failed completely due to inadequate configuration controls. A spare part for a system with redundant trains was purchased and put on the shelf after the original system was installed and tested. Firmware on that spare part had a different revision level than the working system, but the module was purchased from the same manufacturer with the assumption that it was an identical part. Later, one train failed, and the other took over, so there was no loss of function. The bad part was replaced with the spare, at which time the entire system crashed and could not be restored until the spare part was removed. The firmware on the spare board was incompatible with the original board's firmware, which caused both trains to abort. When both trains had the same revision level of the firmware, then everything worked.*

4.7 Operating Experience

It is generally accepted that operating experience can be used to help prove the suitability and reliability of components and can therefore be used in support of meeting the regulatory requirements for the use of the device. However, rather than the reliability data provided, the greatest benefit from operating experience seems to be from the lessons learned as shown by the examples of CCFs such as susceptibility to dc inductive kick.

While operating experience alone does not provide sufficient evidence for the safety justification of a safety-related digital I&C system, it may provide, with proper documentation and under certain conditions, supporting evidence when performing licensing reviews and/or I&C system inspections. However, the large volume of operational experience from industrial applications may not be applicable because of a lack of documentation, uncertainty in the version of the device used, process conditions, operating environment, service history, proper failure reporting and recording of data, and any modifications made to the device.

Guerra et al. [111] state, "under-reporting by the smart device users could lead to over-optimistic estimates of the MTTF [mean time to failure]." In fact, in Research Information Letter (RIL)-1002 [112], NRC recognizes that data from operating experience cannot be aggregated and is statistically insignificant, spotty, and scattered. The staff has indicated that operating experience and failure mode data provided by industry to support claims of digital equipment reliability in submittals such as "Benefits Associated with Expanding Automatic Diverse Actuation System Functions" [113] has been insufficient [114].

Traditionally, I&C operating experience is recorded and evaluated only if disturbances and failures occur. One of the problems with operating experience is that manufacturers do not disclose details on the design and operating experience of their products, so operating experience at the component and system level is difficult to obtain, and manufacturers and users do not readily share data. Although specific operational experience data for digital devices has proven difficult to come by, especially for software failures, what data is available has been reviewed to identify the failure modes (see Subsection 4.8).

It is recognized that operating experience by itself is insufficient for estimating the reliability of the device. High reliability of software can only be demonstrated by means of an independent

assessment with full access to the design documentation [115]. A user of a smart sensor/actuator, however, would not usually have access to the design documentation. The supplier would not normally allow other parties to review its design documentation, and as a result, it is not usually produced for that purpose. The Adelard process, discussed in this report, has access to design information, operating history, and essentially dedicates the component.

Factors that may compensate for lack of operating experience—a digital device's simplicity and high testability—may provide assurance of dependability that helps to compensate for a lack of operating history.

EPRI TR-106439 states, "Successful operating experience in applications that are relevant to nuclear power plant safety systems may be used as part of the means for determining the acceptability of a commercial item. … applicable operating experience can be a determining factor for COTS [commercial off-the-shelf] product qualification but is only a part of the dedication process and should not be considered the only determining factor."[7] EPRI has analyzed the operating experiences of Korea, France, China, and other countries where digital I&C has been deployed to some extent. The analysis showed that, according to the operating experience, software CCFs is no more problematic than non-software CCFs [116].

Section 5.1 of EPRI TR-107339 refreshes the studies of software-based systems, showing that a large fraction of problems with software is attributable to problems in the requirements specifications. It recommends a controlled procedure or methodology for development of system requirements similar to that described in EPRI TR-108831 [110]. Based on the system requirements, a set of critical requirements can then be generated for the CGD process or evaluation of the software tools used.

Similarly, proven-in-use arguments are based on objective evidence that is generally insufficient to justify use as a Category 1 (safety related) component [94]. In Canada, a "mature product" that builds on proven-in-use data, cannot be used at Category 1 [176]. Also in Canada, proof through testing, "which can only be used at Category 3, and only for low-complexity items, requires a certain level of in-use tests in a configuration representative of the application" [176]. Preponderance of evidence allows a previous qualification to be considered provided the scope and applicability are justified.

The relevance of the operational experience significantly depends on the quality of data collection (including the version number, the number of demands, and the failure mode, for example) and the contractual arrangement for defect notifications. Operating experience is also limited in identifying systematic failures and hence must be complemented with efforts such as additional assessment of the design process and further analyses.

A key issue regarding operating experience is that extensively used products can still have crucial faults that could cause problems in safety systems. The tendency is to consider operational experience to be like extensive random testing. In this regard, operational experience suffers from the same shortcoming as testing in that testing cannot prove the absence of faults, except for very simple devices [117].

Operating experience can be a useful tool for identifying lessons learned. The examples of hardware-related CCF events at Brunswick, Shearon Harris, Browns Ferry, and Beaver Valley

7 The safety evaluation (SE) on EPRI TR-I06439 (NRC ADAMS Accession No. ML092190664) states, "TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10 CFR Part 21."

reinforce regulatory concerns regarding the quality and reliability of safety-related equipment with EDDs and also highlight the use of components in a manner not intended.

Industry seems to overly rely on operating experience without focusing that experience on critical characteristics for their specific use. The review of vendor material for EDDs highlights the overall use of the EDDs and licensees may not question the process conditions, operating environment, service history, proper failure reporting and recording of data, and any modifications made to the device.

4.8 Failure Modes

Understanding of dominant failure mechanisms helps in estimating failure probabilities and beta factors and on understanding the failure modes that can result in the specific failure being studied. The failure mode is linked directly to the failure mechanism. IEEE Std 100 defines failure mechanism as "the physical, chemical, or other process that results in failure." It notes that "The circumstance that induces or activates the process is termed the root cause of the failure." The failure mechanism defines the physlcs of the failure. Thls involves the description and sequence of those mechanical, electrlcal, or chemical processes or a comblnatlon of these, whlch occurred during the period in which the failed item changed from an operational item to a failed item. Thus, the *failure mode* is the physical or functional manifestation of a failure. For example, the failure mode for a system may be characterized by slow operation, incorrect outputs, or complete termination of execution [127]. EPRI 1019182 [128] states that "A failure mode of a system, component or function is defined by its external behavior, with the system, component or function effectively viewed as a black-box."

Understanding the failure modes of EDDs is vital when relying on self-diagnostics to identify and correct for failures. The presence of new and potentially unknown failure modes in digital systems and components translates into a slower rate of incorporating digital systems into NPPs compared to the process industries [129].

The term failure mechanism should not be confused with the term failure mode. Failure modes result from the activation of failure mechanisms. That is, as defined in IEEE Std 100, the failure mode is the effect by which a failure is observed to occur. The failure mode is generally categorized as electrical, mechanical, thermal, and contamination. IEEE Std. 100 defines the software failure mode as "The physical or functional manifestation of a failure. For example, a system in failure mode may be characterized by slow operation, incorrect outputs, or complete termination of execution." For electronics, failure modes are usually identified as shorts, opens, or electrical deviations beyond specifications. For mechanical components, the failure mode may be low-cycle fatigue.

RIL-1002 provides a synthesized generic set of system-level DI&C failure modes that may be useful when developing a system's design basis and analyzing the degradation of its performance. This is relevant because EDD failure modes could degrade the safety function of a DI&C safety system. However, RIL-1002 notes that

> *"The synthesized set of system level DI&C failure modes, however, may not be helpful for determining the level of safety of a DI&C safety system. Additional critical generic and system—specific failure modes may exist. Some or all of the failure modes identified may not manifest in a particular system. In addition, the staff also learned that a digital system may experience unintended or undesired behaviors without the occurrence of a failure. As such, the synthesized set may not*

be comprehensive for purposes of making determinations of reasonable assurance."

IEC 61508 only acknowledges two types of failure—safe and dangerous. Summers states that "analysts believe that any degraded, not safe, or not dangerous failure can be assumed to be a safe failure. Ironically, while these non-failures are generally included in the SSF [safe failure fraction] calculation, the analysis reports actually recommend not including them in any spurious trip rate calculation [123]."

Most recognize that the special nature of the design of smart sensors compared to analog sensors have a greater potential for unintended behaviors and subtle or new failure modes. However, an NRC review of the new design boards for the SSPS, which uses PLDs, states that the programmable devices do not produce a different failure mode than previously analyzed [125]. Thus, the I&C portion of the EDD may be shown through extensive testing to behave and fail just like other I&C systems and components.

There are significant differences between the dependability aspects of deploying smart sensors vs. conventional ones. Some failure modes do not exist in conventional sensors, such as those involving information overload and timing aspects. Other failure modes emerge through the use of different technologies, such as those involving complexity, data integrity and human interface. Not surprisingly, failures originating in human interface, complexity, and information overload are dominant [121]. Operating experience (see Subsection 4.7) is well suited for identifying failure modes and failure mechanisms.

In a PRA, very simplistic high level failure modes are represented explicitly on an application-specific basis, as detailed below:

- Probabilities of failures on demand
- Frequencies of failures in continuous conditions (e.g., spurious actuation and mission time failures, if applicable)

Many NPPs maintain maintenance records and use this information to update their PRAs. However, licensees do not provide the specific failure data in their PRAs; instead they use the generic failure mode of "fails" (i.e., "the component fails to function").

Although there may be a large amount of failure data for the products delivered, this information is typically proprietary and is seldom made publicly available. This makes identifying and collecting a set of failure modes for EDDs difficult.

For an EDD, the failure modes could be defined by function—monitoring, diagnostics, communication, and control. For those EDDs that provide control, the failure modes should explore complexity by identifying the type of device and providing details on whether it has configurable/programmable internals such as CPLD, etc. The many combinations of types and functions of EDDs can be used to create a list of failure modes specific to that EDD.

At present, FMEAs and PRAs that include software/digital failures assess the same typical failure modes as analog systems, such as fails on/off, high/low, causes/prevents actuation, etc., for its digital failures. These failure modes are applicable to both analog and digital systems, but they fail to account for any potential new failure modes introduced by the digital systems.

Knowing the failure modes can serve two purposes—evaluating the effects of those failures and providing input for diagnostics. To identify any new failure modes for digital I&C-based systems, ORNL reviewed the following databases or data handbooks [134]:

1. OREDA Offshore Reliability Data Handbook;
2. Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2006 Edition;
3. Guidelines for Process Equipment Reliability Data, with Data Table, AICHE;
4. Safety Equipment Reliability Handbook, Exida.com;
5. Reliability, Maintainability, and Risk: Practical Methods for Engineers, 6th edition (D. J. Smith);
6. SPIDR—System and Part Integrated Data Source; and
7. Nuclear Plant Reliability Data Systems (NPRDS) and Equipment Performance and Information Exchange (EPIX), INPO.

All of these sources are available for purchase except the INPO databases (NPRDS and EPIX).

Exida's Safety Equipment Reliability Handbook (SERH) provides a collection of failure rate data that contains equipment item reliability data from over 200 OEMs.

Technological failure modes in embedded systems can be divided into two main groups:

1. Physical failures of the hardware

2. Failures associated with errors in design such as improper requirements, integration, or software faults.

ORNL/TM-2010/32 [132] identified new failure modes for digital systems compared to analog systems such as relay race, complexity of the software program allowing an undetected latent error to escape testing, communications presenting unique problems for digital systems because of the ease of changing digital programs, and a quasi-trip state in which the output of the failed NAND gate would not allow a true HI. These examples represent failures of the hardware, the software, and its integration. In these reports design errors that may result from requirements or integration are often allocated conceptually to the "software fault" category.

The events at Brunswick with the Allen-Bradley relay and the CPLD boards at Shearon Harris also show changing some aspect of the digital devices may introduce new failure modes for that device.

All failure modes of I&C systems identified in ORNL/TM-2010/32 can be characterized as (a) detectable/preventable failures, (b) age-related failures, (c) random failures, (d) random/sudden failures, or (e) intermittent failures.

For convenience, a list of failure modes collected from these sources is presented in Table 4-2. This table may include failure mechanisms (as defined above) but because the original sources identified these as failure modes this report maintained that classification.

Table 4-2 Collection of Digital System Failure Modes [132,133,134,135]

Open	Shorted	Output stuck high (high output)
Output stuck low (low output)	Supply open	Data bit loss
High leakage current	Slow transfer of data	Incorrect results
Alters data, address, memory	No output	Spurious operation
Fails to function	Erratic output	In-service problem
Faulty signal	Software failure	Instrument failure
Control failure	Calibration error	Human error
External events	Overload	No change in output (with change in input)
Functioned without signal	No function with signal	Maximum output
Intermittent operation	Functioned at improper signal level	Out of sequence
Corrupted input		

Specific operational experience data for digital devices has proven difficult to come by, especially for software failures. However, a review of software errors uncovered during integration and system testing of two spacecraft found that safety-related software errors are shown to arise most commonly from the following [137]:

1. Discrepancies between the documented requirements specifications and the requirements needed for correct functioning of the system, and

2. Misunderstandings of the software's interface with the rest of the system

Similarly, another study [138] found that only a tiny proportion of software failures can be attributed to bugs,[8] as detailed below:

1. The largest class of software problems arises from errors made in the eliciting, recording, and analysis of requirements.

2. The second largest class of problems arises from poor human factors design.

The two classes are related.

Gruhn and Lucchini report similar results for the failure cause of software errors [139]:

- Requirements: 56%
- Design errors: 27%
- Other errors: 10%
- Coding errors: 7%

The primary causes of failure by lifecycle phase are [140]:

8 *Bugs* refer to errors in the software code that cause a program to fail to meet its specification

- Specification: 44%
- Changes after commissioning: 20%
- Operations and maintenance: 15%
- Design and implementation: 15%
- Installation and commissioning: 6%

Especially for complex systems, it is difficult to discover all errors. In practice, one must assume that an undiscovered error remains when the system becomes operational.[9] especially for complex systems. Typically, a system (dormant error) may be discovered (i.e., becomes active). Thus, a software failure occurs as a result of the combination of a dormant error and the onset of the specific set of conditions that triggers the error. In general, it is difficult to predict the impact of a triggered fault. The fault may cause the system to behave in undesirable ways. In addition, since the fault is unknown, it is difficult to predict how it will impact the system when it does occur.

For convenience, a list of the causes of software-related failures collected from these sources is presented in Table 4-3.

Table 4-3 Causes of Software-related Failure Modes [135]

Incomplete description of requirements	Incorrect firmware coding
Faulty calculation in program	Requirements error
Incorrect interpretation of requirements	Task/Application crash
Inadequate software version control	Software update incompatible with design basis
Inadequate software V&V	Software lockup

Application-independent classes of failure modes from the DI&C processor can be defined and standardized at the processor level, with the I&C effects defined separately. The Advisory Committee on Reactor Safeguards (ACRS) provided a list of processor classes of failure modes reported in the literature (Table 4-4).

9 While developing the avionics software for the space shuttle, the National Aeronautics and Space Administration (NASA) determined that the statistical average for software used in critical systems (e.g., flight control, air traffic control, etc.) averaged 10 to 12 errors for every 1,000 lines of software code. Because this was unacceptable to NASA for use on the space shuttle, NASA forced one of the most stringent test and verification processes ever undertaken for the primary avionics system software. An analysis performed after the Challenger accident showed that the primary avionics system software (PASS) for the space shuttle had a latent defect rate of just 0.11 errors per 1,000 lines of code. However, this achievement did not come easily or cheaply. In an industry where the average line of code costs the government (at the time of the report) about $50 (written, documented, and tested), PASS cost NASA slightly over $1,000 per line. The total cost for the initial development and support for PASS was $500 million (http://history.nasa.gov/sts25th/pages/computer.html).

Table 4-4 Causes of Processor-related Failures [136]

Failure Mode	Description
Task crash	The control software task exits unexpectedly
Task hang	The process goes into an infinite loop
Task late response	The output of the task exceeds the specified response time
Task early response	The output of the task is too early
Task incorrect response	The output of the task is timely but violates specifications
Task no response	There is no output from the task (but the task is not hung)
Processor crash	The processor software kernel (or operating system) crashes bringing down all tasks running on the operating system
Corrupted input	The input signal from the plant sensors receives corrupted data due to either an analog electrical problem, an analog-to-digital conversion problem, or noise in a digital network
Corrupted output	The output signal to plant actuators is corrupted due to an analog electrical problem, a digital-to-analog conversion problem, or noise in a digital network is corrupted
Out-of-sequence data	Data packets arrive at the destination in a sequence different than expected (applicable to digital networks using transmission)

4.9 Component Data

Component data is hard to collect and even harder to assess if the failure data is appropriate for the use intended. May factors such as attributes, properties, critical characteristics, operating environment, use, how the data is collected, etc. is typically not provided and users accept the values without question. Failure data, even vendor supplied data, with millions of hours of use, does not reflect how the component will be used for specific applications and can result in unsubstantiated claims of reliability. As always, care should be used when relying on operating experience and component reliability data,

The limited data from operational experience in the NPP industry makes the use of reliability claims difficult to defend, although the non-nuclear industry has extensive operating experience, and vendors claim increased reliability. Complexity of the software can also impact its reliability. Even though the single execution sequence of a complex software system has a vanishingly small probability of occurrence, there is very little one can say about the reliability of any such system, no matter how long it has actually executed without a failure [119].

Some databases—such as the Equipment Performance and Information Exchange System (EPIX) that is maintained by the Institute of Nuclear Power Operation (INPO)—contain data, but the specifics are time consuming and difficult to obtain, and the data are not publicly available.

The reporting of hardware and software failures is critical for monitoring the reliability of EDDs. This is addressed under 10 CFR Part 21. Just as critical is the vendor's willingness to provide assurance that the licensee would be notified of OS software errors and to support any necessary configuration controls for any future required software changes. Although the use of EDDs is widespread in industry and vendors have data, specifics have not been obtained for review by this project.

Although EDDs are not systems (even though they are frequently treated as such), the software process characteristics for a system are applicable, including completeness, consistency, correctness, style, traceability, unambiguity, and verifiability.

Data for the evaluation of the credit that can be given to feedback experience should be collected, including site information, operational profiles, demand rate, operating time, error reports, release history [115].[10] However, an acceptable amount of feedback to take credit for operating experience requires data on devices with the same make, model, and software/hardware version operating in the same environment. Data on devices are difficult to obtain and become very difficult to collect on specific devices.

Vendor failure rates assume perfect operating conditions and perfect mechanical integrity, ignoring how the process and the operating environment contribute to equipment degradation and failure. Actual failure rates highly depend on the operating environment and MI and can be orders-of-magnitude higher than vendor-reported rates. Consequently, reliability data should be assessed based on field feedback: the less feedback, the more the uncertainty in the data [120].

The physical failure rates of smart sensors seem to be comparable to those of conventional sensors. Examples given by Meulen [121] show that the failure rate of the digital Honeywell STT250 smart temperature transmitter is calculated to be 3.9 × 10-7/h, and the failure rate of the digital Fisher-Rosemount 3051C Pressure Transmitter is 7 × 10-7/h: both failure rates are for all failure modes. The Nuclear Plant Reliability Data System (NPRDS) failure rate for analog transmitters is 1.42 × 10-7/h [122]. There is no reason to believe that the failure rate of smart sensors will be significantly better than for analog sensors, because conventional sensors are typically built using robust components, whereas smart sensors may contain more vulnerable components.

Prior to the release of IEC 61508, many manufacturers provided in-service and accelerated test failure data. Following the approval of IEC 61508, manufacturers increasingly began claiming compliance based on a shelf-state analysis with seemingly perfect operating environment conditions. IEC 61508 allows manufacturers to make SIL claims based on predictive analysis without any burden to substantiate the claims later using actual field data. However, the failure rates and PFD values declared in analysis reports are much better than those that can be achieved in actual field applications [123].

Failure rates are used to estimate the reliability of the devices. SAP ERL.1 [124] states,

> *The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods.*

Paragraph 191 in the SAP further states,

> *Where reliability data is unavailable, the demonstration should be based on a case-by-case analysis and include:*

10 NRC staff participated in the meetings of the Regulator Task Force on Safety Critical Software (TF SCS) for nuclear reactors, which is comprised of international nuclear regulators and authorized technical support organizations. The task force met from 2009 to early 2016 and NRC provided input to the 2015 revision of the report. Although the NRC did not endorse the 2015 revision for regulatory use by the NRC, it published it as a technical report in NRC's NUREG/IA series [NUREG/IA-0493].

(a) a comprehensive examination of all the relevant scientific and technical issues;

(b) a review of precedents set under comparable circumstances in the past;

(c) where warranted, e.g., for complex items, an independent third-party assessment; and

(d) periodic review of further developments in technical information, precedent and relevant good practice.

Because embedded systems are now largely defined and controlled by software, it is likely that software failures will form a major threat for reliability. Therefore, appropriate reliability analysis and design techniques should be provided to support the anticipation and prevention of potential failures. Diagnostics of active components should be self-evident, whereas diagnostics of standby components, although problematic, could be used to actuate and monitor the device's health.

Analyses can be used to support the reliability assessment of the EDDs [125]:

- Reliability
- Mean time between failure calculations
- Single point vulnerability studies
- Failure modes and effects analyses

If the reliability assessment demonstrates that the EDD's reliability is at least as good as the reliability of analog boards, then the reliability of the EDDs should be acceptable, and credit may be able to be given to the sufficiency of the device to meet its safety standards.

EDDs that have a limited amount of software and lines of code in EDDs (some contain as little as a few kilobytes of assembler code) may support a proven-in-use argument based on their large operating history. However, for licensees to use this argument they (or the vendors) would have to provide the data and basis to demonstrate EDD reliability.

Although there are significant differences in the systems in the various industries that use IEC SILs for demonstrated integrity and reliability of components, there is not much difference at the individual component level. Leveraging the similarities at the component level has the potential to lead to a mutually beneficial relationship for industries and manufacturers through a larger pool of operating history because of the larger customer base. However, care must be taken before installing any EDD in a safety application based on a generic reliability value rather than choosing one based on its integrity and reliability in a similar operating environment.

The available data on failure rates and diagnostic coverage do not provide detailed design information [121]. Manufacturers' evaluations may provide the numerical data required by IEC 61508-6—failure rates and fault coverage—but the details for arriving at those values may not be provided and may not be applicable.

Industry seems to over rely on failure data compiled from operating experience without determining if that data is appropriate to make a determination with respect to the critical characteristics for their specific use. The review of vendor material for EDDs highlights the overall reliability of the EDDs and licensees may not question the process conditions, operating

environment, service history, proper failure reporting and recording of data, and any modifications made to the device.

4.9.1 FMEA

After the failure modes for the digital parts of the EDDs are identified, an FMEA can be used to identify the potential effects of these failures on the components/system. Vendors, licensees, and applicants must understand the operation and failure modes of digital systems, including EDDs, as well as the effects of these failure modes on operations and safety.

The failure modes need to be understood and fully specified for each operating mode . Software requirements for handling both hardware and software failures should be provided, including requirements for analysis of and recovery from computer system failures. It is important to understand the full functionality of an EDD and its behaviors.

FMEA is a logical, structured process for identifying process areas of concern. FMEAs are typically used to show that the design meets the single failure criterion in 10 CFR 50, Appendix A, and to assess the potential for an undetectable failure. However, these uses of FMEA are at the system level.

More specific to this work is that FMEAs, at the component level, are used as part of the CGD process, determining the completeness of the diagnostics (if applicable). For evaluating component level reliability for IEC 61508 certifications, a failure modes, effects, and diagnostic analysis (FMEDA) is sometimes used.

In some cases, as described below, such as to determine if a malfunction with a different result could occur, multiple levels could need to be considered.

The effects of failure modes for the EDDs can be investigated at the following levels:

1. First-level effects: at the digital device's boundary
2. Second-level effects: on the component
3. Third-level effects : on the control or safety system
4. Fourth-level effects: on the plant/the safety function of the system

Determining the first-level effects requires knowledge of the failure modes for the I&C portion of the EDD.

Typically, the results from an FMEA at the component level are inputs to the FMEA at the system level. Similarly, the results from an FMEA at the EDD (device) level are input to the FMEA at the component level. The failure of the EDD and its effect on the associated component may be bounded by an existing FMEA that evaluates the failure of the component. This is bounding if no new failure mechanisms at the component level are introduced.

NEI 96-07, Rev. 1 (endorsed by RG 1.187), states,

> *Malfunctions of SSCs are generally postulated as potential single failures to evaluate plant performance with the focus being on the result of the malfunction rather than the cause or type of malfunction. A malfunction that involves an initiator or failure whose effects are not bounded by those explicitly described in the UFSAR [Updated Final Safety Analysis Report] is a malfunction with a different result. A new failure mechanism is not a malfunction with a*

different result if the result or effect is the same as, or is bounded by, that previously evaluated in the UFSAR.

Certain malfunctions will not be explicitly described in the FSAR because their effects are bounded by other malfunctions that are described.

The safety evaluation of the SSPS board replacements reported in Topical Report WCAP-17867-P [125], describes the FMEAs performed on the three safety-related boards. The FMEA studies resulted in two conclusions (as documented in the topical report):

1. There are no non-detectable failures that when paired with a detectable failure would cause a loss of safety function (Addressing IEEE 603-1991, Clause 5.1).

2. The new design boards do not produce a different failure mode than has been previously analyzed (Addressing GDC 23).Rather than using the FMEA for an EDD as input to the system and to the plant FMEA, an FMEA could, within the same table, consider the failure modes of the EDD and evaluate their effects to assess if there are any new failure modes at the system level or that affect the safety function. This is important to know prior to installation, because having no new failure modes at the component or system level means that there are no new consequences other than what has been considered previously.

This is similar to the FMEDA on the RadICS platform. The safety evaluation for the RadICS [144] states that the RadICS FMEDA was used as input data to support a system-level FMEA and reliability analysis for an NPP-specific RadICS Platform system. The RadICS FMEDA for the FPGA based Safety Controller (FCS) was performed for each platform module and includes four groups of module components.

In regard to the issue of CGD and FMEA, NRC IP 38703 [142] includes the following statement:

> *An evaluation of credible failure modes of an item in its operating environment and the effects of these failure modes on the item's safety function may be used in the safety classification of an item and as a basis for the selection of critical characteristics.*

Subsequently, NRC IP 43004 [143] states that technical evaluations should include "performance of a failure modes and effects analysis (FMEA) to identify the credible failure mechanisms of the item in the specific application under consideration."

Although not the only method, EPRI noted that "A failure modes and effects analysis (FMEA) is an effective tool to determine critical characteristics when complete design information is not available" [53].

Additionally, evaluating EDDs and their potential impacts at the system level may require extending the results of a component level FMEA to the system level, which then could be used in a plant level FMEA or PRA.

FMEDA is similar to an FMEA in that a systematic analysis technique is used to obtain subsystem / product level failure rates and failure modes with an added assessment of the diagnostic capabilities (i.e., the "D" in FMEDA) to detect failures. That is, an FMEDA combines the FMEA techniques with an extension to identify diagnostics techniques with failure modes relevant to safety instrumented systems. For example, the FMEDA for the RadICS platform analyzed

potential failures in each of its component groups and categorized the effects of these failures in terms of detectability/undetectability [144]:

- Fail-safe state (detected/undetected)
- Fail dangerous state (detected/undetected)
- Analog input (deviation more than 2% of span)
- Annunciation (detected/undetected)
- No effect
- Fail dangerous (undetected after surveillance test)

FMEA and extensions such as FMEDA are widely accepted methods for systematically analyzing a device to determine its hardware failure modes, their frequency, and their impact.

However, the key point is that these methods, FMEDA in particular for IEC 61508 certifications, are focused on random hardware failures. They explicitly do not consider systemic failures, and use operating experience indicating failures beyond what is anticipated by the FMEDA as an indication that there may be systemic issues with the component and would as a result require further review [276].

Further, FMEAs are limited in that they focus on singular events, CCFs are typically not evaluated, and the likelihood of multiple failures that are not evaluated could be more likely than the single failures.

Another challenge for FMEAs is software. Based on a review of software hazards analyses and software FMEAs, a collection by ORNL, based on the ORNL researcher's experience, of the consequences (effects) of a software hazard is provided in Table 4-5. Because the consequences (effects) from the failures of software in Table 4-5 are at the system level, they do not all apply at the EDD level. They can be used to inform those performing an FMEA on an EDD what types of effects are typically considered.

Table 4-5 Collection of the Consequences (Effects) of a Software Hazard

None	Loss of redundancy
Inadvertent trip	Failure to trip when required
False channel trip	Partial loss of redundancy; system remains operable
Display data failure	Loss of redundancy for division voting; system remains operable
Processor display; operator receives erroneous information	Inadvertent alarm
Inadvertent partial trip	Erroneous input data
Erroneous output display	

The NRC ACRS stated that "software FMEA methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable DI&C performance" [141]. This resulted in research by the NRC which is reported in RIL-1002 , which states that:

Appendix C describes six different SFMEA [software FMEA] techniques that were adapted from techniques originally developed for analyzing hardware failures. No sound technical basis was found to require or endorse that any of the SFMEA techniques be performed or submitted as part of licensing applications. Therefore, changes to established regulations and guidance is not recommended.

Below is a short (i.e., not inclusive) list of references that show issues or deficiencies with FMEAs that NRC staff and inspectors could consider that demonstrate additional methods of determining appropriate failure modes:

- NRC Information Notice 1997-081 [145] is not digital specific, nor EDD specific, but rather relates to failures under certain conditions where a component would not operate as it should under certain circumstances.
- L. Betancourt, et. al., [146] recognize that finding faults in CPLDs through FMEA "is akin to searching for a needle in a haystack." Although FMEAs have been successfully used for analyzing traditional hardware applying the technique to Complex Logic does not yield similar benefits.
- RIL-1002 [112] reviewed 11 sets of DI&C system failure modes. These failure mode sets are not supported by documented public consensus and are not endorsed by any accepted standards. The staff's analysis in the RIL found that a synthesized set of system level DI&C failure modes may not be helpful for determining the level of safety of a DI&C safety system. In addition, a limitation of the FMEA is that a digital system may experience unintended or undesired behaviors without the occurrence of a failure. The RIL recognizes that it is unlikely that anyone can identify a complete set of failure modes that can occur in a moderately complex digital system
- EPRI 300200509 [147] concludes that FMEA has its place, but also "The FMEA methods are well suited for postulating single failures and their effects on other systems, sub-systems or components, and they can make use of the proposed failure taxonomy provided in Attachment B. However, these methods are not well suited for use in identifying misbehaviors or hazards beyond single failures, such a multiple hardware failures or unintended interactions of hardware and software components."
- The FAA System Safety Handbook, Chapter 8 [148] considers FMEA and FMEC as means of reliability analysis versus safety analysis.

These issues apply more to some uses of FMEA than others. For example, in the case of using an FMEA to determine if there are new failure modes present at the system level, a review may find that new or potentially new failure modes at the level of the EDD or component are bounded. For example, although some new failure modes had been identified at the I&C level in ORNL/TM-2010/32 [132], these new failure modes did not create new failure modes at the system level. However even if certain types of failures are already considered at the system level, critical characteristics should still be utilized to prevent their occurrence. This particular type of bounding also does not address CCF concerns.

In conclusion, FMEAs are used at different levels and for different purposes and are utilized within the NRC's regulatory infrastructure and in industry. In some applications using the FMEA of an EDD as input to the FMEA for the system or considering them together could be useful. However, an FMEA has limited utility for assessing systemic causes in newer digital configurations. Specifically, systemic causes have pervasive effects whereas an FMEA is oriented to "point-failures" (localized, isolatable) as in the case of hardware items. Therefore, an FMEA may not be as robust in the discovery of (or confirming absence of) system-internal hazards rooted in system development activities. Multiple failures may be more important than single failures. Software failures are difficult to identify, so the effects are hard to predict. In these cases, modern methods

and tools designed to deal with more complex and connected systems may be needed for some applications of FMEA.

4.10 Graded Approach

A graded approach accounts for the characteristics of the risk relevant to a components function and application in a system. A number of parameters can be identified that together describe the nature of the hazardous situation when safety-related components/systems fail or are not available. Several parameters are identified that, when combined, demonstrate an acceptable design to meet the safety functions of the system. Attributes or metrics that can be applied to grade the classification of the EDD could be based on several factors, including complexity/simplicity, redundancy, diversity, safety function of the EDD, failure modes/hazards analysis, etc. Each of the characteristics—digital content, functionality, configurability, classification, and consequences of failure—can provide a basis for guidance on the acceptability of the design and functioning of the EDD. This would start with the current/default position for regulating the use of EDDs and could be tailored to specific component-based guidance.

The regulatory basis for using a graded approach based on safety significance derives from 10 CFR 50 Appendix B, which states, “The quality assurance program shall provide control over activities affecting the quality of the identified structures, systems and components, to an extent consistent with their importance to safety.”

The CGD process (i.e., EPRI TR-106439) is key in the use of EDDs, as most components are not developed under a 10 CFR 50 Appendix B process. A risk-informed approach was proposed in 10 CFR 50.69 and RG 1.174. As described below in observations, a risk-informed approach could also be used for CGD of simple digital devices.

he term *graded approach* could refer to the selective assignment of QA elements with which the software must comply based on its assigned quality classification, or it can refer to the grading of components based on risk. For this assessment, a graded approach is based on the latter—risk to the plant. Thus, a graded approach would tailor the effort’s requirements according to the complexity of the system and application and the importance to safety and plant economics. NRC Inspection Procedure 38703 [142] states:

> *The application of graded quality assurance to the CGI dedication process should include consideration of the item's importance to safety and the factors specific to the item being procured. Certain items and services may require extensive controls throughout all stages of development while others may require only a limited quality assurance involvement in selected phases of development.*

There are two factors to be considered in an EDD—the component in which it is embedded, and the sensor/actuator heart of the EDD. Sensors interact with the plant’s physical processes to measure process variables such as temperature, pressure, and flow. When sensors are embedded in components, they may provide surveillance and diagnostic capabilities that monitor process variables for abnormalities. Actuators such as valves and motors physically operate plant components to adjust physical processes to optimize plant performance for efficiency, safety, and/or shutdown. Actuator status indicators can also visually reflect automatic or manual control actions, such as the switching on or off of a motor or the opening or closing of a valve.

Devices vary widely in terms of functionality, complexity, and testability. EDDs serve many functions in components used in NPPs—monitoring, diagnostics, and/or control. The functionality provided by embedded systems is shifting from hardware to software. The functionality of

embedded systems is not solely developed by just one manufacturer, but it is host to multiple parties. In addition, embedded systems are increasingly integrated in networked environments that affect these systems in ways that might not have been foreseen during their construction.

Factors that could be considered for risk-informing the safety classification, level of review, and dedication of EDDs include:

- Complexity / simplicity
- Classification / quality
- Functionality
- Consequences of failure
- Configurability
- Redundancy
- Dependability
- Diversity
- Defense-in-depth
- Self-diagnostics
- Testing

A risk-informed process would adjust the level of rigor associated with the design to the safety significance of the equipment.

A two legged approach is expected in the demonstration of the suitability of a smart device for a nuclear application in the UK. The two legs consist of:

- Production excellence (PE), which is a demonstration of excellence in all aspects of production from the initial specification through to the finally commissioned system;

- Independent confidence building measures (ICBMs), which provide an independent and thorough assessment of the safety system's fitness for purpose.

The ICBMs provide a graded approach according to class. Examples of ICBMs at the highest class (Class 1/pfd = 10^{-3}) are:

- Instrument type tests
- Examination, inspection, maintenance and test records
- Proof test records
- Commissioning tests
- Hardware reliability analysis
- Prior use
- Supplier pedigree
- Independent certification
- Independent review of supplier's standards and procedures
- Independent functional safety assessment
- Independent review of tools
- Static analysis
- Dynamic analysis
- Statistical testing

ONR TAG-046, with respect to a graded approach, stresses that:

> *It is important to stress that the independent confidence building measures should be applied only to the finally delivered product - ie after completion of the manufacturer's verification and validation, including the completion of any compensating activities. The duty-holder may, however, be able to make a case for applying techniques to code that has completed the manufacturer's independent verification.*

One key part of the regulatory process, upon which NS-TAST-GD-046 [126] is based, is that the grading allowed in the guidance impacts the reliability claim that the licensee can take for the device. While ONR does use a best estimate PRA (called *PSA* within their regulatory infrastructure) for certain purposes, when it comes to determining the needed grade of a system, a high confidence value (limited as in Table 1 of the reference) must be used. This means that if one device is implemented at a lower grade, then it may result in others being required to be implemented at a higher grade. However, currently, no such reliability feedback mechanism as a consequence of using a graded approach exists within the NRC's regulatory infrastructure.

From a standards perspective, both the nuclear IEEE (e.g., IEEE Std. 603) and the nuclear IEC (e.g., IEC 61513) standards suites use system-level requirements that are not easy synthesized down to component- or EDD-level requirements. The area of reliability is a good example of this. In both nuclear standards suites, the system-level requirement for reliability is the single failure criterion. This requirement assumes some minimum level of reliability of the individual components, but it does not provide a clear requirement. There is no clear target for the reliability of the individual components. The situation is similar for other system-level requirements related to system architecture, such as redundancy, independence, and diversity. Of particular note is the area of CCF, which assumes that the systematic integrity of the individual components is insufficient, thus defeating redundant architectures. It remains a challenge to translate the IEEE and IEC system-level requirements related to this topic into component-level requirements.

Considering the complexity, classification, functionality, configurability, and consequence of failure is an approach that could be considered. Those countries with multiple safety classifications incorporate function or consequence into the safety classification. NASA uses a consequence-based approach. The IAEA's approach to the safety classification of SSCs considers safety classification (important to safety and not important to safety), functionality, and consequences that result if the function fails when it is required to perform, and it is also related to the consequences in the event of a spurious actuation [173]. DoD relates consequence to a condition, event, operation, process, or item whose mishap severity consequence is either marginal or negligible (*safety-related*) or a condition, event, operation, process, or item whose mishap severity consequence is either catastrophic or critical (*safety-critical*). EPRI recommends using a safety-significance–based graded approach that considers the context of the I&C in the plant, the likelihood of failure, and the failure consequences in assessing the adequacy of the implemented preventive and mitigative measures.

Each of these factors are addressed below and could be combined in some manner to provide a structured, defensible graded approach for the use of EDDs.

4.10.1 Complexity / Simplicity

While there is no consensus on the best way to quantitatively measure complexity, there is broad agreement that simplicity helps ensure high dependability, and it is expected that a qualitative assessment of platform and functional simplicity may be practical [150]. The simplicity of critical functions is fundamental in achieving reliable components and systems.

The complexity of the EDD, and whether it has a processor, and if so, the type of processor it has, all also impact the level of potential risk.

Other factors that could affect the complexity of the device include (1) whether the code manages the hardware directly, if there is a distinct operating system, if interrupts are used for device inputs and outputs and timing, and the size of the code (number of lines).

Changes that increase complexity should be considered very carefully. For example, adding automated self-testing features to the relatively simple safety function logic may add complexity to thefunctionality, with corresponding adverse effects on several aspects of development. More specifically, the requirements can become more complicated, making it more difficult to specify with high confidence that they were complete, correct, unambiguous, etc. With added complexity, it becomes more difficult to anticipate, specify, and test all the potential abnormal and faulted conditions that the system might observe, etc.

4.10.1.1 Complexity

There are many definitions of *complexity* with the common theme of “difficult to understand and verify.”

IEEE defines *complexity* as “the degree to which a system or component has a design or implementation that is difficult to understand and verify” [150].

The UK Ministry of Defence states that a system is classified as complex if its behavior cannot be verified by exhaustive testing [151].

The IEEE defines complexity as “the degree to which a system or component has a design or implementation that is difficult to understand and verify” [150, 152].

EPRI’s digital engineering guide (DEG) [154] addresses complexity in terms of configurability. This measure of complexity is based on the degree of configurability and how configurable a system or component is in the field. A key aspect of EPRI’s digital engineering guide is grading engineering processes by complexity. However, this complexity is not in terms of the absolute complexity of the functions being performed by the device, but rather by the degree of configurability left for the integrator to perform or for creation of application-specific code. Therefore, a device could ultimately achieve the exact same function, but in one case, more design was performed by the OEM, leaving only parameter setting and connections to the integrator or licensee, and in the other case, parts of the design were left to the integrator or licensee. Hypothetically this could result in identical devices, but the DEG would treat each case very differently.

Part of the appeal of smart sensors is that they allow integration without the need to understand the particulars of the sensor’s design. For example, for a smart sensor, purchasers rely on the OEM code and hardware within the sensor itself to perform functionality, such as analog-to-digital (A/D) conversion, filtering, and various checks on the signal being performed in the device itself. Furthermore, the software and hardware are created by the same company that created the sensor itself. However, the purchaser’s understanding of the complexity of the device and any potential consequences would be limited.

For manufacturers, higher complexity may mean a higher probability of errors in the design of the EDD. For users, higher complexity may lead to a greater probability of errors when setting up and maintaining an EDD. (Note that this also applies to I&C systems.)

The issue related to EDDs is that of complexity. For very simple and very old systems, the failure modes were relatively straightforward. As complexity increases, which can be the case in EDDs, using methods designed for more complex systems makes sense. When discussing the technical evaluation, EPRI TR-106439 supports this concept, stating that a step is to "determine how complex the device and the software are, which sets the levels of scrutiny for many aspects of the assessment." However, the additional digital oriented guidance in EPRI TR-106439 does not discuss FMEA nearly so much as it discusses a broader failure analysis in order to correctly identify requirements and critical characteristics.

A risk-based/graded approach would evaluate the complexity of the EDD with its level adjusted accordingly.

4.10.1.2 Simplicity

Simplicity—the converse of complexity—may provide a more useful attribute.

IEEE defines *simplicity* as "the degree to which a system or component has a design and implementation that is straightforward and easy to understand" [150, 152]. IEEE also recognizes that "All else being equal, a simpler system will be more reliable [155]."

RIS 1002 [112] defines *simplicity* (by changing the negative expression of complexity to positive) as "the degree to which a system or component functionality, design or implementation can be understood and verified."

For simplicity, IEEE Std. 7-4.3.2-2016 [26] states,

> *it is recognized that simplicity is not a measurable characteristic of a safety system. As such, no acceptable degree of simplicity can be established for these systems however, measures should be taken to avoid unnecessary complexity. Added complexity associated with the performance of functions not directly related to the safety function may introduce design errors or create system hazards. As an example, the added the complexity resulting from self-test and self-diagnostics can improve safety and reliability. A balanced approach is required between the hazards associated with adding functionality and the benefits those functions provide. All functions allocated to safety systems shall be justified, documented and analyzed to determine if hazards are introduced to the safety system.*

This shows that any added features to the EDDs, such as human systems integration (HSI), will result in additional risk of failures not associated with the original equipment when used by operators and maintenance personnel.

The question still remains as how to measure simplicity. A review by EPRI on Rosemount transmitters [156] provides qualitative metrics on assessing simplicity:

- No internal looping
- Embedded software is very small in size (less than 8K lines of executable code)

- Hardware is relatively simple
- Limited diagnostics (helps limit the size and complexity of the software)
- A single version of the software used for all identical EDDs

These qualitative metrics and the overall simplicity of the device strengthen the use of historical data in evaluating the adequacy of the transmitter.

To have very high simplicity in a design, the component (or system) should:

- Contain simple priority commands
- Have minimized device functionality as much as possible
- Demonstrate 100% testability

Appendix B of CSA N290.14-15 [94] provides guidance for determining an item's complexity. That appendix must be used in conjunction with the mature product method. A good summary of the approach to determining the complexity of a digital item is show in Table 4-6:

Table 4-6 Determination of Software Complexity [94]

Complexity level	Complexity categories		
	Lines of code	Internal modules	Interface complexity index
Low	< 1000	< 20	< 5
Medium	1000–9999	20–199	5–9
High	10,000-99,999	200–1999	10–29
Very high	≥100,000	≥ 2000	≥ 30

The proof-through-testing method can only be used for category 3 applications that involve items that fit into the low complexity designation as determined by Appendix B of CSA N290.14-15. This method involves running enough testing on an item to provide confidence that it operates correctly. The minimum successful test executions for a category 3 low complexity item is 250, and the minimum successful test hours is 100.

The preponderance-of-evidence method may be used for category 1, 2, or 3; this approach is dependent on engineering judgement. This method considers the following elements: proven-in-use arguments, partial compliance with applicable industry standards, evidence from a previous qualification, complementary testing, analysis of the candidate product, and use of verified software modules, objects, libraries, or components. A case is built to justify the use of a digital item based on any or all of these elements. This method is the most like the approach typically used in the United States based on EPRI TR-106439. This method also has some similarities to the approach prescribed in IEC 62671.

The code for smart sensors used in the United Kingdom has a number of distinctive features [111]:

- Assembly language was used in early devices, but C code is found in most modern smart devices.

- The code size is small; there are tens of thousands of lines of code, although this may increase significantly if the instrument includes fieldbus or other types of communication protocols. (A discussion of communication protocols is provided in Appendix E of this report.)

- There is no distinct OS; the code manages the hardware directly.

- Interrupts are used for device I/O and timing, so there are concurrent code threads.

These features are not surprising for small, embedded systems. The benefit of using EDDs compared to a system is that they are simple enough to be amenable to a wide variety of techniques while still providing real, practical examples for which the outcome of the analysis has value.

From the information gathered, a risk-informed / graded approach for the classification of EDDs was evaluated. A risk-informed / graded approach would eliminate requirements for low safety significant uses of EDDs and would have little adverse effect on safety while reducing unnecessary regulatory burden. An FMEA may be suitable to fully evaluate simple devices and could provide insights into more complex devices. That is, if the EDD has been designed to accomplish only one clearly defined function or only a very narrow range of functions, the complexity is low, and including V&V efforts as part of a component's quality design process should minimize the likelihood of a latent fault. In contrast, if the device is designed so that it is reprogrammable after manufacturing, or if the device functions can be altered in a general way so that it performs a conceptually different function, it would not be considered a simple device. To be deemed a simple device only pre-defined parameters can be configurable by users. These variables could be used in defining a classification of EDDs.

In conclusion, simplicity may be measured primarily through executable code size, functionality, and testability. These can be useful in making guidance on a graded approach.

4.10.2 Classification

In the nuclear power industry I&C systems have been historically classified according to safety significance. This classification approach is based on a deterministic assessment of the system functions' ability to assure safety. Safety classification is well established, and the scope of this project does not involve replacement or modification of the current structure. Nevertheless, safety significance is a key characteristic of I&C systems at NPPs, and there are notable variations within international safety classifications. A risk informed/graded approach to providing guidance to assess the risk of EDDs would require insights into a classification scheme for components and subcomponents, such as an EDD. Therefore, this section provides an overview of the prevailing safety classification approaches employed by the international nuclear power industry.

Safety classification is one of the fundamental safety concepts used to ensure that NPPs pose minimal risk to public safety. The classification of SSCs identifies the importance to safety for that SSC and the consequence of its failure. The classification of SSCs is closely related to the plant states and the postulated initiating events.

The term *plant states* can refer to the events to be considered for plant operation— normal operating states and anticipated operational occurrences [AOOs], or the term can be used to identify the status of the plant to be reached after an event has occurred—physical conditions such as pressure, temperature, radiation, etc.

The classification of safety systems between countries, organizations, and even within the same organization may have a common term, but the terms may or may not have different meanings. For example, within the NRC, there are examples of terminology differences and overlaps regarding coverage for safety-related, regulatory treatment of non-safety systems (RTNSS), safety-significant systems requiring special treatment, and important-to-safety SSCs. If a component is classified as RISC-2, it is in a nonsafety-related system that performs a safety-significant function.

10 CFR 50 establishes a classification approach for SSCs in a nuclear facility. 10 CFR 50.2 defines safety-related SSCs in terms of reliance on those SSCs to remain functional during and after design basis events to assure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain a safe shutdown condition, and (3) the capability to prevent or mitigate the consequence of accidents that could result in unacceptable offsite exposures.

For electrical and I&C equipment, 10 CFR 50.49 documents the requirements associated with environmental qualification of electric equipment important to safety for nuclear power plants. The scope of the electric equipment important-to-safety covered by this regulation is safety-related systems, those nonsafety-related systems whose failure under postulated environmental conditions could prevent satisfactory accomplishment of safety functions, and certain post-accident monitoring systems.

NRC's regulatory guidance for classification for EDDs would be the same as for systems: safety or nonsafety, although in some instances the classification could be at the subcomponent level. This allows individual pieces parts, like a spring or bonnet to be classified at a lower level than the component it is a part of. The U.S. nuclear industry has a clearly defined level of rigor at the system level, but because the framework only contains two categories, the level of rigor at the individual component level is vague. A prime example of this is in commercial-grade dedication of digital components. In the guidance and standards associated with this type of activity, it is commonly stated that the level of rigor should be determined based on the "safety significance and complexity of the device" [157]. EPRI 107339 [77] states that "the safety significance and complexity of the equipment and the application determine the scope of activities required to accept the equipment — this is referred to as a 'graded approach'."

IEEE identifies I&C systems that are important to safety as *Class 1E equipment*. More specifically, IEEE Std. 323-2003 [158] defines Class 1E as the "safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment."

In addition to the traditional deterministic classification approach, a risk-informed approach to safety classification has been established in 10 CFR 50.69. Specifically, SSCs are divided into risk-informed safety classes based on both deterministic safety classification and probabilistic significance to plant safety. In this classification approach, insight from a probabilistic risk assessment (PRA) on the safety significance of the function performed by a system is captured based on its contribution toward reducing the risk of release of radioactive material to the

environment. 10 CFR 50.69 defines a *safety-significant function* as "a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk."

10 CFR 50.69 applies a risk-informed categorization and treatment of SSCs into four risk-informed safety classes (RISCs) for passive advanced light water reactors:

RISC-*1* SSCs: safety-related SSCs that perform safety significant functions.

RISC-*2* SSCs: nonsafety-related SSCs that perform safety -significant functions.

RISC-*3* SSCs: safety-related SSCs that perform low safety significant functions.

RISC-*4* SSCs: nonsafety-related SSCs that perform low safety significant functions.

A *safety significant function* is a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk.

The RTNSS process applies broadly to those nonsafety-related SSCs that perform risk-significant functions and therefore are candidates for regulatory oversight. The RTNSS process uses the following five criteria to determine those SSC functions:

1. SSC functions relied on to meet deterministic NRC performance requirements such as those set forth in 10 CFR 50.62 for mitigating anticipated transients without scram (ATWS) and in 10 CFR 50.63 for station blackout (SBO).

2. SSC functions relied on to ensure long-term safety (beyond 72 hours) and to address seismic events.

3. SSC functions relied on under power-operating and shutdown conditions to meet the Commission's safety goal guidelines of a core damage frequency (CDF) of less than 1×10^{-4} each reactor year and a large release frequency (LRF) of less than 1×10^{-6} each reactor year.

4. SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents.

5. SSC functions relied on to prevent significant adverse systems interactions.

The Regulator Task Force on Safety Critical Software (TF SCS) for nuclear reactors is comprised of international nuclear regulators and authorized technical support organizations. Although the NRC is not a member of the TF SCS, the NRC staff have participated in meetings and have documented this participation in NUREG/IA-0463 [179]. A common position of those participating in the task force is as follows:

> *For a smart sensor/actuator, the licensee shall define the safety class, which shall be the same as the class of the system in which the smart sensor/actuator is embedded unless justified otherwise.*

Using lessons learned from how other regulators, industries, and countries are addressing the regulation and use of EDDs requires an understanding of how the devices are classified in terms of safety. The World Nuclear Association's task force on digital I&C [161] identified the following difficulties in classifying the I&C safety functions:

- *Inconsistency between international standards and local regulations*
- *Ambiguous requirements for safety classification*
- *Incomplete rules for I&C function categorization*
- *Inconsistent requirements for systems provided specifically as diverse backup to protection systems*

A summary table of classification grades for systems is provided in Table 4-7. The data in this table is based on information from several organizations [159, 160, 161, 162]. The table does not represent precise relationships among the various categories in the classification of systems, but rather, it provides a qualitative assessment of the relative binning. While the table does not constitute a high-fidelity mapping of the classes and categories, it is intended to provide a general indication of the approximate relationship among the classification approaches. The summary table shows that the classification is not standard between countries and that the classifications and require interpretation by vendors and utilities. Therefore, classification based the methods used in other countries could be challenging to extend to U.S. regulations. However, lessons could be learned from other classification systems that may align with NRC regulations. For example the NRC may be uncomfortable with using reasoning for class 3 systems in the UK classification in safety-related systems, but class 1 systems might be acceptable for any safety related system. Similarly, the classification using IEC SILs and the ability to have different SILs for the same component depending upon its application and having separate hardware and software SILs for the same device may provide insights into providing guidance for EDDs at the individual component level.

The United States has the most coarsely graduated classification scheme—safety-related/not safety-related—and a more finely graduated scheme based on 10CFR50.69—RISC values. GDC 1—quality standards and records, and GDC 21—protection system reliability and testability, provide some flexibility in that the systems important to safety, including the protection system, shall be designed fabricated, erected, and tested to quality standards *commensurate* with the importance of the safety functions to be performed. However, when ordering parts from vendors for nuclear facilities, licensees order *safety* or *nonsafety* parts; other designations are confusing to vendors (e.g., the DOE safety class designations, based on the experience of the ORNL researchers).

The ***critical characteristics*** are identifiable and measurable attributes and variables of a CGI, which once selected to be verified, provide reasonable assurance that the item received is the item specified [73]. When applied to NPPs licensed pursuant to 10 CFR Part 50, critical characteristics are those important design, material, and performance characteristics of a CGI that, once verified, will provide reasonable assurance that the item will perform its intended safety function [163].

If the classification systems in use or proposed based on consequences were tailored to components, then the EDDs that monitor or provide diagnoses of the health of the component would likely be in the lowest classification category. In addition, because the consequences of a single failure are low, the classification category, even for those EDDs that provide control functions, would not be very high if the likelihood of a CCF were considered low. If communication is added, then the device now behaves like a system, and CCFs are a potential contributor.

NUREG/CR-6421 [164] uses a classification scheme based on the importance to safety of the system in which the product will be used. The suggested number of categories is larger than two (safety and nonsafety) and less than five. The suggested safety categories of A, B, C, and unclassified in the NUREG/CR are derived from a predecessor to IEC 61226 and RG 1.97.

Table 4-7 Comparative NPP I&C Safety Classifications [159, 160, 161, 162, 173]

National or international standard		Safety classification grade			
U.S. (NRC)		Systems important to safety			Not important to safety
		Safety-related			Not safety-related (Nonsafety)
IAEA NS-G-1.3		Systems important to safety			Systems not important to safety
		Safety system	Safety-related system		
IAEA SSG-39		Systems important to safety			Systems not important to safety
		Safety system	Safety-related system		
IAEA SSG-30	Function	Category A	Category B	Category C	Non-classified
	System	Class 1	Class 2	Class 3	
IEC 61508		IEC SIL 3/4	IEC SIL 2	IEC SIL 1	IEC SIL 0
IEC 61226		Category A	Category B	Category C	Unclassified
IEC 61513		Class 1	Class 2	Class 3	
Canada		Category 1	Category 2	Category 3	Category 4
European utility requirements (EUR) time dependent		F1A (automatic)	F1B (automatic and manual)	F2	Not classified
Finland		Class 2	Class 3	EYT/ STUK	EYT
France N4		1E	2E / SH	Important to safety	Systems not important to safety
France		F1A	F1B	F2	Non classified
Germany		Category A	Category B	Category C	Non-classified
Japan		PS1/MS1	PS2/MS2	PS3/MS3	Non-nuclear safety
India		1A	1B	1C	NINS
Korea		IC-1	IC-2		IC-3
Russia		Class 2	Class 3		Class 4
Switzerland		1	2	3	Non-classified
UK		Class 1	Class 2	Class 3	Not classified

EPRI 1025243, Rev. 1 [165], endorsed by RG 1.231 [166] (with exceptions), uses two functional safety classifications for the acceptance of commercial-grade computer programs—safety-related and non-safety–related. A subset of non-safety–related items may be classified as *augmented quality*. EPRI 3002002289 [167], which is not endorsed by RG 1.231, supersedes EPRI 1025243.

As with hardware, when a computer program having the functional safety classification of *safety-related* is furnished as a commercial item, it should be procured as commercial grade and dedicated for use as a basic component in a safety-related application.

EPRI NP-6895 [168] documents the functional safety classification process for plant SSCs in detail. The safety classification of computer programs is performed to determine if any function(s) performed by the computer program could prevent associated SSCs from accomplishing their safety-related functions. If a postulated failure of a computer program (failure of a function performed by the computer program) could impact the capability of an associated SSC to perform its safety-related function(s), then the computer program is considered to be safety-related. Therefore, functions of a computer program associated with SSCs could be identified as part of the safety classification process for computer programs.

The U.S. Department of Energy (DOE) uses three categories of SSCs plus an additional category that does not involve equipment: safety class, safety significant, non-safety, and specific administrative controls. None of these categories correspond to the definitions used by NRC.

The NEET project proposed a four-category classification structure:

- No impact
- Low impact
- High impact
- Critical impact

The classification structure is based on the high-level characterization of potential impact of failure of an EDD on an instrument's performance of its fundamental function. The classification framework can provide a means of preprocessing information about equipment with an EDD to support a determination of when and how a diversity and defense-in-depth analysis should be performed. This project is complementary to and not duplicative of the current NRC EDD project.

For the FAA, software is classified based on how an error affects the software and the system containing the software [169]. The software classification defines the rigor necessary to demonstrate compliance with software development requirements.

NASA uses a software classification system that is unique to the industry in that embedded system software, support software, software tools, and routine office software are all covered by the single classification system [170].

The railway industry uses a probabilistic risk-based process for safety-related system and software development [171].

Another name for *safety categorization* could be *risk index*. NASA separates the system risk, which specifies the hazard risk for the system as a whole. NASA's Software Hazard Risk Index is given in Table 4-8. The level of risk relates directly to the amount of analysis and testing that should be applied to the software.

NASA's hazard prioritization is important for determining allocation of resources and acceptance of risk. Hazards with the highest risk of Level 1 are not permitted in a system design. A system design exhibiting "1" for hazard risk level must be redesigned to eliminate the hazard. The lowest risk levels of "5" and above require minimal, if any, safety analysis or controls. For risk levels 2, 3, and 4, the amount of safety analysis required increases with the level of risk.

Table 4-8 Software Hazard Risk Index [70]

Software hazard risk index	Suggested criteria
1	High risk: significant analysis and testing resources
2	Medium risk: requirements and design analysis and in-depth testing required
3–4	Moderate risk: high level analysis and testing acceptable with management approval
5	Low risk: acceptable

EPRI 1025243 uses two functional safety classifications: *safety-related* and *non-safety-related*. A subset of non-safety-related items may be classified as *augmented quality*.

EPRI NP-6895 documents the functional safety classification process for plant SSCs in detail. The safety classification of computer programs is performed to determine if any function(s) performed by the computer program could prevent associated SSCs from performing their safety-related functions. If a postulated failure of a computer program (failure of a function performed by the computer program) could impact the ability of an associated SSC to perform its safety-related function(s), the computer program is safety-related. Therefore, functions of a computer program associated with SSCs could be identified as part of the safety classification process for computer programs. There are two deterministic methodologies that result in a functional safety classification—one that considers failure modes, and effects and one that considers the impact that the computer software has on associated SSCs.

The primary contributors to assuring adequate protection will likely be different for safety and non-safety equipment for several reasons. EPRI succinctly discusses the differences between safety and nonsafety equipment in the passage shown below [149]:

> *Safety Systems*
>
> *Safety equipment have nuclear quality assurance pedigree, including qualification testing, with corresponding documentation. Software development practices and documentation will be in accordance with relevant nuclear safety standards and guidance. The system functionality will tend to be relatively simple, permitting high test coverage and a lower likelihood of requirements and design errors, but the operating experience may be limited, especially for systems developed specifically for nuclear safety applications. Safety equipment will also benefit from design requirements for separation and independence, which help decrease the likelihood of CCF. For safety systems, coping analysis is typically done using best estimate assumptions, ostensibly because its nuclear safety pedigree is adequate assurance that the likelihood of a CCF is quite low.*
>
> *Non-Safety Systems*
>
> *In contrast, non-safety equipment is likely to be commercial grade, for which development practices, qualification testing and documentation vary widely. Operating experience may prove far more useful, provided it is sufficient, successful, relevant to the intended application and adequately documented. Mature commercial systems are likely to have defensive design measures that have been shown to be effective in avoiding and eliminating potential triggers, because of efforts to address problems and increase dependability as the product evolved. Nonsafety systems are often*

of lesser risk significance, so for them, reasonable assurance and adequate protection may be achievable at a more modest level than for safety equipment. For non-safety systems, coping analysis using best-estimate methods may be justifiable on the basis of its strong defensive design measures and lesser risk significance.

The IAEA defines a *deterministic safety classification for I&C systems* in IAEA Safety Guide NS-G-1.3 [172]. The classification approach involves assigning a safety class based on the importance to safety of the function performed by the I&C system. Thus, the safety guide divides I&C systems into *systems important to safety* and *systems not important to safety*. An I&C system important to safety is one whose malfunction or failure could lead to unacceptable radiation exposure of the site personnel or members of the public. Systems important to safety are further subdivided into *safety systems* and *safety-related systems*. Safety systems perform protective functions, while safety-related systems are those I&C systems that perform important functions other than the main protective functions.

IAEA's approach to classification typically begins with categorization of the functions to be performed by I&C systems, which are assigned to categories according to their importance to safety. The safety importance of a function is related to the consequences that result if the function fails when it is required to perform, and it is also related to the consequences in the event of a spurious actuation [173].

The IAEA classifies the safety class of SSCs based on the severity of consequences of their failures (Table 4-9).

Table 4-9 IAEA Safety Classes of SSCs Based on Consequence of Failure [174]

Safety class	Description
1	Any SSC whose failure would lead to consequences of *high* severity
2	Any SSC whose failure would lead to consequences of *medium* severity
3	Any SSC whose failure would lead to consequences of *low* severity

The standards issued by the IEC adhere to the safety principles established by the IAEA. The IAEA and IEC approaches that start with the classification of the functions and then assign categories according to their importance to safety agree well with the use of a graded approach. However, the IEC refines the safety classification approach established by the IAEA by resolving the important to safety class based on a three-tiered approach to identifying both I&C systems and the functions they perform. The IEC safety classification approach is based on the IAEA safety philosophy and the plant design basis. All SSCs that are items important to safety, including software for digital I&C systems, are classified on the basis of their function and their significance with regard to safety. Basically, I&C systems that provide functions to cope with postulated initiating events (PIEs) are classed in the highest safety class, whereas less important functions and equipment are assigned to lower safety classes. The IECs highest safety class is similar to the NRC's definition of s*afety-related SSCs* as those SSCs that are relied upon to remain functional during and following design basis events.

IEC standards provide criteria for assignment of functions to safety categories and establish design requirements for the corresponding I&C systems and equipment. In IEC 61513 [79], the general requirements for I&C systems important to safety are established in terms of safety classes. I&C systems are assigned to one of three safety classes—Class 1, Class 2, and Class

3—or they are unclassified based on their main safety function. The determination of classification for safety functions is established in IEC 61226 [175]. This standard classifies functions into three categories—Category A, Category B, and Category C. Category A corresponds to functions that play a principal role in achieving or maintaining safety by preventing design basis events from leading to unacceptable consequences. Category B covers functions that play a complementary role to the Category A functions in assuring safety, especially functions required to operate after a nonhazardous stable state has been achieved. Category B also includes functions whose failure could initiate a design basis event or worsen the severity of an event. Category C addresses functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Other functions that do not meet the criteria of the three categories are identified as *nonclassified* (NC).

IEC 61226 [175] establishes a method to classify I&C systems and equipment according to their importance to safety. The classification of I&C functions depends on their contribution to the prevention and mitigation of PIEs. The resulting classification is then used in IEC 60880 [81] and IEC 62138 [82] to determine relevant specification and design requirements, including qualification requirements for software tools used to develop I&C software and systems important to safety.

IEC categories of I&C functions [177] are:

- Category A: any function that plays a principal role in ensuring nuclear safety
- Category B: any function that makes a significant contribution to nuclear safety
- Category C: any other safety function contributing to nuclear safety

IEC 61513 [79] defines the following classes, which are similar to the categories in IEC 61226:

1. Class 1: – any SCC that forms a principal means of fulfilling a Category A safety function

2. Class 2 – any SCC that makes a significant contribution to fulfilling a Category A safety function or forms a principal means of ensuring a Category B safety function

3. Class 3 – any other SCC contributing to a categorized safety function

Office for Nuclear Regulation (ONR) TG-046 [126] relates the safety class to the probability of failure on demand for standby and frequency of failure per year for active components. TG-046 states that “the safety demonstration of hardware elements of CBSIS [computer-based systems important to safety] should take account of relevant standards. In particular, systems classified as either class 1 or class 2 should follow IEC 60987. Class 3 systems should follow IEC 61508 as a minimum.”

By default, EDD/component combinations in those systems with potential safety consequences given their failure (e.g., digital sequencers, sensors, motor control centers, diesel generator sequencers, uninterruptible power supplies) will pose regulatory challenges to implementation. This is because guidance for classification of components is based on the classification of systems or the safety functions of those systems and not on the consequences of the failure of those components. Thus, an EDD is typically treated as the same safety class as the component, which is the same safety class as the system, regardless of the consequences of failure.

It is unlikely that the failure of a single EDD, even one used for control, would lead to high or medium severity consequences. Consider as an example one of the components likely to have

an EDD—a pump controller. The pump controller used in this example contains a microprocessor, and therefore contains both hardware and software. Pump controllers can be used for managing pump flow and/or pressure, from full off to full on, and may incorporate flow or pressure control via varying pump speed or use of flow or pressure control valves, utilization bypass lines, etc. Digital displays provide access to the performance and condition of the pump and well as other integrated components. Failure modes of the pump controller are not taking corrective action when needed or incorrectly taking action by adjusting pump flow and/or pressure when no action is required. The effect on the system, via the pump, is no flow, low flow, or high flow. Thus, an incorrect response from the pump controller results in the incorrect control of the pump flow and/or pressure for one pump in one flow loop. Failure to correctly respond or an incorrect response from this pump (and its controller) meets the single failure criterion because of redundant pumps in redundant flow loops.

A risk-informed approach allows a finer gradation of classifications than the safety/nonsafety method. Any deviation from this categorization must account for what vendors can provide. For example, a vendor may not be able to provide a RISC-3 component but could deliver a safety-related component or an IEC SIL 2 or 3 component. Some countries assume that an IEC SIL 3 component is comparable to a component designated as safety related, so their licensees can purchase IEC SIL 3 components. However, regulators that accept IEC SIL ratings recognize that certifications to a specific IEC SIL by themselves cannot be used as a basis for qualification because licensees are responsible for what is installed in their plant [176].

It is difficult to correlate safety classifications across agencies, standards, and uses. The NRC's categorization of safety/not safety does not match well with most other agencies and does not lend itself to risk-informing component/system failures. In the nuclear arena, IAEA, Canada, Finland, France, Germany, Japan, India, Switzerland, and the UK have finer granulations of safety classifications. This finer granulation could present a viable risk-informed classification of components/systems.

4.10.3 Functionality

Function relates to purpose and could serve as a primary basis for establishing safety classification. For example, UK, Germany, and France relate the safety function of the device to its classification of safety for the SSC whereas India considers the consequences of the failure rather than the function. Much of the guidance on functionality acknowledges the difference between control and non-control functionality. However, a low functionality EDD may still provide a control function. In addition, the functionality of the EDD may be different than the functionality of the device. For example an EDD that only performs diagnostics could be present within a pump without having a control function, or within a sensor without having a monitoring function.

SRP BTP 7-17 [178] states that "The safety classification of the hardware and software used to perform automatic self-testing should be equivalent to that of the tested system unless physical, electrical, and communications independence are maintained such that no failure of the test function can inhibit the performance of the safety function." A device with diagnostic or display functionality will need to maintain physical, electrical, and communications independence from the control functionality, otherwise it would need to be considered part of the control functionality or an "other auxiliary feature."

NUREG/IA-0463 does not separate the functionality from the classification of the component, but it aligns with Appendix B and Part 21 with the statement "unless justified otherwise."

The first step in the development of a graded approach is to identify the types of functions performed by EDDs and to separate those functions into non-control functions and control functions.

A risk-informed / graded approach based on the functionality of the EDD would evaluate the complexity of the EDD with its function to set the level of review sufficient to reach a safety conclusion. Devices performing simple monitoring, a low functionality with the lowest complexity level, may not require much guidance on software tools or type of digital device. At the other end of the graded approach, existing guidance would apply to those EDDs that perform a control function with more scrutiny if the component performs a safety function. However, the control function assessment could be graded based on its simplicity. Thus, an understanding of the EDD's functionality can be applied to facilitate a graded approach to qualification, testing, and inspections.

Even a device with non-control functionality must demonstrate that its failure would not compromise a safety function, either by demonstrating non-interference or by constructing a safety demonstration that considers the nonsafety functions as if they are safety functions [126].

EDDs that perform self-diagnostics and can alert users to failures or degradations should reduce the failure rate of the NPP. In addition, the operability of the component (i.e., active or on-demand) will influence the likelihood of a failure being detected or not. The use of a watchdog timer could initiate a corrective action given certain software malfunctions.

As defined at the device level (in this case the EDD), this functionality differs significantly from that at the system/plant level. The functions identified in IEC 61226 [175] are very high level and are the measures of quality by which the adequacy of each function in relation to its importance to plant safety is ensured. For example, one of the Category A functions for the I&C system is to shut down the reactor and maintain it in a subcritical state. An initial safety analysis of the specific NPP design is required to be completed prior to the classification of the I&C functions.

Similarly, the fundamental safety functions identified in IAEA NS-R-1 [180] and IAEA SSG-39 [16] are at the plant level. These functions identify the following fundamental safety functions for an NPP for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store, and (iii) confinement of radioactive material, shielding against radiation, control of planned radioactive releases, and limitation of accidental radioactive releases.

IAEA recommends that the functions required for fulfilling the main safety functions in all plant states, including modes of normal operation, should be categorized on the basis of their safety significance. These documents acknowledge that at a lower level, the use of digital systems for I&C functions provides advantages that include the flexibility to provide complex functions, improved plant monitoring and improved interfaces with operators, as well as the capability for self-test and self-diagnostics, a better environment to facilitate the feedback of the operating experience based on tremendous capabilities for data recording, small physical size, and minimal cabling needs. Digital systems can include test and self-check functions that improve reliability, and they can provide a means for monitoring the status of the plant to ensure that the required safety functions are fulfilled. The required safety functions are determined based on the NPP design process, and a systematic approach must be required to be followed to allocate these functions to plant SCCs. A risk-informed / graded approach could eliminate or reduce requirements for low safety significant uses of EDDs and would have little adverse effect on safety while reducing unnecessary regulatory burden.

Software CCF is always a concern for digital systems. The functionality of the EDD will greatly influence the concern of a software CCF. If the functionality is to monitor, provide information, or perform diagnostics, its failure could be more of a nuisance rather than a safety concern. However a CCF of sensors measuring a process variable could prevent a reactor trip. A risk-informed approach may recognize that there is not an increase in plant risk if used in this way. Thus, even if the EDD has some limited control function, its failure may or may not be a safety concern.

One method that could be used to assess the risk because of the failure of an EDD would be to evaluate its risk using an FMEA at the component level and as input to a system level FMEA. An FMEA may be applicable for simple devices and could provide insights into more complex devices. If the EDD has been designed to accomplish only one clearly defined function or only a very narrow range of functions, then the complexity is low (i.e. it is a simple device of limited functionality), and V&V efforts on a quality-designed component should minimize the likelihood of a latent fault. Furthermore, if the device is designed so that it is re-programmable after manufacturing or the device functions can be altered in a general way so that it performs a conceptually different function, then it would not be considered a simple device; only pre-defined parameters can be configured by users.

Related to this, an FMEA would evaluate the failure modes from any known hardware and software faults and failures and would also assess how the vendor resolved or addressed each of these known failure modes. The FMEA would evaluate whether these failures affect the functionality of the EDD and whether the vendor has addressed these failures in the user documentation, although the FMEA may not be available.

4.10.4 Configurability

Programmablity represents the capability within hardware and software to change; that is, to accept a new set of instructions that alter its behavior. Programmability generally refers to program logic. Configurable logic and flip-flops can be linked together with programmable interconnects. Memory cells control and define (1) the function that the logic performs, and (2) how the logic functions are interconnected. PLDs come in a range of types and sizes, from simple programmable logic devices (SPLDs) to FPGAs.

Configurability represents the extent to which the system/component facilitates selection, setting up and arrangements of its modules to perform I&C tasks. For hardware, configuration methods include connections by wiring, setting jumpers or switches, and inserting modules (on-line or off-line) [34]. Software configuration methods include selecting and setting parameters, programming, inserting software modules, down-loading programs (on-line or off-line), etc. An EDD may be configurable but not programmable, such as one with fixed firmware. Other devices can be configurable and programmable. Thus, configurability, programmability (and complexity) can vary greatly between devices. It is important to note that the ancillary functions that provide configurability must also be evaluated.

In most instances, dedicated devices are typically pre-developed devices with specific functionality. Once the configuration is changed it is not the same as the device that underwent factory acceptance testing or CGD. Therefore, prior to installation its use it would need to be reevaluated.

The configurability or programmability of the EDD represents the extent to which the system/component facilitates selection, setting up and arrangements of its modules to perform

I&C tasks. Configurability can be either through hardware, such as through the use of wiring, setting jumpers or switches, inserting modules, or through software configuration methods such as selecting and setting parameters, programming, inserting software modules, down-loading programs. IEC 62671 [17] states that restricted configurability applies to devices that can be configured in only very limited ways to select from among relatively few options the manner in which a device will function in its intended application. An HMI can allow increased configurability.

The more complex a device, the greater the potential that it is configurable; reconfigurability increases the likelihood of the device being reused, which in turn increases the potential for the reconfigured device adversely affecting the execution of a safety function [181]. Reconfigurable devices will also necessitate an increase in the level of V&V that should be required.

HMI can significantly increase the capabilities and ease of changing the configurability of the EDD. By separating aspects of the system such as configurable vs. programmable or critical vs. non-critical functions of the device, it is possible to bound the scope of the dedication process. The goal is to reduce uncertainty via techniques to provide more supporting evidence for devices that lack pedigree (i.e., a lower RISC or IEC SIL).

Some devices are designed not to be re-programmable after manufacturing; nor can the device functions be altered in a general way so that it performs a conceptually different function. In these types of devices, only predefined parameters can be configured by users.

Examples of types of firmware are listed as follows:

- Non-configurable, non-modifiable firmware: oven controller, diesel generator, pump
- Configurable, nonmodifiable firmware: fire alarm control panel, flow meter, spectrometer
- Modifiable firmware: PLC, PAL, PLA, CPLD, FPGA

The engineers at ORNL's HFIR classify devices in two forms—configurable or modifiable—by asking the question "can you make changes to the software on the EDD?" If changes cannot be made to the software, then it is classified as *configurable*.

IEC 62671 [17] provides the following guidance for the functions of a candidate device of limited functionality that is configurable and the ancillary functions that provide configurability:

> a. *The configuration parameters of the primary functions shall be limited in capability to on/off (activate/de-activate) settings or scale-like adjustments such as calibration of process range and output, gain or damping setting, etc.*
>
> b. *For systems applications of class 1 and 2, configuration protection shall include deliberate design features so that more than one mistake is necessary before an error in setting a configuration parameter is committed.*
>
> c. *The configuration parameters of the primary functions shall be protected from inadvertent, malicious or unauthorised adjustment in a manner consistent with the overall security plan for the nuclear facility (see 5.4.2 of IEC 61513). This protection shall include password protection if it is supported by the candidate device.*
>
> d. *Where it is necessary to configure ancillary or superfluous functions so that they cannot interfere with primary functions these configuration parameters shall be protected as in items b) and c).*

e. *It shall be possible to check a device after its configuration parameters have been changed to verify that the change has been done correctly.*

f. *If the device provides operators with display or modify-enabled access to configuration parameters, then the device shall provide enabled access for only those configuration parameters that they require to execute their duties.*

g. *Where the device provides operators with modify-enabled access to configuration parameters, all operator inputs shall be subject to applicable range and validity checks and or limits appropriate to the application.*

h. *Where it is required that configuration parameters and any necessary associated logic states be automatically restored following a power failure, whether partial or total, and this property is configurable, these configuration parameters shall be protected as in b) and c).*

i. *If the device is to operate in a channelized system, provisions shall be in place to ensure that only one channel of the redundant system can be subject to configuration changes at a time.*

An objective of EPRI's DEG is to provide a graded approach to engineering activities using applicability, configurability, and consequence of error as key attributes to achieve a level of risk-informed efficiency. EPRI's technology configurability screen is a proxy for the likelihood of error. As technology configurability increases, so does the likelihood for errors in requirements, design, implementation, operations, and maintenance. The DEG matches the risk as a function of two measures: (1) I&C system or component configurability, and (2) the consequences of an error.

Beyond configurability is programmability. Control devices may be considered to be nonprogrammable or programmable, although both types of devices are programmable to a degree. IEC 61508-4 [182] defines a programmable electronic (PE) device as a component based on computer technology which may be comprised of hardware, software, and of input and/or output units. This term covers microelectronic devices based on one or more central processing units (CPUs) together with associated memories, etc. Examples provided by the IEC for programmable electronic devices include:

- microprocessors,
- micro-controllers,
- programmable controllers,
- ASICs,
- PLCs, and
- other computer-based devices (for example smart sensors, transmitters, actuators).

All CPLDs allow simple design changes through reprogramming, and all commercial CPLD products are re-programmable although not necessarily by the user. With in-system programmable CPLDs, it is even possible to re-configure hardware—an example might be to change a protocol for a communications circuit—without powering down [184].

Devices can be designed with fixed programming language (FPL) software that cannot be modified by the end-user, or limited variability [programming] language (LVL) that is modified by the end user. The IEC 61508 compliance process does not extend to the application software that resides in LVL devices.

4.10.5 Consequence

Safety-related systems are designed to reduce the frequency or probability of the hazardous event and/or its consequences.

When determining the safety integrity requirements, it should be recognized that when making judgments on the severity of the consequence, only the incremental consequences should be considered. That is, one must determine the increase in the severity of the consequence if the function did not operate compared to that when it operates as intended. This can be done by first considering the consequences if the system fails to operate, and then considering what difference will be made if the mitigation function operates correctly. In considering the consequences that would occur if the system fails to operate, there will usually be a number of outcomes, all with different probabilities to be considered.

The principal consequence that physical barriers are designed to preclude is the uncontrolled release of radioactivity. Thus, for purposes of this review, the term *consequence* means *dose*.

The three physical barriers that provide defense-in-depth are:

1. Fuel and clad boundary
2. Reactor coolant system boundary
3. Containment boundary

Safety systems are required to mitigate the consequences of accident events. Maintaining the integrity of these three barriers can prevent or mitigate the consequences of an accident event.

In this review, the focus is not at the system level but at the device level (i.e., EDD) and its effect on the system. The objective is to assess the consequences resulting in the action or inaction of an EDD on the component and then to assess the consequences of the component's failure on the system. This is different than evaluating the use of the EDD to mitigate the consequences of an accident event. In this use, the definition of *safety-related* for the EDD based on the system may not correspond to the consequences of its failure.

There are three ways to assess if the failure has an increased consequence:

1. Its failure is modeled in the PRA or FMEA, or via similar tools and its consequences can be calculated.

2. The safety class of the SSC is known (although again, this is based on the system rather than device in a component).

3. Supporting issues, appropriately evaluated, may allow a risk-informed approach for the review and use of EDDs. The quality process (10 CFR 50, Appendix B), very high usage and operating experience outside the nuclear industry (millions of component types with EDDs), completeness of diagnostic coverage, etc. may inform a graded approach on the review and use of EDDs.

4.10.5.1 Device-level risk

The proposed use of a graded approach is based on the consequences from the failure of a single device. The proposed consequence-based approach at the device level is similar to the

NASA-GB-1740.13 grading based on the consequences to the system because the consequences of the device failure are evaluated according to their impact on the system.

At the device level, an EDD with its own independent sensor data and the OS software for the EDD operating on its own time and is thus also independent from other devices. Therefore, from the plant's point of reference, the failure of an EDD and its associated component is a single failure that the plant is designed to withstand, so long as it is not a failure of a new type or occurs as a CCF. Such a single failure (again at the device level), based on the plant's safety basis, may not have unacceptable consequences.

The use of a graded approach also can provide relief from the design standpoint by relaxing the IEEE SIL 4 requirements for safety SSCs. Based on the guidance in Annex B of IEEE Std. 1012-2004, a risk-based approach could categorize devices with announced failures or with diagnostics as IEEE SIL 1-2 in the opinion of the ORNL researchers. This same approach would categorize devices with unannounced failures anywhere from IEEE SIL 1–4. If there are other devices that monitor the same parameter of interest to the EDD, then the failure of an individual EDD becomes less important.

For EDDs in their current usage, independence is maintained. However, based on foreign reactor usage, IoT, and industry, failures that were previously postulated to be independent on a train or system level may no longer be independent, or the proposed activity introduces a cross-tie or credible CCF. This would change the consequence-based assessment results.

EPRI 3002012755 [184] confirms that faults and misbehaviors in digital I&C systems manifest themselves by the impact they have on controlled equipment. Risk models indicate that controlled equipment has varying degrees of importance relative to events like core damage or lost generation.

In some simple EDDs, the digital-based board does not have the characteristics associated with microprocessor-based systems such as modifiable code, branches or interrupts, decision-making capability, and therefore would not be susceptabilie to lockups, and have significantly less software CCF susceptibility. That is, these EDDs primarily operate as fixed logic devices. Thus, failures are primarily single random hardware failures. However, CCFs, including CCFs due to software, such as the software used to design the device, can still occur.

Although CCFs result from a single cause, they would not all necessarily manifest themselves in all channels simultaneously. For example, if an error occurred in the EDD due to a sensor, processor, or programming error, then the error could be common to all identical EDDs and could thus lead to a CCF. However, all of the EDDs may not be on the same time scale, sensor reading, etc. and therefore would not have the same critical factor leading to failure. Therefore, failures may occur at different times in the different EDDs or not at all.

In addition, the architecture of programmable systems allows them to carry out internal diagnostic testing functions during their on-line operation. If internal faults are revealed before they can result in a failure, then the probability of single localized fault or failure that can ultimately contribute to a CCF is significantly reduced.

The above classes of failure modes (see section 4.8) could also be useful in the review of CCF analyses. Suppose for example that the application software has an algorithmic or arithmetic flaw of some type and that this flaw could be triggered on all channels simultaneously. However, for timing-related failures such as crashes or hang ups, this is not necessarily the case. The

particular sequence of events that causes a hang up because of a priority inversion on one processor in a multi-channel system might not cause the same event to occur on another processor simply because of the difference in which events were processed. Even in the case of coding flaws that cause memory leaks leading to a processor crash, it is unlikely that memory leaks will cause all processors to fail at precisely the same time. However, non-concurrent triggers still need to be evaluated on a case-by-case basis and the applicant/licensee should technically justify why a non-concurrent trigger is not applicable for a given EDD design/configuration.

A four-category consequence-based classification structure was proposed by a research project sponsored by the DOE NEET program [118]. The proposed structure involves four classes:

- No impact
- Low impact
- High impact
- Critical impact

Like classification, consequences must be defined. NRC generally invokes three categories of consequences; two are in regulations (10 CFR 20 and 10 CFR 50.34), and one is in the safety goal policy that provides a quantitative health objective (QHO). The DOE consequence threshold is set for the public, co-located worker (CLW), and facility worker (FW) based on the total effective dose equivalent (TEDE) for the public, TEDE for CLW, and prompt death for FW.

Because EDDs may perform their functions differently than similar components without EDDs, their failure modes and the consequences of their failure may be different. These consequences can be at the individual device level or the CCF level.

Because each EDD is its own component, diagnostics on each individual component could indicate any detectable fault or failure of software or hardware almost immediately. Diagnostics could monitor hardware and software. A watchdog timer could indicate a software lockup. However, it is important to ensure that failure of an EDD cannot cause another failure or render a safety system unavailable or to spuriously actuate.

This is not to say there will not be a software-related error, which in itself is a potential CCF; it is just that the likelihood of a software CCF is lower because of the diagnostics, independent environments they are interacting with, and independent sensor readings.

The likelihood of a software fault is small, and a trigger is necessary to activate the fault to result in a failure. For an EDD, the likelihood of a software CCF will be largely dependent upon the type of component and how it is used. Independent relays on the same electrical line reading frequency, voltage, or current are likely to read the same values. Components such as valve controllers that read temperature, flow, etc., are more likely to have different input readings. Thus, having individual digital devices acting on independent localized sensor readings can minimize the concern of CCFs for some component types, but it does not eliminate the concern for all types. In addition, internal diagnostics and watchdog timers in the EDD can identify software hang-ups or failures, as well as hardware failures.

The independent application software and independent OS software (based on timing) reduces the CCF risk of multiple EDDs resulting from a concurrent software-related failure. However, external factors such as EMI, electrical, or operating environment factors are potential CCF contributors. For example, the voltage, current, or frequency inputs to an EDD would be the same

for any EDDs in the same division of power, regardless of distance. EMI would have a sphere of influence around the source and could cause the failure of any EDD within that sphere.

Control devices can be divided into active control devices or on-demand devices. The primary difference is that the failure of an active control device will be evident either through faulty output or diagnostics. The failure of an on-demand device is not known until the device is demanded for service unless the built-in testing/self-diagnostic features could indicate that there is a failure present in the device prior to demanding its service. This is important if other acceptance processes are deemed acceptable such as IEC SIL because they are tied to probability of failure or probability of failure on demand.

4.10.5.2 System-level risk

The understanding of risk and how it is managed is paramount to ensuring protection of computer systems.

The ASME/ANS PRA Standard [185] defines the term *risk* as the "probability and consequences of an event, as expressed by the 'risk triplet,' that is the answer to the following three questions: (a) What can go wrong? (b) How likely is it? (c) What are the consequences if it occurs?" (NRC website glossary [186]).

IEC 61226 [175] categorizes the functions for I&C systems based on the consequence of malfunction. IEC 61226 classifies the I&C functions important to safety into categories based on their contribution to the prevention and mitigation of PIE, and to (1) develop requirements consistent with the importance to safety for each category, and (2) to assign specification and design requirements to I&C systems and equipment which perform the classified functions.

Similar to the IEC requirements, IAEA SSG-30 [174] states that "The functions required for fulfilling the main safety functions in all plant states, including modes of normal operation, should be categorized on the basis of their safety significance." The severity of consequences is divided into three levels—high, medium and low—on the basis of the worst consequences that could arise if the function were not performed. The current version of IAEA SSG-30 [174] identifies the relationship between functions credited in the analysis of postulated initiating events and safety categories (Table 4-10).

Table 4-10 Relationship Between Functions and PIE [174]

Functions credited in the safety assessment	Severity of the consequences if the function is not performed		
	High	Medium	Low
Functions to reach the controlled state after AOO	Safety category 1	Safety category 2	Safety category 3
Functions to reach the controlled state after design-basis accident (DBA)	Safety category 1	Safety category 2	Safety category 3
Functions to reach and maintain a safe state (transfer from controlled state to safe state)	Safety category 2	Safety category 3	Safety category 3
Functions for the mitigation of consequences of a design extension criterion (DEC) (i.e., beyond design-basis accident [BDBA])	Safety category 2 or 3	Not categorized	Not categorized

Table 4-10 shows the method specified by SSG-30 for categorization of functions depending on the magnitude of PIE (AOO / DBA / DEC) in relation to the plant states to be reached (controlled state / safe state) and the severity of consequences (high / medium / low) if the related function is not performed. The use of severity levels supports the process for safety categorization of the required functions. To optimize the process, a more detailed level of severity (e.g. by probabilistic values) should be identified.

NASA ties the required software safety review effort to the hazard severity level. The level of effort is related to the criticality of the software and is divided into the following:

> Full software safety effort: Systems and subsystems with severe hazards which can escalate to major failures in a very short period of time require the greatest level of safety effort.
>
> Moderate software safety effort: Systems and subsystems which fall into this category typically have either a limited hazard potential or, if they control serious hazards, then the response time for initiating hazard controls to prevent failures is long enough to allow for notification of human operators and for them to respond to the hazardous situation.
>
> Minimum software safety effort: For systems in this category, either the inherent hazard potential of a system is very low or control of the hazard is accomplished by non-software means. Failures of these types of systems are primarily reliability concerns.

For NASA, the scope of the software development and software safety effort is dependent on risk. Similarly, the review and certification of EDDs is broadly tied to risk through the use of safety and nonsafety classifications. This does not address nonsafety related components whose failure can be risk significant.

Like IEEE 1012, NASA-GB-1740.13 provides guidance on the types of assurance activities which may be performed during the life-cycle phases of safety-critical software development for the different criticality levels of the software.

The U.S. Department of Defense (DoD) assesses and documents risk based on the severity category and probability level of the potential mishap(s) for each hazard across all system modes [83]. To determine the appropriate severity category as defined in Table 4-11 (MIL-STD-882E, Table I) for a given hazard at a given point in time, the potential for death or injury, environmental impact, or monetary loss is identified. A given hazard may have the potential to affect one or all of these three areas.

Table 4-11 Severity Categories [83]

Description	Severity category	Mishap result criteria
Catastrophic	1	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10 M.
Critical	2	Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1 M but less than $10 M.
Marginal	3	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100 K but less than $1 M.
Negligible	4	Could result in one or more of the following: injury or occupational illness not resulting in a lost workday, minimal environmental impact, or monetary loss less than $100 K.

To determine the appropriate probability level as defined in Table 4-12 (MIL-STD-882E, Table II) for a given hazard at a given point in time, the likelihood of occurrence of a mishap is assessed. Probability level F is used to document cases in which the hazard is no longer present. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap probability to level F.

Table 4-12 Probability Levels [83]

Description	Level	Specific individual item	Fleet or inventory
Frequent	A	Likely to occur often in the life of an item	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in the life of an item	Will occur several times
Remote	D	Unlikely, but possible to occur in the life of an item	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item. (The improbable level is generally considered to be less than one in a million)	Unlikely to occur, but possible
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated

DoD uses MIL-STD-882E to perform and document a subsystem hazard analysis (SSHA) to verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks, to identify previously unidentified hazards associated with the design of subsystems, and to recommend actions necessary to eliminate identified hazards or mitigate their associated risks. At a minimum, the analysis shall not only verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks, but it shall also identify previously unidentified hazards associated with the design of subsystems. Identifying previously unidentified hazards includes ensuring that the implementation of subsystem design requirements and mitigation measures has not introduced any new hazards. It also includes determining the modes of failure, including component failure modes and human errors, single point and common mode failures (i.e., CCFs), the effects when failures occur in subsystem components, and the effects resulting from functional relationships between components and equipment comprising each subsystem. This process should also include consideration of the potential contribution of subsystem hardware and software events, including those developed by other contractors/sources, COTS software tools, government-off-the-shelf (GOTS) software tools, and modified-off-the-shelf (MOTS) software tools, as well as nondevelopmental items (NDIs), government furnished equipment (GFE) hardware or software, faults, and occurrences such as improper timing.

The goal for the military is to always eliminate the hazard if possible. When a hazard cannot be eliminated, then the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence, which identifies alternative mitigation approaches and lists them in order of decreasing effectiveness [83].

a) *Eliminate hazards through design selection. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether.*

b) *Reduce risk through design alteration. If adopting an alternative design change or material to eliminate the hazard is not feasible, consider design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s).*

c) *Incorporate engineered features or devices. If mitigation of the risk through design alteration is not feasible, reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.*

d) *Provide warning devices. If engineered features and devices are not feasible or do not adequately lower the severity or probability of the mishap potential caused by the hazard, include detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.*

e) *Incorporate signage, procedures, training, and PPE. Where design alternatives, design changes, and engineered features and devices are not feasible and warning devices cannot adequately mitigate the severity or probability of the mishap potential caused by the hazard, incorporate signage, procedures, training, and PPE. Signage includes placards, labels, signs and other visual graphics. Procedures and training should include appropriate warnings and cautions. Procedures may prescribe the use of PPE. For hazards assigned Catastrophic or Critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.*

The software and review could be classified based on how an error affects the software and system containing the software (see classification).

Redundancy for the use of EDDs could be

1. redundant processors in the same EDD package,

2. two EDDs supporting the same component or function, or

3. the component itself could be redundant either in a bypass line or in a redundant train, each with its own EDD.

EDDs could have internal redundancy, and theoretically, these redundant internals could be diverse. The concern with this arrangement is that the processors could compete (e.g., Byzantine General problem), or they could create an electromagnetic field that could be a likely contributor to CCF for an EDD.

Other means for adding fault tolerance (i.e., redundancy) at the device level would be similar to what is done in other systems: like a valve or pump in a train, an additional bypass line or another component in series with EDDs, placing redundant operating systems in the EDD, or having redundant EDDs to the same component or function. Note that some industries correlate redundancy, or the number of independent protection layers (IPLs), to IEC SILs.

There are a number of recognized methods for determining IEC SILs, such as layer of protection analysis (LOPA), which uses frequency of the event as a basis, or safety layer matrix (SLM), which uses available information of IPLs as a basis for selection of the SIL for the safety instrumented system (SIS). The DOE standard uses a deterministic methodology (a modified SLM methodology), which is the approved method in ANSI/ISA 84.00.01-2004 [76]. The basis for this modified SLM methodology is that the safety classifications of SSCs are based on documented safety analyses (DSAs), so likelihoods and consequences do not have any further role in SIL determination.

As an example of correlating IPLs to IEC SILs, Appendix B of DOE-STD-1195 [187] correlates the number of IPLs to IEC SILs (Table 4-13) when determining the appropriate SIL for safety

significant (SS) safety instrumented function (SIFs) for DOE nonreactor nuclear facilities. The target SIL provides design input to a SS SIS that is credited with reducing the risk of a hazardous event by itself or in combination with other features to an acceptable level, as defined in the safety basis documentation.

Table 4-13 SIL Determination Based on IPLs [187]

Number of IPLs	IEC SIL
3	1
2	2
1	2

Table 4-13 shows that if only two IPLs are credited in the hazard analysis for a particular event, and one of them is an SS SIS, then the SS SIS target SIL is SIL-2. If three or more IPLs are credited for this scenario, then the SS SIS would have a target SIL of SIL-1.

If two SISs are credited with preventing or mitigating the same event, then one of the SS SISs may be assigned as SIL-1. The second SS SIS would have its SIL determined according to Table 4-13. Both SS SISs can be credited if they meet the following requirements [187]:

- *The IPL shall be designed to prevent an event or to mitigate the consequences of an event to a level that is supported by safety basis documents;*
- *The IPL safety function shall be identified and documented in the safety basis documents of a facility;*
- *The IPL shall be designed to perform its safety function during normal, abnormal, and design basis accident environmental conditions for which it is required to function; and*
- *The IPL shall be sufficiently independent so that the failure of one IPL, or of a component or subsystem of an IPL, does not adversely affect the probability of failure of another IPL credited for the same event.*

DOE applies the following rules to the selection of SILs:

- If some combination of components or systems is required to function together to complete the safety function, then they are considered as one IPL.
- If an instrumented system has been classified as SS, then regardless of the number of IPLs credited, it shall have a target SIL of no less than SIL-1.
- The SIL determination methodology cannot be used by itself to reduce the classification of a SS SIS to non-safety significant.

The greater the fault tolerance in the system, the lower the SIL requirement. Redundancy would increase fault tolerance, thereby lowering the IEC SIL for an individual component. This combination could be used to assign a higher IEC SIL to a system through a combination of individual devices, or it could be used to incorporate lower IEC SIL components into the system.

The SIL provides confidence in the design and development of the component. Thus, multiple SIL components can be used to increase the comparable SIL, or lower grade SIL components can be used to maintain the system SIL. Theoretically, 8 SIL-1 components in series could be comparable to a SIL-4 safety level. However, the quality and processing of the SIL-1 component is much lower than that for SIL-2 or SIL-3 components. It is important to remember that the lower IEC SIL-rated device does not have the same quality and pedigree as the higher rated device.

Some industries correlate redundancy, or the number of IPLs or LOPA to IEC SILs. Similarly, adding EDDs to the same component or function may not be a viable solution because of cost and the possibility of having competing EDDs.

The device manufacturer must provide data on the SIL rating with respect to systematic faults. This information is usually present in the conformity certificate of the individual devices [188]. This information can be supported by certificates produced by independent organizations such as the TÜV (German Technical Inspectorate) or companies specialized in testing.

Redundancy can be used to reduce the SIL of each component, or it can be used to increase the SIL if an extra or redundant sensor is implemented into the SFF [11]. Tables 4-14 and 4-15 show this concept. The IEC 61508 certificate provides an SFF. Table 4-14 and Table 4-15 provide the corresponding hardware fault tolerance (HFT) for that SFF. The HFT at the top of that column is used to determine the number of redundant devices required. For example, an SFF of 91% is in the range of the third row in the table. The HFT for this component for SIL-2 is 0, which means that a SIL-2 application does not require any redundant sensors. Similarly, the HFT for a SIL-3 application is 1, which means that SIL-3 requires one redundant sensor (i.e., two sensors total).

Table 4-14 Architectural Constraint Table for Type A Devices [75]

Safe failure fraction	Hardware fault tolerance		
	0 (1 sensor)	1 (2 sensors)	2 (3 sensors)
<60%	SIL-2	SIL-2	SIL-3
60% to <90%	SIL-2	SIL-3	SIL-4
90% to <99%	SIL-3	SIL-4	SIL-4
≥99%	SIL-3	SIL-4	SIL-4

11 *Safe failure fraction* (SFF) describes the proportion of failures that are either not hazardous or hazardous but revealed by some auto-test. For example, SFF = 1, the proportion of unrevealed hazardous failures. The IEC 61508 standard specifies the levels of SFF required to claim conformance to a given SIL target according to the amount of redundancy being employed. There are two tables of rules indicating whether an item of equipment or component is simple (with well-defined failure modes, known as *Type A*) or complex (such as a programable instrument, known as *Type B*).

Table 4-15 Architectural Constraint Table for Type B Devices [75]

Safe failure fraction	Hardware fault tolerance		
	0 (1 sensor)	1 (2 sensors)	2 (3 sensors)
<60%	Not Allowed	SIL-1	SIL-2
60% to <90%	SIL-1	SIL-2	SIL-3
90% to <99%	SIL-2	SIL-3	SIL-4
≥99%	SIL-3	SIL-4	SIL-4

The SFF can be related to the diagnostic coverage (DC) (see Subsection 4.10.8) and to detected and undetected failures, as shown below [189]:

$$SFF = \frac{\lambda S + \lambda DD}{\lambda S + \lambda D}$$

$$DC = \frac{\lambda DD}{\lambda DD + \lambda DU}$$

where SFF is the safe failure fraction; DC is the diagnostic coverage; λ_S is a safe failure; λ_{SD} is a safe, detectable failure; λ_{SU} is a safe, undetectable failure and λ_D is a dangerous failure; λ_{DD} is a dangerous, detectable failure; λ_{DU} is a dangerous, undetectable failure.

Safe failure may not affect the system's ability to perform its functions whereas dangerous failures prevent the system from working properly. Both safe and dangerous failures are divided into detectable and undetectable failures.

Redundancy is unlikely for EDDs. The safe failure fraction in IEC 61508-2 (Tables 4-14 and 4-15 above) would require SIL-3 for ≥99% safe failure fraction. The use of IPL and SFF does not appear to provide relief for risk-informing a safety related component from a SIL-3 to a SIL-2. That is, functionality and consequences of failure are not considered.

However, in the railroad industry, Mikro Elektronik (MEN) has taken redundancy to the board level [190]. Its A602/D602 – SIL 4 / DAL-A SBCs has triple redundancy on a single board. The board was developed according to RTCA DO-254, EN 50129, and IEC 61508, and it is certifiable up to SIL 4 (report from TÜV SÜD) and DAL-A. MEN's railway computer platform complies with the EN 50126 (Reliability, Availability, Maintainability, Safety [RAMS]), EN 50128 (software) and EN 50129 (hardware) railway development standards for functional safety, and the single components are certified up to SIL 4.

4.10.6 Dependability

Dependability is a measure of correctness. The amount of published research in the area of dependability of smart sensors is limited [121]. However, the overall objective of how to achieve dependability does apply to EDDs. RIS 2002-22, Supplement 1 recognizes that a key element in determining dependability is through having a quality design process. Other factors to consider in determining dependability include evaluating *relevant* operating experience and using suppliers that incorporate quality processes such as continual process improvement and incorporation of lessons learned and document how that information demonstrates adequate equipment dependability provide another measure of providing a dependable product.

Per the guidance In EPRI TR-106439 and IEEE Std. 7-4.3.2-2003, *dependability characteristics* address attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device. EPRI TR-106439 [54] indicates that dependability is a broad concept that incorporates various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. EPRI 3002002982 [53] (an update of EPRI NP-5652 [73]; EPRI TR-102260 [74]) measures dependability with respect to built-in quality (quality of design and manufacture), failure modes and failure management, problem reporting, and reliability. Others identify the following dependability characteristics: integrity, reliability, maintainability, and security [35].

In the process industry, the most important standards regarding the use of software are IEC 61508 and IEC 61511. The requirements for software in both of these standards also apply to the EDDs software and follow the standard and expected life cycle process, configuration management, specification methods, the use of formal methods, error detection and correction, etc.

IEC 62671 Clause 7 addresses dependability by providing evidence of correctness. This can be achieved through QA, design and development process, design configuration management, and design change control. Compensating measures to support dependability include operating experience and documentation improvement.

IAEA NE series document NP-T-3.27 [191] addresses the dependability of smart devices. Not surprisingly, vulnerabilities in a system could be detrimental to its dependability. Examples of vulnerabilities include uninitialized variables, divide by zero, timing issues, and tool chains.

Laprie [192] addresses the attributes, means, and impairments (threats) of dependability:

- *Attributes* of dependability include properties such as availability, reliability, safety, confidentiality, integrity, and maintainability.
- *Means* of achieving dependability include fault prevention, fault tolerance, fault removal, and fault forecasting.
- *Threats* to dependability are characterized as faults, errors and failures.

EPRI 1002833 [18], the final guideline on *Licensing Digital Upgrades* (NEI 01-01 / EPRI TR-102348, Revision 1), provides guidance on implementing and licensing digital upgrades and provides guidance on performing qualitative assessments of the dependability of digital I&C systems. RIS 2002-22 Supplement 1 [223] provides a pathway for implementation of EDDs as

digital modifications, and cites NEI 01-01/EPRI TR-102348, Revision 1, as industry guidance for evaluating EDDs in NPPs and fuel cycle facilities.

The qualitative assessment factors are (1) design attributes, (2) quality of the design process, and (3) operating experience.

Some important characteristics that should be evaluated for determining dependability include [18]:

- The development of QA processes implemented for both the digital platform and the plant-specific application software
- Demonstration of compliance with appropriate industry standards and regulatory guidelines for development, software safety analysis, V&V, and configuration control
- Hardware and software design features that contribute to high dependability such as built-in fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis

In addition, the maturity of the product and in-service experience with the platform and the plant system application should be considered. Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability. Credit should also be taken for using digital platforms that have previously been reviewed by the NRC as part of dedication for safety-related applications.

As shown, dependability is a broad, general term that covers many characteristics. The difficulty is in determining if and when a system is sufficiently dependable. When a system is sufficiently dependable, its likelihood of failure should also be sufficiently low.

For EDDs with non-control functionality, the failure of the EDD is an individual component failure; the lack of control functions eliminates most CCF concerns. All analog and digital components can be susceptible to other factors such as EMI. Even diverse, redundant, independent EDDs could be susceptible to EMI to different degrees. For example, an Allen Bradley relay generated an inductive kick [49]. External effects of EMI can be mitigated by proper shielding; however, internal effects such as the inductive kick in the Allen Bradley may be more difficult to identify and address.

4.10.7 Diversity and Defense-in-Depth

Diversity and defense-in-depth are design measures used to demonstrate that vulnerabilities to CCFs have been adequately addressed. NUREG/CR-7007 [193] identifies three diversity strategies that include the use of

1. fundamentally diverse technologies, such as analog and digital implementations,
2. distinctly different technologies, such as the distinct approaches represented by general-purpose microprocessors and field-programmable gate arrays, and
3. variations within a technology within the same technology, such as that provided by different microprocessors (e.g., Pentium and Power PC).

For digital systems, the defense-in-depth and diversity in the overall plant design are analyzed to assure that where there are vulnerabilities to software CCFs, the plant has adequate capability to cope with these vulnerabilities. Most defense-in-depth and diversity analyses generally focus on system-level consideration of CCF and does not explicitly address treatment of equipment/components. Characteristics that can serve to alleviate concerns about CCF vulnerability include 100% testability, which is applicable to EDDs, and sufficient internal diversity, which is not practicably applicable within a single EDD.

SRP BTP 7-19 provides measures guidance for evaluation of diversity and defense-In-depth in digital computer-based instrumentation and control systems. Diversity and defense-in-depth analysis methods are consequence based and system focused. This creates a challenge for assessing equipment with EDDs. Supplement 1 to RIS 2002 offers potential relief through qualitative assessment of the likelihood of failure—the failure likelihood is sufficiently low, or the failure likelihood is not sufficiently low.

For EDDs, diversity in the use of sensors has the advantage that it can reduce the probability that two or more sensors failing simultaneously, although this effect is limited by the fact that diverse sensors may still contain the same faults. A disadvantage of diversity can be the increased complexity of maintenance, which in itself can lead to a higher probability of failure of the sensors in EDDs. Whether the use of diversity is advisable depends on the design of the and the details of their application.

Meulen explores how diversity could improve the dependability of redundant EDD configurations. Diversity can reduce the main causes of CCF information overload, complexity, and HMI, or as Meulen calls it, *human computer interactions* (HCIs) [121]:

1. Diverse sensors might react differently to information overload conditions.

2. EDDs designed for the same use will likely have comparable design, algorithms, and complexity; however, diversity will reduce the possibility of CCF because of complexity.

3. Diverse EDDs will most probably have different user interfaces.

Diversity of individual EDDs (e.g., each component has two or more diverse sensors) is not currently a practical solution and could cause competing information to operators or control capabilities in addition to maintenance issues. At the device level, with each device having its own sensor and operating on its own time scale, the risk of a CCF is reduced unless caused by external events or a software-related CCF similar to the chart recorder at Sellafield. Diversity on the highly redundant subsystem level introduces maintenance problems, spare parts issues, etc. Thus, diversity at the device level may not be a practical solution. As noted by Meulen [121] and supported by this review that at this stage for EDDs, “it is not possible to give general recommendations for the use of diversity.”

Other diversity measures may not be at the component level but at the V&V level. This could include conventional testing with simulator testing and the use of independent testing facilities.

4.10.8 Self-Diagnostic Coverage

Self-diagnostics can be used to detect faults in a safety instrumented system, can be performed on a system or component level and can enforce a known state as the fault recovery action. Many EDDs and systems have embedded self-diagnostics that are executed continuously. These

self-diagnostics can be used to determine the health status of the EDD. Self-diagnostic coverage could never be 100%, similar to how testing could never provide 100% coverage, because of the unknown unknowns and not knowing all of the failure modes. Nevertheless, the greater the knowledge and history of a component could provide a means to provide a graded review by accepting the diagnostic coverage and the confidence in that coverage.

Self-diagnostics, also referred to as diagnostics, are used to ensure that failures are detected, and as a result, they will use the appropriate default states. Self-diagnostics for EDDs are dependent on knowing the failure modes of the device. This is one reason why knowing the failure modes of the EDDs are so important.

Diagnostic coverage is defined as the "fractional decrease in the probability of dangerous hardware failure resulting from the operation of the automatic diagnostic tests," and a *dangerous failure* is defined as a "failure which has the potential to put the safety-related system in a hazardous or fail-to-function state" [194].

The main purpose of self-diagnostics is to increase reliability, so introducing diagnostics has benefits, even if the volume of surveillance tests cannot be reduced. With periodic testing, some faults may remain undetected until the next periodic test, or in the worst case, until functional failure. The probability of these events can be greatly reduced using self-diagnostics. As there are potential unrevealed failures, some of which may be unsafe failures, there is still a need to perform functional testing to ensure that there are no unsafe failures remaining. The use of self-diagnostics may help to reduce the extent of the functional testing, but it will not eliminate the need for this testing.

Self-diagnostics can reduce the likelihood of a single failure, but it is practically impossible to detect all failure modes. This is why having as compete set of failure modes and an understanding of the EDD is so important. With self-diagnostics, EDDs installed in non-safety and safety applications should be able to reliably detect failures, provide early warning of potential failures, and notify plant operators to take appropriate action so that safety margins are maintained. Moreover, EDDs with self-diagnostics can provide added assurance that time-related degradation due to operation has not accumulated to a point that necessitates tests or preventive maintenance ahead of an extended surveillance interval.

Ideally, self-diagnostics would provide comprehensive coverage of the failure mechanisms. However, this is not always possible, and it can be difficult to conclusively prove that the self-diagnostics can provide 100% coverage of all faults. Hence, it is necessary to make a conservative assumption about the percentage of failures that the self-diagnostics will identify. IEC 61508-2 [75] provides levels of diagnostic coverage. This is usually a judgement based on the extent of the self-diagnostics and the complexity of the digital device, and it is often supported by a component-level FMEA or similar tool and operating history. By combining the percentage of failures detected by the self-diagnostics with the predicted failure rate, the unrevealed failure rate can be calculated.

EDDs that perform self-diagnostics and that can alert users to failures or degradations should lower the rate of failure identified as part of surveillance testing. In addition, the operability of the component (i.e., active or on-demand) will influence the likelihood of a failure being undetected.

SRP BTP 7-17 [178] defines a *self-test* as "a test or series of tests performed by a device upon itself. Self-tests include on- line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics." The BTP recognizes that, although there are positive

aspects of self-test features, these should not be compromised by the additional complexity that the self-test features may add to the safety system. Simply stated, the improved ability to detect failures provided by the self-test features should outweigh the increased probability of failure associated with the self-test feature.

IEEE Std. 7-4.3.2-2003, Clause 5.5.3, states that

> *Computer systems can experience partial failures that can degrade the capabilities of the computer system but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. … If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.*
>
> *…, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:*
>
> - *Memory functionality and integrity tests (e.g., PROM checksum and RAM tests)*
> - *Computer system instruction set (e.g., calculation tests)*
> - *Computer peripheral hardware tests (e.g., watchdog timers and keyboards)*
> - *Computer architecture support hardware (e.g., address lines and shared memory interfaces)*
> - *Communication link diagnostics (e.g., cyclic redundancy check [CRC] checks)*

Much of the operability of EDDs rely on self-diagnostics to identify failures and the failure of the device in a safe mode, etc. This makes the reliance on self-diagnostics one of the most important aspects to be evaluated. Self-diagnostics can add a lot of benefit by identifying errors and deviating performance; however, self-diagnostics add complexity, may have untested steps, and may falsely increase confidence in a device.

Excessive diagnostic coverage claims are routinely made on programmable electronic field devices [123]. Claims in excess of 90% are common, even with the restricted boundary and operating environment assumptions. A high diagnostic coverage translates directly into a high IEC SIL claim limit and low reported PFD. Such a claim makes sense when the credited diagnostic actually yields safer operation and is periodically proven to work—the same rule applied to any safety device. Self-diagnostics must be verifiable and auditable. Unfortunately, many manufacturer-supplied self-diagnostics are not capable of being tested in compliance with IEC 61511 Clause 11.3, “requirements for system behavior on detection of a fault,” and 16.3.1.1, which states that “periodic proof tests shall be conducted using a written procedure to reveal undetected faults that prevent the SIS from operating in accordance with the safety requirements specification.” Additionally, analysis reports do not include information on the product’s integrity if the self-diagnostics are not configured per the safety manual or if the product fails during operation.

The basis and accuracy of self-diagnostics, like operating experience, is difficult to assess with actual data because collecting data and information is very difficult because of intellectual property (IP) issues. Access to design documentation presents a challenge to nuclear operators/licensees. In practice, this access is hindered by several factors, such as:

- the need to protect the supplier's IP rights,
- the potential revelation of anomalies in the suppliers' processes and products,
- the time and effort required of the manufacturer,
- the argument that previous certification (if available) should suffice, and
- the relatively small size of the nuclear market, which typically means that nuclear licensees have limited influence on smart sensor/actuator suppliers.

Self-diagnostics and fault detection are features within a design that can provide immediate identification of a failure. Failures can be announced or unannounced. One of the worst scenarios for a safety system is that it is in a failed state and there is no indication of a problem until the system is called upon to perform its safety function.

A risk-informed approach would evaluate the likelihood and consequences of failures in application software, the OS, or self-diagnostics software. The very high usage and operating experience outside the nuclear industry (millions of component types) will reduce the likelihood of software failures, including software CCFs. Self-diagnostics help identify failures. If an OS or application software CCF occurs, then there should be feedback of the failure to the vendor, and the vendor could revise (fix) the software. No indication of this type of CCF was found, most likely because all EDDs are locally controlled and are on different time loops.

Self-diagnostics would monitor hardware and software. This is not to say there will not be a software-related error, which in itself is a potential CCF, it is just that the likelihood of a software CCF is low because of the self-diagnostics and independent sensor readings for the independent EDDs.

Diagnostic coverage (DC) represents the fraction of dangerous failures rates detected by self-diagnostics [195]. Overall, DC has four failure states in which the component fails in a safe/unsafe state and the failure is detected/undetected by self-diagnostics:

λ_{SD} - failed in a safe manner, and failure is detected by the diagnostics or plant trip

λ_{SU} - failed in a safe manner, but failure was undetected by the diagnostics but identified through proof tests

λ_{DD} - failed in a dangerous manner, and failure is detected by the diagnostics

λ_{DU} - failed in a dangerous manner, and failure is undetected by the diagnostics but identified through proof tests or incident

The total dangerous failure rate is then as follows:

λ_{DT} is the total dangerous failure rate ($\lambda_{DT} = \lambda_{DD} + \lambda_{DU}$)

For safety applications, the DC is typically applied to dangerous failures:

- the DC for the dangerous failures of a device is DC = $\lambda_{DD}/\lambda_{DT}$

- for a safety instructed subsystem with internal redundancy, DC is time dependent: $DC(t) = \lambda_{DD}(t)/\lambda_{DT}(t)$.

The specific percentages of DC are specified to make it likely that any dangerous failure is detected by the self-diagnostics, thereby reducing the probability of the existence of an undiscovered failure.

DC can be:

- low: 60–90 % coverage
- medium: 90–99 % coverage
- high: >99% coverage

The hardware assessment consists of a failure modes, effects and diagnostics analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined, and consequently, the SFF is calculated for the device. For full assessment purposes, all requirements of IEC 61508 must be considered.

Complete practical fault insertion tests can demonstrate that the DC corresponds to the assumed DC in the FMEDAs.

It has become easier to certify a high total failure device with a high DC claim to SIL 3 than it is to certify one with a low total failure rate but no diagnostics [123].

Often, self-diagnostics cannot be directly tested [198]. In fact, in most cases, there is no means to test the self-diagnostics to determine if they are working.

ISA-TR84.00.02-2015 [140] defines detected failures in relation to hardware and software failures, or faults, which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods. *Undetected failures* is the term used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, or operator intervention like physical inspection and manual tests). Such failures cannot be repaired until they have been revealed. The term *revealed* is used for failures or faults that become evident due to being overt or as a result of being detected.

DOE Order 420.1C requires safety-significant SSCs to be designed to reliably perform all of their safety functions. The order states that this can be achieved through a number of means, including use of redundant systems/components, increased testing frequency, high reliability components, and diagnostic coverage (e.g., on-line testing, monitoring of component and system performance, and monitoring of various failure modes) [199].

ISA 84.00.01-1 Clause 11.9, ISA-TR84.00.02, provides guidance on (a) assessing random and systematic failures, failure modes and failure rates; (b) understanding the impact of diagnostics and mechanical integrity activities on the SIL and reliability; (c) identifying sources of common cause, common mode, and systematic failures; and (d) using quantitative methodologies to verify the SIL and spurious trip rate.

The consequence of the failures can be classified as safe or dangerous based on the impact or effect that the failure has on the device's operation [140]. A safe failure is a failure which favors a

given safety action, whereas a dangerous failure is a failure which impedes or disables a given safety action; a failure is dangerous only with regard to a given SIF.

IEC-61508 [194] defines these as follows:

> *Dangerous Detected Failure - A detected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous detected failures do not include hardware failures and software faults identified during proof testing, represented by the plant's surveillance testing.*
>
> *Dangerous Undetected Failure - An undetected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous undetected failures do not include hardware failures and software faults identified during proof testing.*

Detected failures are in relation to hardware and software failures, or faults, which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods. The term *undetected* is used to describe failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed. The term *revealed* is used to describe failures or faults that become evident due to being overt or as a result of being detected.

In IEC 61511, the term *dangerous detected failures/faults* describes dangerous failures detected by diagnostic tests. The word *overt* is used to describe failures or faults which announce themselves when they occur (e.g., due to the change of state). Repair of such failures can begin as soon as they have occurred. When the detection is very fast as when discovered using diagnostic tests, detected failures or faults are considered *overt* failures or faults. When the detection is not as fast, as when discovered using proof tests, the detected failures or faults cannot be considered overt when addressing SILs. A dangerous, revealed failure can only be treated as a safe failure if effective automatic or manual compensating measures are taken early enough to ensure that safety integrity requirements are met for the safety function.

In IEC 61511, the term *dangerous undetected failures/faults* describes dangerous failures/faults that are not detected by diagnostic tests. However, *undetected failures* may also go undetected by operator intervention such as physical inspection and manual tests, or through normal operation.

Annex C of IEC 61508-6 gives an example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2. M. van der Meulen [121] notes that:

> *A problem that remains is the confidentiality of information; manufacturers do not want to disclose details on the design of their sensors. This explains why reports on failure rates and diagnostic coverage exist on sensors, but they do not provide detailed design information. These evaluations give the numerical data–most importantly, failure rates and fault coverage–required by IEC 61508 for the calculations as presented part 6.*
>
> *Sometimes independent assessors will perform fault insertion testing. In principle, this is comparable to performing a FMEDA. One advantage is that it concerns real insertion of faults, a disadvantage is that the number of faults that can be tested is lower and that some tests might be catastrophic. Also, the distribution of inserted faults might not reflect the distribution in actual use, and thus give a biased assessment of the fault behaviour that is to be expected. At the moment, the*

approach to smart sensor assessment, including fault insertion testing, is the subject of a new IEC standard [IEEE 60770, Part 3], now in its draft phase.

The absence of design details makes it hard for users to assess the validity of the results and their applicability to each user's setting. Independent assessors (like EXIDA.com, TÜV, TNO and Factory Mutual) are therefore essential.

4.10.8.1 Announced Failures

Failure modes described as *self-monitored* or *covered* are faults that can be detected and compensated for using the components downstream and operator actions. This does not indicate that non-covered faults are not detected; instead, faults that are not covered through self-monitoring will likely need to be subjected to periodic surveillance tests [200]. Fault coverage (i.e., self-monitored versus non-self-monitored failure modes) could play an important role in whether on-line monitoring (OLM) and self-diagnostic feature can be credited in a risk-informed assessment of the EDDs. This assumes that there is sufficient coverage of the self-diagnostics to detect the failure mechanisms and a determination of uncertainty, which is important if an EDD that provides self-diagnostics is relied upon to extend technical specification surveillance intervals.

A key consideration in the crediting of monitoring is the treatment of what are termed *dangerous detected* and *dangerous undetected failure fractions*, which are established to provide input to the reliability model for the device and the associated system [201].

IEC 61508-2 was developed to provide requirements for achieving safety integrity in the hardware of the safety-related systems, including sensors and final elements. Techniques and measures against both random and systematic hardware failures are required. These techniques and measures include an appropriate combination of fault avoidance and failure control measures. For cases in which manual action is needed for functional safety, requirements are given for the operator interface. IEC 61508-2 specifies diagnostic test techniques and measures based on software and hardware (for example diversity) to detect random hardware failures.

IEC 61508-3 was developed to provide requirements for achieving safety integrity for the software, including both embedded (including diagnostic fault detection services) and application software. IEC 61508-3 requires a combination of approaches to ensure fault avoidance (QA) and fault tolerance (software architecture). IEC 61508-3 requires the adoption of such software engineering principles as (1) top-down design, (2) modularity, (3) verification of each phase of the development lifecycle, (4) verified software modules and software module libraries, and (5) clear documentation to facilitate verification and validation. The different levels of software require different, appropriate levels of assurance that these and related principles have been correctly applied.

Diagnostics may not be capable of detecting systematic errors such as software bugs [202]. However, appropriate precautionary measures to detect possible systematic faults can be implemented.

The detection of a fault on a standby device can be identified by exercising most devices, such as an isolation valve. Faults on active devices are in most cases self-identified. Standby devices such as a relay or breaker may be more difficult to exercise. Condition monitoring by exercising a standby device allows process variables or inputs to be read.

Unavailability of protection includes problems that lead to a failure to operate one or more functions of the device [203]. The deficiency must be self-demonstrating and must be signaled by

the device via target or display messages, fail-safe relay, communication protocols, or other means so that manual or automatic corrective actions can be taken to rectify the problem. If the problem is not self-demonstrating, then it belongs to the category of *hidden failures* to operate.

The prevailing NRC policy and guidance specifically invokes a consequence-based assessment approach that is primarily applied at the safety system (or redundancy/subsystem) level for sense and command functions. These safety functions are generally characterized as *on-demand*, in which the safety action is commanded and executed when indication of an infrequent (transients) or rare (accidents) PIE is sensed. This conventional assessment approach has not been extensively applied at the component level; nor has it been applied to equipment for which the safety-related function is generally characterized as continuous, frequent, or predictable (such as for many sensing, actuation, and support service equipment) [204].

A *latent error* in software is an undetected defect in the software caused by incorrect requirements, software implementation error, untested hardware failures, etc., that only occurs when triggered. The probability of an undetected latent error increases with complexity. ORNL/TM-2010/32 [132] identifies new failure modes or the increased likelihood of failures for digital vs. analog systems such as relay race, the probability of an undetected latent error increasing with complexity, communications presenting unique problems for digital systems because of the ease of changing digital programs, and a quasi-trip state in which the output of the failed NAND (NOT AND) gate does not allow a true HI output.

Under IEC 61508 requirements, a product with a high total failure rate can achieve a high SIL claim limit as long as its failure is detected and annunciated. ISA-TR84.00.04-2015, Part 1 [205] notes safe failure fraction (SSF) is a ratio of failure rates. It is a measurement that does not depend on the total failure rate. A device can have a high total failure rate, and as long as the failures are safe or detected, the SFF is also high. This means that a device can have a high SFF and be highly unreliable. Process users need reliable equipment to ensure safe operation. Possessing a high SFF does not necessarily mean that the device performance is adequate for safe service. Summers [120] notes that “the SFF is not penalized by the choice to alarm rather than achieving the safe state. Therefore, the more failures that are detected, the higher the SFF becomes, regardless of the number of times, or the total amount of time, that the device is in the failed state, essentially dumping responsibility for process protection back on the operator.”

Fault detection simply informs the user that the device is no longer capable of operating as required; it does not achieve or maintain process safety.

The self-diagnostics can detect failures (if it has a complete set of failure modes); however, if the device cannot communicate to the safety/control system that a failure has been detected, or if the alarms on the device are not visual or audible to staff, then the benefits of self-diagnostics are minimal. This is true even if the diagnostic coverage is 100% and its fault detection capabilities (self-diagnostics) are working properly. In this case, the operators would not know that the device has failed, even though the device is capable of warning them. This means that the SIL requirement of the SIF / instrumented protective function (IPF) implementation is not satisfied. This is a tradeoff for the use of EDDs in an NPP, because the communication capabilities, especially 2-way communication, increases the complexity of the EDD and could then require a much more complicated system review. Although 2-way communication is not an issue with the current use of EDDs, it is expected to be an ET that will be implemented sooner rather than later.

Industry and the available standards seem to over rely on diagnostic coverage. Diagnostic coverage is very dependent on knowing and understanding the failure modes of the EDDs. A diagnostic cannot detect a failure mode that it is not testing for.

4.10.9 Testing

No matter the diagnostic, the only way to be certain that a device is working is to test it. However, the test itself must adequately simulate real demand conditions.

Testing is one method to provide assurance of the availability and effectiveness of functions important to safety and to confirm that these have not been degraded. For an EDD, testing is implemented to ensure that device functions as intended. In EDDs where failures would not be detected by testing or revealed by alarms or anomalous indications, the EDD should be analyzed for such undetected failures: the preferred course is to redesign the system or the test schemes to make the failures easily detectable. Interconnected systems should also be tested to confirm that all of their interfaces operate correctly.

Testing falls into two areas:

1. Initial – Design V&V

2. Periodic (surveillance)

Initial testing can be used to prove functionality and operability upon completion of design or at the end of the CGD process. Periodic testing of an installed device can never be comprehensive. In particular, it is difficult to ensure that the test (or the self-diagnostics) will find and announce internal failures is still working.

The surveillance test is manually initiated but may include automated or semi-automated test equipment to implement the test and/or record the test results. Proof testing is a synonym for surveillance testing used by IEC 61508. Surveillance testing should be designed to confirm that safety-critical functions of the EDD are being performed properly (e.g. overlapping end-to-end) with the test frequencies preferably being risk-based. Self-diagnostics are testing protocols embedded within the EDD and can be executed continuously. They try to perform most of the same functions but are implemented differently.

Failures of an EDD are grouped in IEC 61508 into two main categories—safe failures and dangerous failures. Safe failures are divided into detectable (λ_{SD}) and undetectable failures (λ_{SU}) that do not affect the system's ability to perform its functions. Dangerous failures prevent the system from working properly on demand. Dangerous failures are also divided into detectable and undetectable failures with failure rates λ_{DD} and λ_{DU}, respectively. Some dangerous detectable failures can be detected by online self-diagnostics, whereas dangerous undetectable failures remain unobserved until the surveillance test. Therefore, the purpose of surveillance testing is to detect unrevealed faults at the time of testing, while diagnostic coverage allows the detection and remediation of fail-to-danger fault conditions between surveillance tests [206].

Although NRC uses the term surveillance test rather than proof test, ANSI/ANS NQA-1 requires tests, including, as appropriate, prototype qualification tests, production tests, proof tests prior to installation, construction tests, preoperational tests, operational tests, and computer program tests such as software design verification, factory acceptance tests, site acceptance tests, and in-use tests to be controlled. Required tests shall be controlled under appropriate environmental

conditions using the tools and equipment necessary to conduct the test in a manner to fulfill test requirements and acceptance criteria. The tests performed shall obtain the necessary data with sufficient accuracy for evaluation and acceptance.

Proof testing is defined in IEC 61508 as a "Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an "as new" condition or as close as practical to this condition." A proof test is designed to reveal all the undetected/unrevealed failures that are not revealed until a demand is placed upon the component/system. A proof test is not a functional test or a diagnostic test. A functional test is conducted to ensure that a specified function is working correctly. However, a functional test in redundant channels does not necessarily reveal all faults. For example, a functional test in a subsystem with a 1oo2 voting configuration may detect a dangerous fault of the sensor architecture, but it may not highlight the number of faults. A proof test, however, would reveal all faults, even if there are multiple faults, as (typically) all elements are individually tested. In summary, the proof tests should demonstrate that all parts of the system are fully effective in delivering the relevant safety function, including any automatic or diagnostic test equipment that is used as part of testing either during service or during the proof test [207].

The perceived benefit for industry is that the application of diagnostic techniques for cases in which none previously existed has the potential to decrease the surveillance test frequency and the scale of routine testing. However, surveillance testing does not necessarily render components any more reliable. Surveillance test intervals are the same as surveillance test intervals and are set up to be consistent with the operating goals for the system.

Periodic surveillance tests, automated self-diagnostics, and surveillance tests can be performed to show the operability of the device and to meet availability targets. An EDD can be in a failed state while appearing to be running properly, and it is recognized that some failures will be undetected by self-diagnostics and surveillance tests. Surveillance testing should be designed to confirm that safety-critical functions are being performed properly (e.g., overlapping end-to-end). The test frequencies for surveillance tests should be risk informed.

ONR recognizes that surveillance testing can be more easily shown to be comprehensive for a simple system, so a failure that does occur can be expected not to persist beyond the next test interval [207]. For complex systems, especially software-based systems in which systematic faults are much more likely, the time-to-failure distribution is completely unknown, and periodic surveillance tests can only reveal random faults arising from non-software sources. In these cases, the level of uncertainty is higher, the safety margin must be larger, and the level of dependence placed on the system should therefore be correspondingly less.

Model-based testing methods may provide effective demonstration of whether devices are subject to certain types of CCF and may establish a cost-effective automated testing framework for industry stakeholders to qualify equipment with EDDs.

Automated testing programs are available for many OSs and languages. When a test will be run more than a few times, automated testing will usually save time and effort. Automated testing also removes the possibility of human error when a test procedure is followed. This removes the random error component, but it does leave open the possibility of systematic error, in which the automated test makes the same error every time it is run [208].

IEEE Std. 1012-2004 [209], endorsed by RG 1.168, Rev. 2 [319], and IEEE Std. 829-2008 [210], endorsed by RG 1.170, Rev. 1, as well as the newer, unendorsed revisions do not provide the

particulars of testing described herein, though perhaps they are implied. References to static analysis seem to refer to something more like code review and less like modern static analysis tools. Formal testing methods are mentioned briefly but not covered at length in later versions of IEEE Std. 1012, which is not endorsed by the NRC at this writing.

Testing may be performed by various organizations within the development effort. The IEEE Std. 1012 standard requires a minimum level of V&V testing, depending on the integrity level. Table 4-16 summarizes the minimum level of V&V testing required for the types of testing and integrity level. The term *perform* means that the V&V organization specifies and creates its testing products (i.e., test plan, test design, test cases, and test procedures) and either conducts the testing or analyzes the results when testing is conducted by another organization. The term *review* means that the V&V organization reviews the testing plans and analyzes the test results.

Table 4-16 Minimum Level for V&V Testing by Integrity Level (IEEE Std. 1012)

Software	V&V testing by IEEE integrity level			
	4	3	2	1
Software component testing V&V	Perform	Perform	Review	No action
Software integration testing V&V	Perform	Perform	Review	No action
Software qualification testing V&V	Perform	Perform	Review	No action
Software acceptance testing V&V	Perform	Perform	Review	No action

NUREG/CR-4621 [164] evaluates six different testing strategies:

1. Static source code analysis
2. Structural testing
3. Functional testing
4. Statistical testing
5. Stress testing
6. Regression testing

NUREG/CR-4621 states that “It is possible to use statistical testing for the goal of finding failures (random testing). Statistical testing does not rely on any knowledge of the internal composition of the software object and is the only way to provide assurance that a specified reliability level has been achieved. Statistical testing is a practical method in many cases when moderate-to-high reliability (in the range of 10-4 to 10-5 failures per demand) is required.”

NUREG/CR-7044 [211] compared three different quantitative software reliability methods (QSRMs): the software reliability growth method, the Bayesian belief network method, and the statistical testing method. The NUREG/CR concludes that the statistical testing method is the preferred approach for estimating demand-failure probabilities of safety-critical protection systems.

NUREG/CR-7234 [212] presents a successfully developed PRA-based statistical testing method, applied this method to a deployed digital system, and demonstrated its feasibility for digital I&C safety systems in NPPs.

All other factors being equal, techniques which are ranked as *highly recommended* (HR) in Table 4-17 (Table B.2 in IEC 61508-3) will be more effective in either preventing the introduction of systematic faults during software development or, in the case of the software architecture, more

effective in controlling residual faults in the software revealed during execution than techniques ranked as simply *recommended*.

Table 4-17 Dynamic Analysis and Testing by IEC SIL (IEC 61508-3 Table B.2)

	Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
1	Test case execution from boundary value analysis	R	HR	HR	HR
2	Test case execution from error guessing	R	R	R	R
3	Test case execution from error seeding	--	R	R	R
4	Test case execution from model-based test case generation	R	R	HR	HR
5	Performance modelling	R	R	R	HR
6	Equivalence classes an input partition testing	R	R	R	HR
7a	Structural test coverage (entry points) 100%	HR	HR	HR	HR
7b	Structural test coverage (statements) 100%	R	HR	HR	HR
7c	Structural test coverage (branches) 100%	R	R	HR	HR
7d	Structural test coverage (conditions, modified condition [MC] / decision coverage [DC]) 100%	R	R	R	HR

*R = Recommended, HR = highly recommended

IEC 61511 requires users to validate and periodically demonstrate via diagnostics, alarms, manual operation, and safety functionality that the equipment operates according to the safety requirements specification.

Formal verification techniques such as proof of correctness have traditionally only been applied to high criticality systems because of their high cost. However, in many systems, particularly embedded systems such as smart sensors, only a small fraction of the code performs high criticality functions. Sofia Guerra et al. propose a focused proof that makes formal proof applicable at all SILs [111]. A combination of techniques is used to achieve this, as detailed below.

- Use modern proof tools.

- Restrict attention to critical code. A code review identifies the regions of the code that are directly responsible for the process variable. This code may be as little as 20% of the codebase and is typically comparatively simple. The code typically implements simple scaling and other transformation functions on the process variable. This means it can be proved correct quite easily.

- Perform independence analysis. The code that deals with user interaction, housekeeping, etc., is audited to identify points of interaction with the critical code. A variety of techniques can be used to show independence.

As an alternative to the independence analysis, Guerra et al. propose testing to exercise the parts of the code not covered by the formal analysis. This may be incorporated into an existing test program already planned for the device.

For some parts of the code, the approach described above may not be sufficient. For example, in one example encountered by Guerra, a sequence of large switch statements was used to determine the device behavior in any of several dozen input sensor types which were selected using a configuration parameter. Determining the device's actual behavior proved difficult. By deriving a version of the program specialized to a single input sensor type (like a particular type of thermocouple, for example), the computation became very clear and was easy to analyze. This strategy can be effective when only a limited number of the device configuration options are intended to be used in actual nuclear applications.

In general, the surveillance test procedures do not address testing product diagnostics [123]. Conversely, the diagnostic coverage fraction of dangerous failure rates is not detected by diagnostics [195]. Diagnostic coverage does not include any faults detected by surveillance tests. Many devices have achieved a high IEC SIL via large diagnostic coverage factors, yet the means and procedures for testing the diagnostics are not provided or discussed in safety manuals.

An example of the need fortesting is the cause of a 9-hour outage of the AT&T long-distance telephone system which occurred on January 15, 1990. The outage can be traced back to a software upgrade that was loaded into all 114 of AT&T's Class 4 Electronic Switching System (4ESS) switches in the United States in mid-December 1989. The updated software changed the communication protocol between the 4ESS switches [213]. Prior to the software update, once the first switch began processing calls after the trunk interface reinitialization, it would send another message to all the switches that it was connected, informing them that it was accepting new calls again. After receiving this message, the other switches would confirm that the first switch was indeed working and then would accept call routing signals from that first switch. After the update, instead of the first switch messaging the other switches that it was working again with subsequent confirmation, the new software simply had the first switch start sending routing signals to the other switches. Consequently, each switch would interpret the signals as an indication that the first switch was again working because they were receiving its routing signals.

The software problem resulted from a programming error in which the programmer misunderstood the effect of the placement of a command within an if statement in the coding. This branch of the if statement was never exercised during testing; if it had been, then the fault would have been recognized. This example emphasizes the necessity of a comprehensive, complete testing plan for software routines and the necessity of redundancy in both hardware and software to overcome any overlooked or unforeseen software errors. It is likely that testing of the system would have identified the undetected error at the system level.

Most safety manuals provide limited scope surveillance tests with estimated test coverage; product operation is typically not fully proven by these partial tests. Because failure modes and distributions are not provided, it is not possible to determine if the claimed surveillance test coverage is reasonably conservative or to define which failures the suggested test covers or does not cover.

Some failures are undetected by both diagnostic tests and surveillance tests. Because surveillance tests are not a very fast means for detecting undetected failures, the detected failures or faults cannot be considered overt failures or faults [195].

The degree of design testability promotes proper operation and provides confidence that no new failure modes will be introduced. Testability is enhanced by the simplicity of the design. If the EDD performs simple logic functions that are easily and comprehensively tested, and the logic functions can be thoroughly tested in the validation test program, then relief may be possible for

the review and dedication of the EDD or may possibly accept the use of SIL-specified devices with the caveat that it is properly tested for the critical characteristics for its end use.

4.11 Emerging Technology (ET)

Advances in ET may occur at the I&C level or the EDD level. A more detailed of likely advances in ET related to EDDs is provided in Appendix D.

ET in I&C systems include:

- sensors and measurement systems,
- communications media and networking,
- microprocessors and other integrated circuits
- computational platforms,
- diagnostics and prognostics,
- Human-system interactions,
- human-system interactions,
- high-integrity software, and
- I&C architectures in new plants.

ET in the use of EDDs include:

- increased functionality,
- cyber security hardening,
- high temperature uses,
- Increased wireless technology,
- localized control,
- combined control (similar to system control),
- additive manufacturing of devices, and
- embedded sensors.

Advances in I&C systems, EDDs, advanced reactor uses, and manufacturing will all make an impact on industry and will eventually be included in I&C systems in NPPs.

ET can originate from advances in industry migrating into the nuclear arena, or it can be developed to meet the unique needs for new nuclear plant designs.

Embedded digital capabilities will enable new types of components that are not feasible without the high-speed data acquisition and processing capabilities supplied by the on-board electronics and advances in I&C systems and components. A review of ET that could affect the use of EDDs is provided in Appendix D with a summary provided below.

For nuclear applications, there are some emerging applications of autonomous control for creating reactor components that operate in extreme environments. For example, replacing mechanical bearings with magnetic bearings can allow a pump to be made from materials that can operate above 650 °C.

Current-generation NPPs use a centralized control architecture that requires exceptional operator knowledge of the power plant; the cost and difficulty to design the operational and safety systems are significant due to system complexity. Localized control through the use of EDDs could allow

designs to be simplified and could streamline operation of complex systems while improving modularity similar to object-oriented control architectures.

Future advanced reactors may employ EDDs more extensively than the existing fleet due to the opportunity to integrate instrumentation into the SSCs during fabrication and/or construction. Embedding digital devices into components is also more likely to be implemented in advanced reactors due to the advanced capabilities of digital technologies and the consequent potential for improving component performance and reliability.

A significant part of ET will be the advancement and use of wireless technologies. In the ET arena, increased communication capabilities and wireless technology would advance the capabilities of the EDD significantly beyond its analog counterparts. Cybersecurity and issues with electromagnetic propagation (electromagnetic and radio frequency interference, fading, interference abatement) are the major concerns with implementation of wireless technologies. The NRC and industry are already engaged in this issue with past NRC [214], ORNL [215, 216], EPRI [217], and DOE efforts [218, 219].

The NRC and ORNL have been researching wireless communications as an emerging technology in nuclear facilities. This research is aimed at developing a technical bases for regulatory guidance applicable to wireless technologies. A key element of regulatory guidance will be whether or not nuclear facilities can demonstrate that having data flowing in their wireless networks is secure. Wireless communications technology is not currently used in safety-related systems in nuclear facilities, but it is being used in non-safety–related and business applications, many of which have not been under the purview of NRC's regulatory authority.

A Canadian plant has used wireless sensors as part of online monitoring to enable condition-based monitoring. The EPRI research helped Ontario Power Generation deploy its first wireless sensor network.

DOE has been funding research efforts into the advancement of wireless technology such as thermoelectric generators for self-powered wireless sensor nodes. While the safety significance of the application of such technology is not indicated, the research evaluated the effects of gamma radiation on the materials for uses in harsh environments.

5 EXISTING PRACTICES

Domestic and international uses of EDDs and identification/analysis of those uses were reviewed to learn how other industries and countries regulate and implement the use of EDDs and to possibly leverage their experience into the framework of NRC regulations and guidance.

Many of the regulatory agencies outside of the nuclear industry are concerned with public safety of consumer products and do not provide requirements or guidance on how this is accomplished. Often the use of a standard comes down to insurability and possibly component quality and safety checks by Underwriters Laboratories or a similar organization. For example, Occupational Safety and Health Administration (OSHA) requires that information pertaining to the equipment in the process shall include design codes and standards employed. In some cases, insurance dictates which standards or processes are used.

5.1 Domestic Agencies

In addition to NRC guidance on the uses of EDDs, the domestic uses of EDDs were evaluated for how other regulators within the United States evaluate the use of EDDs (Table 5-1).

Table 5-1 Domestic Agencies Reviewed for Guidance on the Use of EDDs

Agency
NRC – Nuclear Regulatory Commission
DoD – Department of Defense
DOE – Department of Energy
FAA – Federal Aviation Administration
FDA – Food and Drug Administration
FERC – Federal Energy Regulatory Commission
FRA – Federal Railroad Administration
NASA – National Aeronautics and Space Administration
OSHA -- Occupational Safety and Health Administration

5.1.1 U.S. Nuclear Regulatory Commission (NRC)

This section provides a brief overview of the NRCs current practices regarding EDDs. As part of this project, ORNL performed a thorough review of NRC practices throughout the lifecycle of an EDD, from early development processes to installations and the activities of the vendor inspection branch. Based on this ORNL concluded that NRC guidance is sufficient to review and approve EDDs. However, for more complicated EDDs this would require performing the review outside of the CGD process using existing guidance for systems. The key factor in determining whether the review could occur under CGD is if appropriate critical characteristics can be identified and verified.

RIS 2016-05 defined and provides guidance on the use of EDDs. The RIS does not provide any new guidance or set any new expectations [220] but rather compiles the guidance in one place. The regulatory framework for EDDs is the same set of standards and guidance as that for the design and evaluation of SSCs containing in I&C systems. NRC also stressed CGD of EDDs, citing Appendix B, Part 21, and EPRI and IEEE standards.

The RIS raises awareness among licensees that EDDs, which may not have existed previously, may be introduced into a plant or facility via upgrades or replacement of equipment used in safety-related applications. The RIS encourages the identification, review, documentation, and control necessary to demonstrate quality and reliability. It also highlights possible vulnerability of equipment and systems to potential hazards like CCFs caused by software defects in EDDs. NEI noted that the RIS on EDDs brings attention to hidden digital components in devices that are often overlooked (e.g., breakers, inverters) [221].

Although the RIS does not address cyber security, 10 CFR 73.54 provides the regulations on cyber security [222].

For NPPs, basic components , which are safety related, must be designed and manufactured under a 10 CFR 50, Appendix B QA program or must have successfully undergone CGD, which must itself have been performed under an Appendix B QA program. The basis for a CGD program is found in 10 CFR 21.

In addition to using products designed and manufactured under a 10 CFR 50, Appendix B–compliant QA program, licensees may use appropriately dedicated CGIs for replacement parts.

Per 10 CFR 21, dedication may be performed by the manufacturer of the item, a third-party dedicating entity, or the licensee itself. In all cases, the dedication process must be conducted in accordance with the applicable provisions of 10 CFR Part 50, appendix B. This includes a requirement that for the persons or part of the organization performing quality assurance activities sufficient independence from those involved in design, organizational freedom, and direct access to an appropriate level of management must exist. The entity performing the dedication is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process. In addition to the dedicating entity having that responsibility, the licensee also has that responsibility whether they use a commercial grade dedicating entity or not.

EDDs should be identified early in the design to ensure procurement activities are sufficient to ensure quality and reliability, and the licensee's 10 CFR 50.59 process should identify the presence of an EDD:

- CGD should ensure that EDDs are identified.
- Inclusion of these devices is not always "advertised" by equipment vendors.
- Discovery of these low-level embedded devices is sometimes difficult, both for NRC and licensees and CGDs.

To increase regulatory clarity and reduce regulatory burden without impacting safety, guidance for EDDs, which already addresses the potential for CCFs due to software error, includes discussions on the following:

- Susceptibility to software CCF
- Use in redundant systems
- Different (independent) sensors
- Graded approach – active or standby component
- Guidance on CCFs at the system level rather than at the component level (addressed by BTP 7-19, Rev. 7)

The current regulatory infrastructure is sufficient for those vendors and suppliers that normally provide components to NPPs throughout the supply chain (Figure 5-1). The front end of the supply chain begins with the development of the component and the guidance and processes used to develop that component. NRC provides guidance on the development of hardware and software in I&C systems. The middle of the supply chain represents the component being sent from the vendor to a commercial grade dedicating entity, before it is sent to a plant for use. The back end represents when the component or device is delivered to the NPP.

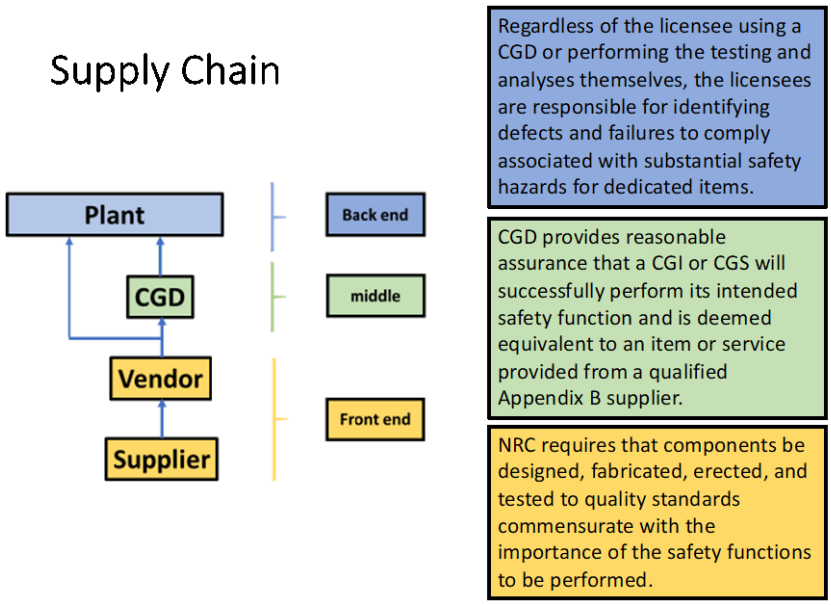


Figure 5-1 NPP Supply Chain

It is expected that EDDs will significantly increase at NPPs. This in turn means that many vendors not previously supplying components or digital field devices to NPPs will most likely begin to supply components or digital field devices to NPPs. Because the use of EDDs at NPPs will increase and more vendors of EDDs will not be from inside the nuclear industry (see the Subsection 4.11 and Appendix D on ET in EDDs), cyber security vulnerabilities and concerns will be greater. In addition, concerns with respect to software development and the use of software tools will also increase.

Licensees/applicants obtaining items and equipment from vendors that includes components with EDDs should:

- In early stages, fully understand challenges that EDDs may pose.

- Include requirements to identify the use of EDDs consistent with the safety significance of the equipment in specifications for vendors.

- Include in specifications requirements for the vendor to document the quality of items with EDDs in a manner sufficient to support CGI dedication consistent with the safety significance of the equipment.

Suppliers new to the nuclear industry should become familiar with NRC requirements and guidance while also enabling the CGD process to be effective and efficient.

For new and existing suppliers, the NRC vendor oversight workshops provide an open forum for exchanging information regarding the supply of components and materials to both new and operating NPPs. These workshops are attended by NRC, vendors, industry groups, commercial grade dedicating entity facilities, government regulatory agencies, and foreign and domestic utilities. These workshops have addressed EDDs and CGD facilities. The workshops allow staff and industry to learn how testing and inspections are performed on I&C systems or EDDs.

During the development of this report, RIS 2002-22, Supplement 1 [223] was issued, providing a pathway for implementation of EDDs as digital modifications, such as those in the example below, without prior NRC approval using properly documented qualitative assessments:

- replacement of analog relays (including timing relays) with digital relays

- replacement of analog controls for safety-related support systems such as chiller (heating, ventilation, and air conditioning) systems and lubricating oil coolers

- replacement of analog controls for emergency diesel generator supporting systems and auxiliary systems such as voltage regulation

- installation of circuit breakers that contain embedded digital devices

- replacement of analog recorders and indicators with digital recorders and indicators

- digital upgrades to non-safety related control systems

However, as the modification of the Allen-Bradley 700-RTC relay shows, even simple replacements of analog devices with digital devices or upgrades to digital devices can be vulnerable to a new or different failure mode that did not previously exist for that application.

Regulatory Issue Summary (RIS) 2002-22 [223] cites Nuclear Energy Institute (NEI) 01-01/EPRI TR-102348, Revision 1, [18] as industry guidance for evaluating EDDs in NPPs and fuel cycle facilities. The NRC is currently evaluating the sufficiency of NEI 96-07, Appendix D [224] to supersede the supplemental RIS 2002-22. [Regulatory Guide 1.187, Rev. 2, published in June 2020, endorses NEI 96-07, Appendix D, Revision 1, as a means for complying with the requirements of 10 CFR 50.59 when conducting digital I&C modifications, subject to clarifications.]

5.1.2 U.S. Department of Defense (DoD)

DoD standards (MIL-STD, MIL-SPEC, or (informally) MilSpecs) were searched for embedded digital control. No guidance was identified that specifically related to EDDs, but MIL-STD-882E [83] was identified as addressing the higher level topic of safety systems. Furthermore, the *Software Systems Safety Engineering Handbook* [84] was issued as guidance by the Joint Software System Safety Committee.

DoD's approach to safety systems is geared very much towards process and intentionally does not focus on requiring specific design criteria or specific design techniques. This makes sense when considering the wide range of systems that the DoD utilizes. Focusing on requiring specific design principles may unnecessarily limit certain design activities. Instead, the focus is on the identification of the risks involved in each specific project and defining the appropriate levels of rigor to be implemented to eliminate or reduce those risks appropriately. While this approach works for DoD, it does not work as case study for the nuclear industry, where the scope of applications is much more focused and the requirements are much more prescriptive.

The safety issues associated with COTS products in safety-significant systems increases with the complexity of the safety system. COTS vendors do not usually create the software to be used in safety-significant systems or safety-critical applications, so they may not ensure conformance to safety guidelines or testing. COTS products are often black box and lack complete or adequate documentation of the establishment of safety requirements for the system. Therefore, COTS products may require significant analysis and testing in the context of the safety criticality of the system. Treating COTS products as black boxes is also necessary when the vendor cannot or will not supply a copy of the source code to the user.

EDDs abound in military infrastructure and vehicles of all types. Questions arise regarding the terminology used to describe EDDs how they are considered, and how they are actually used. To an extent, DoD uses the term *smart devices* for EDDs, and they associate smart devices with IoT. DoD has apparently dropped the term *digital* and refers to these devices (and associated guidance) as *infrastructure devices* (e.g., smart electric meters) within industrial control systems [225].

The DoD uses different terminology for EDDs and also considers communication capabilities between those devices.

5.1.3 U.S. Department of Energy (DOE)

DOE uses hardware fault tolerance, IEC SILs, and individual protection layers to promote safety.

DOE facilities use safety instrumented systems for various control functions such as safety interlocks and process alarms. DOE Std. 1195 applies requirements of an industry standard, ANSI/ISA 84.00.01-2004, to support the design of reliable safety significant safety instrumented systems at defense nuclear facilities.

DOE O 420.1C identifies DOE-STD-1195-2011 [187] as providing an acceptable method for achieving high reliability of safety-significant[12] safety instrumented systems. DOE-STD-1195-2011 was developed based on ANSI/ISA 84.00.01-2004 and it identifies ANSI/ISA 84.00.01-2004 as an appropriate alternative means for meeting the reliability requirements. ANSI/ISA 84.00.01-

12 The U.S. DOE classification of *safety significant* (SS) is the second highest level. The highest U.S. DOE classification is *safety class* (SC). DOE-STD-1195 is only for SS equipment in nonreactor nuclear facilities.

2004 and its predecessor, ANSI/ISA 84.01-1996, have been a source of requirements for the design of safety instrumented systems at DOE nonreactor nuclear facilities for more than 20 years.

The U.S. national standard ANSI/ISA-84.00.01-2004 is the same as the international standard IEC 61511, with the addition of a grandfather clause to accommodate existing safety instrumented system installations. Because the majority of DOE safety controls are of the on-demand mode of operation, this is the focus of the DOE standard.

For devices designed per IEC 61508, IEC 61511 Section 11.4.5 states that "alternative fault tolerance requirements may be used provided an assessment is made in accordance to the requirements of IEC 61508 – 2, Tables 2 and 3." This statement directs the user to the IEC 61508 Hardware Fault Tolerance tables for Type A or Type B devices. These tables specify the number of required redundant sensors by the sensor SFF. A device designed per the IEC 61508 requirement of an SFF of >90%, Table 3 (Type B device) has the same fault tolerance requirements as stated in IEC 61511 Table 6, with a reduction of one fault tolerance. This is discussed further in the evaluation of DOE-STD-1195-2011.

The hardware fault tolerance minimum used by DOE is suited for systems dominated by single failures rather than highly redundant systems. To apply this at the component level for an EDD would require an added component in a bypass line; this would solve some problems associated with availability such as inadvertent closure of a valve, but it would create other problems such as added expense and maintenance costs.

5.1.3.1 NEET

DOE's NEET program conducts R&D and makes strategic investments in research capabilities to develop innovative and crosscutting nuclear energy technologies to resolve U.S. industry nuclear technology development issues. Included in this is research to develop an effective approach employing science-based methods to resolve concerns about CCF vulnerability that serve to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications. Other NEET activities are working on developing advanced capabilities for EDDs. As such, the NEET research can be useful for future applications of EDDs rather than current applications.

NEET workshop

In July 2016, NEET held a workshop to address EDD issues [226]. The workshop included over 50 participants with representatives from various government, industry organizations, utilities, universities, and vendors.

The information covered in the workshop presentations is summarized below by group.

EDDs: NRC Perspective

The key issues related to EDDs are sufficient procurement and control, identification of EDDs in procured equipment, adequate quality and reliability, and management of potential software-related CCFs. The NRC recognizes that existing regulations, policies, and acceptance criteria for software-related CCFs may require updating and clarification.

EDDs: Utility Perspective

Discovery of low-level EDDs can be challenging, and adequate consideration of EDDs resulting in potential software-related CCFs is not always straightforward to licensees. In addition, plants must be vigilant in procurement planning and supply chain control to ensure that safety-related equipment with EDDs complies with all regulatory guidance. The industry needs improved and revised NRC-endorsed guidance to facilitate the implementation of digital upgrades and modifications under 10 CFR 50.59. In addition, to help the industry resolve software related CCF issues, digital guidance that is relevant to the capabilities and function of the EDD is important.

Vendor Perspective: Qualification of EDDs

Because software failures are difficult to detect, classify, and correct, qualification of EDDs has been a significant hurdle to its implementation. The nuclear industry needs tools to measure software reliability and fault tolerance. The results of extensive testing on a digital system via the introduction of hardware and software faults proved that traditional statistical testing methods alone are not enough to detect all errors, and in some cases, a combination of testing methods is required to discover the error.

Classification Methods

Based on its findings from a survey of EDDs in general use and an evaluation of the functional impact of EDD failures, the NEET program proposed a four-category classification structure [118]:

- No impact: the digital functionality should have no connection to the analog electrical or mechanical elements of the instrument other than through nonintrusive or passive measurement.

- Low impact: the digital functionality may be connected to the analog electrical or mechanical elements of the instrument and may be able to influence the output or performance of the instrument's fundamental function.

- High impact: the digital functionality is likely to be integral to the analog electrical or mechanical elements of the instrument and is able to affect and potentially compromise the output or performance of the instrument's fundamental function.

- Critical impact: the digital functionality is highly integrated with or replaces the analog electrical or mechanical elements of the instrument and is essential to the execution, output and/or performance of the instrument's fundamental function.

The classification structure is based on the high-level characterization of potential impact of failure of an EDD on an instrument's performance of its fundamental function. The focus of the classification framework is to better characterize the role of the EDD in accomplishing the safety function of the instrument. Basically, the approach is to determine and/or verify the various responsibilities of EDDs so that the potential impact on the safety function(s) of from a software CCF can be classified to enable establishment of a graded scheme for determining the level of evidence and extent of analysis necessary to assess whether a device is subject to CCF.

The classification framework can provide a means of preprocessing information about equipment with an EDD to support a determination of when and how a diversity and defense-in-depth analysis should be performed. For example, if equipment with an EDD is classified as *no impact*,

then it is reasonable to conclude that there is no credible CCF vulnerability and a diversity and defense-in-depth analysis should not be necessary. For the other classes, further assessment is needed to address any prospective failure modes that could degrade the instrument's performance. Depending on the expected impact of a digital failure, it may be possible to identify defensive measures or testing to reasonably confirm that malperformance of the digital functionality provided by the EDD cannot inhibit or compromise the instrument's fundamental function nor induce spurious action.

The NEET project also devised an analysis approach that extends the customary diversity and defense-in-depth analysis to account for the significance and functional impact of potential failures of an EDD and to enable a graded analysis approach based on the classification of EDDs. The proposed assessment approach for systematically evaluating the potential impact of prospective CCF vulnerabilities for equipment with an EDD is described below.

- The presence of an EDD should be reviewed, and all specifications to vendors should include requirements that any EDD be identified and that sufficient documentation of the quality of any commercial equipment be provided (as noted in RIS 2016-05).

- If equipment with an EDD is identified, then the role of the digital device in the performance of any safety-related function either performed or supported by the equipment should be investigated. If it is determined that the EDD has an impact on the equipment performance or sufficient information on the role of the EDD is not available, then further assessment of the potential for CCF vulnerabilities should proceed.

- In accordance with the approach identified in BTP 7-19, the two criteria for which it is considered that the potential for CCF is resolved are (1) there is sufficient internal diversity incorporated in the equipment or the design of the EDD, and (2) the software or software-designed logic is sufficiently simple that it has been or can be fully tested. If either condition can be demonstrated, then no further analysis would be necessary. If the vendor does not provide or have such information available, then further assessment of the potential for CCF vulnerabilities should proceed.

- The performance characteristics of the equipment should be evaluated to determine the nature of its failure response. Given that this assessment applies to equipment rather than systems, a key question for the evaluation is whether the equipment performs a function for which failure is self-revealing (e.g., its failure readily observable). If there is not direct, short-term indication of failure (e.g., failure responses such as fail as is or incorrect but plausible), then the evaluation should consider whether failure of the equipment can be detected through available or additional monitoring.

At this stage, the assessment of equipment with an EDD transitions to the conventional diversity and defense-in-depth analysis.

If the considerations described in the assessment approach above do not fully resolve the potential impact of CCF in equipment with an EDD, then the equipment should be further treated as part of the conventional diversity and defense-in-depth analysis. The assessment of equipment with an EDD, including the results of a diversity and defense-in-depth analysis, are expected to demonstrate that there is sufficient defense-in-depth and diversity to cope with a postulated digital CCF of the EDDs in equipment of the reactor trip system (RTS) and ESFAS, including the credited control systems.

Model-Based Testing

Initial research was performed towards development of a cost-effective testing framework focused on automated generation of mutant operators, establishment of a hardware simulator platform, and adoption of a smart sensor prototype to serve as an initial basis for developing the testing framework [228]. The fundamental technical development underway for this research involves establishment of a cost-effective qualification framework that incorporates model-based testing to support determination of whether equipment with an EDD is vulnerable to CCF. The approach for model-based testing has been generated, a suitable prototype intelligent device has been devised and emulated in a simulation environment, and the basic elements of a testing environment have been developed. The model-based testing methodology under development is based on an extension of a software testing technique known as mutation testing. In this approach, tests are developed based on hypothesized software faults arising from requirements, design, and coding sources.

Other NEET Projects of Interest

Other reports/articles of interest developed under the NEET project include the following:

- Development and Demonstration of a Model Based Assessment Process for Qualification of Embedded Digital Devices in Nuclear Power Applications (Summary report of workshop) [229]
- Embedded Instrumentation & Control for Extreme Environments (ORNL) [230]
- Qualification of Embedded Digital Devices in Instrumentation (ORNL) [231]
- Verifiable Digital I&C and Embedded Digital Devices for Nuclear Power (EPRI) [232]

5.1.3.2 Light-Water Reactor Sustainability (LWRS) Program

DOE's Light-Water Reactor Sustainability (LWRS) program is addressing the qualification of digital devices for safety-related applications by [233]:

- Addressing CCFs associated with digital I&C systems
- Developing an architectural viewpoint that seeks to maximize reasoning, transparency and evidence while avoiding unnecessary complexity (SymPLe)
- Developing a verifiable architecture such as an accessible CPU-based architecture–but without its complexity where function blocks are the execution functions
- Limiting what a device can do by trading computational power for verifiability

Another LWRS program is the "Development of Model Based Assessment Process for Qualification of Embedded Digital Devices in NPP Applications" [234]. The model-based testing (MBT)includes:

- Development of an MBT method to demonstrate proof of operational reliability
- Testing of a digital device using both MBT and conventional black box approaches

- Seed a number of test cases involving mutants or defects ranging from software specification to code in the software
- Detection of faults arising from multiple phases of the software lifecycle
- Implementation and execution time comparable or less than black box testing
- Detection of faults that are not detectable through conventional testing

5.1.3.3 Operational Experience

DOE owns many nuclear reactors and nonreactor nuclear facilities. The use of EDDs is migrating to these facilities, and DOE is vigilant in ensuring the safety of workers and the public. Guidance and implementation of EDDs into several DOE-owned facilities is provided below. Because these are operating facilities the information can be useful in the use of EDDs at NPPs.

HFIR

The engineers at ORNL's HFIR are actively pursuing upgrades in systems that no longer have commercially available analog replacement parts. This is a good example for the use of EDDs in replacement components.

HFIR is developing methods of testing and calibrating devices that contain EDDs. The engineers at HFIR classify devices in two forms—configurable or modifiable—by asking whether changes can be made to the software on the EDD. If changes cannot be made to the software, then it is classified as *configurable*. This directly correlates with the IAEA NE series report where the COTS is configurable but not programmable [235]. Examples of types of firmware are listed as follows:

- Nonconfigurable, nonmodifiable firmware: oven controller, diesel generator, pump
- Configurable, nonmodifiable firmware: fire alarm control panel, flow meter, spectrometer
- Modifiable firmware: PLC, PAL, PLA, CPLD, FPGA

Its classification of the firmware determines the level of testing and calibration of the devices. To assess the risk of the firmware, the task group for HFIR suggests users to assess what can go wrong, to determine which risks are important to address, and to implement actions to address those risks. Once the embedded software is classified as configurable and not modifiable, a dedicated testbed and calibration system are developed following EPRI NP-5652 [73] guidelines.

The engineers at HFIR first develop a procedure to enable the following tests to be performed: simulation test, functionality test, and failure test. The simulation test determines if the code performs the correct calculations. This can be viewed as a black-box test of the software where several known inputs deliver known outputs and any unknown outputs are failures. To perform the functional test physical hardware connects to the testbed to verify that it will perform the operation designated to it, i.e. a motor runs at a set speed or a valve opens/closes. Finally, the failure test is used to inject faults into the system. For example, the failure test might open the breaker supplying power to the PLC to ensure that all outputs fail to their designated position.

HFIR staff are currently designing a servo-system upgrade that is built on a redundancy backup design where three systems are installed to perform a single function. Under this design, if two servo-systems went offline, then the function would still be performed by the third servo-system.

One of the three servo-systems was recently upgraded to include EDDs. Following the steps described above, the system was first identified as configurable but not modifiable. The upgrade was divided into three phases: the prototype, design, and implementation phases. In the first phase of the project, the prototype phase, the team completed a quick design, built a prototype, and had the customer (HFIR) evaluate it. If the customer evaluation had returned with required changes, then the process would have started over again. This iterative process continued until the customer (HFIR) approved the prototype, and then the project moved into the design phase. In the design phase, there was a formal gathering of requirements and SQA, including SQA umbrella documents for risk analysis, security plan, backup and recovery plan, change evaluation, tracking matrix, compliance matrix, procurement tracking, safety evaluation, training, and document control. The third phase included implementation, V&V, and installation and maintenance. Verification includes tests and inspections that ensure the software satisfies the system requirements. Validation includes tests and inspections that ensure the software performs correctly. V&V should be performed throughout the development and implementation of the software life cycle. HFIR was successful in the upgrade of the servo-systems in 2018.

LAWPS

DOE is planning to design and build a Low-Activity Waste Pretreatment System (LAWPS) at the Hanford Site Farms to remove radioactive cesium and solids from some Hanford tank waste. DOE's Defense Nuclear Facilities Safety Board (DNFSB) determined that the proposed alternative methodology for determining the SIL of the instrumented systems does not provide an equivalent level of safety as required by DOE Order 420.1C.

DOE Order 420.1C requires safety significant SSCs to be designed to reliably perform all of their safety functions. The order states that this can be achieved through a number of means, including use of redundant systems/components, increased testing frequency, high reliability components, and diagnostic coverage (e.g., on-line testing, monitoring of component and system performance, and monitoring of various failure modes). The order also requires that the facility design include multiple layers of protection (as part of the design defense-in-depth) to prevent or mitigate the unintended release of radioactive materials to the environment.

DOE Std. 1195 provides requirements and guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of safety instrumented systems with safety significant functions at DOE nonreactor nuclear facilities. This standard covers safety-significant safety instrumented systems that contain analog or digital components. Those analog or digital components include switches, electrical relays, analog transmitters, computer-based systems consisting of embedded hardware and software components (such as programmable logic controllers, smart transmitters with built-in logic functions, and microprocessor-based monitoring systems), and final control devices. *Embedded software* is defined as software that is part of the system supplied by the manufacturer and is not accessible for modification by the end user. Embedded software is also referred to as *firmware* or *system software*.

The methodology for LAWPS used the hazard frequency as the principal factor in determining SIL requirements; this is a key difference from the DOE Standard 1195 approach, which is based on the number of IPLs that exist to mitigate the hazard. The proposed methodology yields a SIL-1 design requirement for cases in which DOE Std. 1195 would require a SIL-2. DOE Std. 1195 allows a SIL-1 design if additional IPLs are identified and credited in the safety basis or if a failure of the safety instrumented system is not expected to result in a facility or collocated worker fatality. Specifically, the use of the alternative methodology may result in safety instrumented system designs that do not meet DOE's intent for reliable performance, as well as safety strategies that

do not incorporate defense-in-depth [199]. Although this does not pose safety consequences for LAWPS, a similar application of the alternate methodology to other facilities may yield unacceptable consequences.

MOX

The MOX facility is being built at SRS in South Carolina. The design, license, construction, and operation are contracted to Shaw AREVA MOX Services, LLC. The Mixed Oxide Fuel Fabrication Facility will be an NRC-licensed facility [236].

The MOX project is a National Nuclear Security Administration (NNSA) facility that will convert surplus plutonium (Pu) from nuclear weapons into MOX fuel for use in U.S. commercial NPPs. MOX currently has 35 vendors on its approved commercial grade vendors list. CGIs for the MOX project are purchased directly by MOX Services. For MOX, the audited and approved suppliers have Part 21 responsibility while the nuclear suppliers can be held accountable through contracts, legal actions, and market place. That is, DOE holds the licensee responsible while MOX Services performs the dedication.

10 CFR 70.22(f) requires licensees to have "a description of the quality assurance program to be applied to the design, fabrication, construction, testing and operation of the structures, systems, and components of the plant." The description of the QA program should include a discussion of how the criteria in Appendix B of part 50 of this chapter will be met. MOX Services has stated that the "Application for…plutonium processing and fuel fabrication facility shall contain…a description of the quality assurance program."

The CGD process for the MOX project is based on EPRI NP-5652. The project's commercial grade item evaluations (CGIEs) develop the technical, quality and documentation requirements for CGIs and establishes critical characteristics for acceptance (CCAs), acceptance criteria, and acceptance methods, and it develops input that controls and documents procurement and dedication activities.

Increased communication, monitoring, and controls are required of suppliers with CGD-related restrictions, depending upon the nature of the restriction.

Vendor-related lessons learned reported by MOX Services include:

- The results stemming from commercial grade surveys must be accounted for when developing the procurement strategy for how to establish a supply chain for a CGI.
- Know your supplier's (and your supplier's supplier) fabrication and CGD processes.
- Demand objective evidence that suppliers and sub-suppliers have appropriate QA programs and CGD processes in place to assure implementation is effective.
- Experience has shown that vendors of items relied on for safety (IROFSs) vary dramatically in their knowledge of standard sampling plans and implementation of sampling plan methodology.
- Vendor communication with project CGD group is very important.
    - Placing CGD personnel in the vendor shop can be very beneficial.

- Aggressive management and oversight of NQA-1 vendor CGD programs is prudent.
    - Review all vendor CGD plans and procedures initially.
    - Reviews may be lessened when confidence is gained with vendor programs.
- The CGD acceptance process needs to be closely coordinated with receipt inspection capabilities.

5.1.4 Federal Aviation Administration (FAA)

Aerospace Recommended Practice (ARP) 4754A [237] is a guideline from SAE International dealing with the development processes which support certification of Aircraft systems. It was recognized by the FAA in AC 20-174. The European Organisation for Civil Aviation Equipment (EUROCAE) jointly issues the document as ED–79. See EUROCAE for a description of ARP 4754 and its relationship to IEC SILs.

FAA tailored IEEE/EIA 12207.0 and IEEE/EIA 12207.2 for the procurement of computer software products and services to meet FAA-STD-026A [169]. Only the sections specifically identified in the FAA standard are requirements of the FAA.

The civil aviation industry software classification system is different from the aerospace industry because the classifications are based on effects of anomalous behavior of the software rather than software functionality. Unlike the aerospace industry, which assigns software tools with a classification separate from embedded system software, the civil aviation industry classifies software tools to the same level as the software developed with the tool.

RTCA DO-178B classifies software using the FAA's five failure levels to characterize the impact of that particular software's failure on an aircraft—ranging from Level A (catastrophic) to Level E (no effect on the operational capability of an aircraft)—and it prescribes more stringent criteria at higher levels. DO-178B tends to focus more on eliminating defects than on preventing their introduction in the first place.

The primary method of tool qualification in accordance with RTCA DO-330 [71] is development, verification, and validation in accordance with a high-quality, well-organized software tool development life cycle process. Alternative tool qualification methods include using service history, exhaustive input testing, formal methods, and use of dissimilar tools. Unlike most other industries that superficially address COTS software tools, RTCA DO-330 provides a comprehensive qualification process for COTS tools that divides qualification responsibilities between the COTS developer and tool user [67]. RTCA DO-330 contains a tool qualification liaison process that contains similar activities and tasks as DI&C-ISG-to facilitate the review and approval of software tools.

RTCA DO-330 also provides alternative tool qualification methods of using service history, exhaustive input testing, formal methods, and use of dissimilar tools. These alternative methods are analogous to CGI dedication when there is not much information available from the vendor beyond the published product description and a user's manual, and commercial-grade surveys (similar to EPRI Method 2) or source verifications (similar to EPRI Method 3) are impractical, leaving only special tests and inspections (similar to EPRI Method 1) and use of supplier and product performance history (similar to EPRI Method 4). The use of service history is analogous to EPRI Method 4.

The corresponding process of CGD for the aerospace industry is called *qualification*.

With respect to lessons to be learned from the FAA for EDDs in NPPs, the aerospace industry characterizes the software by failures on the system and uses five levels of failures whereas the civil aviation industry uses only one level of classification. Tool qualification is through V&V and testing, but also allows alternative methods such as service history and use of dissimilar tools.

5.1.5 Food and Drug Administration (FDA)

Among the products the Food and Drug Administration (FDA) regulates it's treatment of medical devices is most relevant to EDDs, as some of those devices would employ EDDs. No regulations or guidance could be found at the component level when searching the FDA databases on regulations and guidance.

The FDA's guidance document on software validation [238], like the IEC's, has a lengthy section on testing techniques and discusses how the level of criticality should determine the level of testing. It recognizes the limitations of testing and suggests the use of other verification techniques to overcome these limitations, but it does not specify what these might be.

Medical software is generally not subject to uniform standards and certification. However, the larger manufacturers often voluntarily adopt a standard such as the IEC 61508 or its U.S. equivalent, ISA S84.01. Thus, medical devices use IEC SILs to promote safety.

Medical devices have three software safety classifications—Medical Device Class A, B, and C. Under IEC 62304, , an industry-specific adaptation of IEC 61508, medical devices are classified based on the amount of injury that could be caused to a patient, an operator, or an onlooker.

Annex I of the Quality Risk Management guidance for industry [239] provides a general overview of and references for some of the primary tools that might be used in quality risk management by industry and regulators. The FDA recognizes IEC 60812 [240] as a method that can be used to prioritize risks and monitor the effectiveness of risk control activities. The FMEA can be applied to equipment and facilities and might be used to analyze a manufacturing operation and its effect on product or process. It identifies elements/operations within the system that render it vulnerable. The output/results of FMEA can be used as a basis for design or further analysis or to guide resource deployment.

Of interest to the use of EDDs in NPPs, the FDA allows OEMs to prioritize risks through the use of analyses such as FMEAs.

5.1.6 Federal Energy Regulatory Commission (FERC)

Federal Energy Regulatory Commission (FERC) is the federal agency that regulates the transmission and wholesale of electricity and natural gas in interstate commerce and regulates the transportation of oil by pipeline in interstate commerce. FERC also reviews proposals to build interstate natural gas pipelines, natural gas storage projects, and liquefied natural gas (LNG) terminals, in addition to licensing non-federal hydropower projects.

The major orders and regulations for FERC were searched for specific guidance at the device level [241], but no guidance was found. At a higher level, there are five core IEC smart grid families of standards that have been recommended by the National Institute of Standards and Technology (NIST) for U.S. smart grid projects (Table 5-2). They have also been referenced in

smart grid roadmaps published in several countries around the world, including the United States, Germany, and China.

Table 5-2 Smart Grid Standards Developed by IEC

Suite of standards - description	Number
Telecontrol equipment and systems *Facilitate exchanges of information between control centers*	IEC 60870 consists of 37 parts
Substation automation *Communication networks and systems in substation* Facilitates substation automation, communication and interoperability through a common data format	IEC 61850 consists of 18 parts
Common information model (CIM) / energy management *Energy management system application program interface (transmission)*	IEC 61970 consists of 11 parts
Common information model (CIM) / distribution management *Application integration at electric utilities - system interfaces for distribution management*	IEC 61968 consists of 7 parts
Security *Power systems management and associated information exchange - data and communications security addresses the cyber security of the communication protocols defined by the preceding IEC standards*	IEC 62351 consists of 7 parts

An intelligent electric grid allows the two-way flow of information and power. There are six key characteristics of an intelligent energy system:

1. Self-healing to rapidly detect, analyze, respond, and restore
2. Empowered and incorporating the consumer to incorporate consumer equipment and behavior in design and operation
3. Tolerant of attack to mitigate and be resilient to physical and cyber attacks
4. Providing necessary power with a power quality consistent with current consumer and industry needs
5. Accommodating a wide variety of supply and demand, including all distributed resources
6. Fully enabling maturing electricity markets to allow for and be supported by competitive markets

To fulfill a requirement of the Energy Policy Act of 2005 (EPAct 2005) section 1252(e)(3), FERC prepares and publishes an annual report that assesses electricity demand response resources, including those available from all consumer classes. The report evaluates the demand response and advanced metering. At the consumer end, advanced metering systems are comprised of state-of-the-art electronic/digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable

measurement of detailed, time-based information and frequent collection and transmittal of such information to various parties. *Advanced metering infrastructure* (AMI) typically refers to the full measurement and collection system that includes meters at the customer site (e.g., programmable communicating thermostats and smart appliances), communication networks between the customer and a service provider, such as an electric, gas, or water utility, and data reception and management systems that make the information available to the service provider.

AMI systems offered by different vendors will be required to conform to standards established by ANSI.

The standards used by FERC work together to achieve homogeneous communication systems to allow users to interoperate seamlessly. They also minimize the need for costly gateways and adapters that increase complexity and risk. They are already widely used in the industry by integrators (IEC Common Information Model [CIM]) and by manufacturers (IEC 61850). The requirements for a smart grid have to allow a more forgiving system expecting failures. Thus, the overall requirements specific to smart grids are not appropriate for use in EDDs in NPPs.

5.1.7 Federal Railroad Administration (FRA)

The purpose of the FRA is to promulgate and enforce rail safety regulations, administer railroad assistance programs, conduct research and development in support of improved railroad safety and national rail transportation policy.

49 CFR Chapter II, Appendix F to Part 229—Recommended Practices for Design and Safety Analysis cites the latest versions of EN 50128/IEC 62279 and EN 50129, and IEC 61508 as being recognized by FRA as providing appropriate risk analysis processes for incorporation into verification and validation standards. With the use of IEC/BS EN standards, the FRA uses IEC SILs to promote safety.

EN 50128 [171] and EN 50129 are two European standards (EN 5012x) that define safety-related software process standards, hardware, and approval processes for railway applications. EN 50128 provides process standards for software for railway control and protection systems. EN 50129 covers safety-related electronic systems for signaling.

Even though the safety lifecycles for the industry-specific standards, such as EN 50128[13] for a railway, inherit the definition of phases from the generic IEC standard of IEC 61508, the detailed phases of the safety lifecycles for the specific industries are different from IEC 61508.

BS EN 50128 [171] is a railway-specific implementation of IEC 61508 and specifies technical requirements for the development of safety-related software for railway control and protection systems. The railway industry uses a probabilistic risk-based process for safety-related system and software development.

The railway industry essentially uses the IEC SIL classification for components. As this is not currently used for EDDs in U.S. NPPs, its value is in the review and possible acceptance of IEC SILs.

13 The international version of EN 50128 is identical to IEC 62279.

5.1.8 National Aeronautics and Space Administration (NASA)

NASA does not provide specific verification, validation, or qualification requirements for most COTS, GOTS, or MOTS software tools and expects that automatically generated code be treated at the same level as hand-generated code [67].

Similar to other industries, NASA documents state that software tools used in developing software used in safety-critical systems should be identified, and the level of rigor associated with the verification, validation, and accreditation of software tools should be determined by the tool functions and the safety classification of the systems in which the software will be used [67].

NASA documents identify and recommend tools for many of the software engineering processes and define QA requirements for software tools. NASA uses a software classification system that is unique to the industry in that embedded system software, support software, software tools, and routine office software are all covered by the single classification system. NASA requires that an independent QA organization classify software tools to verify proper classification [67].

Using the consequence-based approach in NASA-GB-8719.13 [208] (NASA-GB-8719.13 supersedes NASA-GB-1740.13), the consequences of the device failure are evaluated, along with its impact on the system. This document cites both IEEE and IEC standards. The guidebook states that an operating system certified to the safety standard IEC 61508 is acceptable. The IEC standard IEC 61508 is currently under review by NASA to determine its acceptability as an international standard on software safety for products which contain programmable electronic systems (PESs) [70].

NASA-GB-8719.13 encourages the use of simulators or an in-circuit emulator (ICE) system for debugging in embedded systems because these tools allow the programmer or tester to find some subtle problems more easily. However, the guidebook does not discuss simulator or ICE system verification, validation, qualification, review, or approval practices.

NASA-STD-7009 [242] provides an approved set of requirements, recommendations, and criteria with which models and simulations (M&S) may be developed, accepted, and used in support of NASA activities.

With respect to complex electronics, NASA noted that [243]:

- Logic errors are still common in space-flight projects, with bad circuits making it into flight hardware

- A fundamental issue is how the complexity is managed to permit reliable design

NASA guidance cites both IEEE and IEC standards. Of interest to EDDs is that NASA classifies the software and the software tools by a single classification system. It is important to note that the consequences of the device failure are evaluated, along with its impact on the system.

5.1.9 Occupational Safety and Health Administration (OSHA)

Title 29 CFR 1910.119 [244] contains requirements for preventing or minimizing the consequences of catastrophic releases of toxic, reactive, flammable, or explosive chemicals. These releases may result in toxic, fire or explosion hazards. The process safety management (PSM) standard for OSHA, directs or implies the use of recognized and generally accepted good

engineering practice in the following sections, as opposed to prescriptively specifying particular equipment design and performance requirements. There are no specific requirements regarding consideration of the potential for CCF vulnerability or the use of diversity.

Many industries use IEC SILs to comply with OSHA regulations.

In a March 2000 letter to ISA, OSHA identified compliance with ANSI/ISA 84.00.01 (IEC 61511 Mod) as an acceptable implementation of recognized and generally accepted good engineering practice [245]. The use of ANSI/ISA 84.00.01 (IEC 61511 Mod) within industries that involve hazardous processes stems from the concept of recognized and generally accepted good engineering practice. ISA 84.00.01 is a performance-based standard.

The IEC 61508 standard then comes into play through ANSI/ISA 84.00.01 (IEC 61511 Mod), which identifies the methodology of acceptance of equipment for use in safety systems by certification to IEC 61508.

The industries this applies to are any that fall under the purview of OSHA which, at a minimum, would include the oil and gas processing industry and the chemical processing industry. IEC 61511 is also embraced in a similar manner internationally. For example, the United Kingdom implements a very similar approach through their Health and Safety Executive (HSE) Control of Major Accident Hazards (COMAH) regulations.

There are many equipment manufacturers who use IEC 61508 for their development and certification process. These manufacturers supply products to industries that have implemented IEC 61511 (or ANSI/ISA 84.00.01) in a manner that allows for simplified acceptance of equipment for use in safety applications.

These manufactures apply the development requirement of IEC 61508 to the hardware and software of their products, which encompasses EDDs. The IEC 61508 requirements drive built in quality into the products through implementation of systematic integrity, low probability of failure, detection of failures, and management of failures (fail-to-safe state).

OSHA's Nationally Recognized Testing Laboratory (NRTL) Program recognizes private sector organizations to perform certification for certain products to ensure that they meet the requirements of both the construction and general industry OSHA electrical standards. Each NRTL has a scope of test standards that they are recognized for, and each NRTL uses its own unique registered certification mark(s) to designate product conformance to the applicable product safety test standards.

OSHA created the NRTL program to ensure that certain types of equipment be tested and certified for their safe use in the workplace. OSHA's NRTL regulations were established in 1988. The first organization became recognized as a NRTL in 1989.

A Nationally Recognized Testing Laboratory (NRTL) is a private-sector organization that OSHA has recognized as meeting the legal requirements in 29 CFR 1910.7 to perform testing and certification of products using consensus-based test standards. These requirements are [246]:

- The capability to test and evaluate equipment for conformance with appropriate test standards;

- Adequate controls for the identification of certified products, conducting follow-up inspections of actual production;

- Complete independence from users (i.e., employers subject to the tested equipment requirements) and from any manufacturers or vendors of the certified products; and

- Effective procedures for producing its findings and for handling complaints and disputes

An organization must have the necessary capability both as a product safety testing laboratory and as a product certification body to receive OSHA recognition as an NRTL.

OSHA's standards contain requirements for NRTL product testing and certification for 39 product types. For example, in 29 CFR 1910.303, OSHA requires NRTL approval for many kinds of electrical equipment when they are used in the workplace. OSHA's website contains a listing of the type of products requiring NRTL approval [247].

After certifying a product, the NRTL authorizes the manufacturer to apply a registered certification mark to the product. If the certification is done under the NRTL program, this mark signifies that the NRTL tested and certified the product, and that the product complies with the requirements of one or more appropriate product safety test standards.

The CE mark is unrelated to the requirements for product safety in the United States. It is a generic mark used in the European Union (EU) to indicate that a manufacturer has declared that the product meets regulatory requirements in the EU that may or may not include product safety. In the United States, under OSHA's NRTL requirements, the product must have the specific mark of one of the NRTLs recognized to test and certify this type of product.

Of specific interest to EDDs in NPPs is that OSHA directs or implies the use of recognized and generally accepted good engineering practice. For this, many industries use IEC SILs for both hardware and software.

5.2 International Nuclear Regulating Agencies

International regulatory practices with EDDs were reviewed to learn how others regulate and implement EDDs and to possibly leverage their experience into the framework of NRC regulations and guidance (Table 5-3). Inconsistency and ambiguity within and between standards for the classification of safety systems and functions necessitates a more comprehensive review of how guidance and standards are implemented for approving the use of EDDs in U.S. NPPs. However, the classifications for safety in many countries are divided more finely than in the United States and could provide insights on dividing the broad safety classification into more levels while maintaining safety.

Table 5-3 Countries Reviewed for Regulations and Guidance on the Use of EDDs

Country
Canada
France
Germany
India
Japan
Korea
Pakistan
Romania
Russia
UK

All countries review the information provided by the applicant for compliance with the applicable regulatory requirements [248]. In addition to document reviews, some countries use onsite audits and inspections to confirm that the regulatory requirements have been met. For example, in India, Korea, and the United States, audits or inspections are used in the review of various I&C-related technical topics. In India, an audit of system development life cycle documents (including V&V and QA documents) is performed as part of the review of software reliability. In the United States, inspections are used to evaluate the implementation of a licensee's cybersecurity program.

In all cases, the technical basis for regulatory authorization is provided by a combination of country-specific regulations and regulatory guidance. In addition to the regulations and guidance documents, most countries make use of either national or international consensus standards related to I&C.

Korea, Pakistan, and the United States refer to the IEEE standards as part of the technical basis for regulatory authorization.

India and Russia identified the use of IAEA standards as the basis related to their review of I&C. In Russia, IAEA Safety guide No. NS-G-1.3 and IAEA Draft Safety Guide DS-431 provide part of the technical basis for granting regulatory authorization in several technical topics. Also, in India, IAEA standards or other acceptable codes are used to review specific areas where Atomic Energy Regulatory Board (AERB) documents have not been prepared.

Canada, France, Germany, and the UK identify IEC standards as part of the technical basis for granting regulatory authorization. The most commonly identified IEC standards were IEC 60880, IEC 61513, and IEC 62138. The use of IEC 61511/IEC 61508 would leverage the economies of scale achieved in other industries to those of the nuclear industry. Other certifications are CSA for Canada, ATEX for Europe, and KGS for Korea. For example, CSA 61511[14] is the Canadian version of IEC 61511.

14 IEC standards adopted by Canada as national standards are published as CSA standards by the CSA Group (formerly the Canadian Standards Association). ANSI does this for the United States and the British Standards Institute (BSI) for the United Kingdom. ANSI tends to keep the originating standards body ID in the standard title as in ANSI/ANS or ANSI/IEEE, when it adopts something as a national standard.

Canada, France, and the UK also have their own regulations and guidance in addition to standards developed by IEEE, IAEA, and IEC.

Those countries with multiple safety classifications incorporate function or consequence into the safety classification. For example, in evaluating a component or system, the UK first identifies the safety function of the device and then evaluates how the SSCs deliver those safety functions and their significance to safety. Similarly, Germany considers the safety functions in its classification of safety SSCs. Since 2016, France now considers devices of limited functionality. India, with its three safety categories, considers the consequences of the failure rather than the function.

The nature of the UK regulatory regime is not prescriptive; however, the UK does support international standards that may be prescriptive. Conversely, the NRC uses many standards that may be considered to be overly prescriptive but by considering standards that are performance based may provide some grading of design attributes.

The Canadian regulatory structure does not include a requirement for vendors to produce equipment in compliance with a nuclear-specific QA program. However, CSA N286 is included in plant licenses and there are no QA requirements regulated down to suppliers. The scope of N286 is only the plant. CSA N299 (formerly Z299) does exist for suppliers but it is only guidance. These standards are interesting, in that they are implemented using a graded approach. There are different versions of this standard for each of the four safety categories of equipment. Each version is designated with a .1, .2, .3, or .4 suffix corresponding to the applicable safety category. There is also no defect reporting regulation for suppliers, rather the licensees have obligations to report defects after an event of consequence occurs. No regulation exists that requires licensee or suppliers to report component defects when no consequential event has occurred. Note that in Canada the CGIs still undergo a certification process similar to the CGD. Interesting is that CSA N290.14-15 provides guidance for determining an item's complexity based on lines of code, number of internal modules, and an interface complexity index.

The most commonly used route for qualification of a digital system in Germany is to build on an existing commercial certificate of compliance to an industrial standard such as IEC 61508 and have the device certified by an assessor such as TÜV. When an already-qualified device is to be re-used in another application, the qualification process can claim credit for an existing pre-qualification. Generic qualification is also possible, which can be used as a basis for an application-specific qualification

In India, before a smart device can be used, a review is performed to ensure that device is qualified for use in an NPP. This review requires that the device meets functional and performance requirements that are evaluated with testing (e.g., accuracy, EMI/EMC, seismic, etc.), has extensive operating experience, both inside and outside of the nuclear industry for the same model and software version of the device, has a well-established design process that was used throughout the lifecycle, the HRA and FMEA have been performed,failure modes are predictable, and the manufacturing process was dependable, including ISO-9001 certification, version control, history, and problem reporting. If the device has networking features, then the devices are evaluated for cyber security concerns. The evaluation, which uses a graded approach, evaluates software to IEC 60800, IEEE Std. 603, IEEE Std. 7-4.3.2, and India's AERB SG-D-25. AERB SG-D-25 refers to IEC standards. Additional (and practical) requirements for software in smart devices include the simplicity of the software without additional features, secondary function, and no unused code or features.

The common position paper, “Licensing of Safety Critical Software for Nuclear Reactors [249],”is the result of the work of a group of regulator and safety authorities’ experts. The 2007 version was completed at the invitation of the Western European Nuclear Regulators’ Association (WENRA). The focus of this work was to compare the respective licensing approaches, to identify where a consensus already exists, and to see how greater consistency and more mutual acceptance could be introduced into the current practices. These common positions and recommended practices take into account not only the positions of the participating regulators, but have also been reviewed against the international guidance, the technical expertise, and the evolving recommendations issued by the IAEA, the IEC and the IEEE organisations. Within this comparison, the term *software* also includes firmware and microcode.

A review of the standards and the guidelines are provided in the next subsection (Subsection 6).

5.2.1 Canada

The regulator in Canada is the Canadian Nuclear Safety Commission (CNSC). The CNSC is the issuer of power reactor operating licenses (PROLs) for all of Canada’s nuclear power generating plants. As part of the licensing process, the CNSC ensures that safety systems are in compliance with the relevant standards.

In Canada, certain types of EDDs are referred to by the related term smart devices. With respect to regulatory guidance, the CNSC is currently in a transition period regarding the standard applicable to digital devices. The previous licensing basis referenced CSA N290.14-07 [250], but now all new licenses and re-licensing activities are referencing the second edition of this standard, CSA N290.14-15 [94] and expanding the scope to include hardware and a broader range of software. As of November 2019, Pickering Nuclear Generating Station has been re-licensed using this second edition.

It is important to understand that the Canadian regulatory structure does not include a requirement for vendors to produce equipment in compliance with a nuclear-specific QA program, such as U.S. Title 10 CFR 50 App B or ASME NQA-1, and they also do not include a U.S. Title 10 CFR 21 requirement with which all vendors must agree to comply. In Canada, the justification process is specifically an activity for design suitability or qualification, as opposed to having a separate commercial grade dedication process.

To address QA requirements, CSA N286 is included in plant licenses. However, there are no QA requirements regulated down to suppliers. The scope of N286 is only the plant. CSA N299 (formerly Z299) “Quality assurance program requirements for the supply of items and services for nuclear power plants” does exist for suppliers but it is only guidance. These standards are interesting, in that they are implemented using a graded approach. There are different versions of this standard for each of the four safety categories of equipment. Each version is designated with a .1, .2, .3, or .4 suffix corresponding to the applicable safety category.

There is also no defect reporting regulation for suppliers. The licensees have obligations to report defects after an event of consequence occurs in accordance with REGDOC 3.1.1 “Reporting Requirements for Nuclear Power Plants,” but this does not apply to suppliers. No regulation exists that requires licensee or suppliers to report component defects when no consequential event has occurred.

The system/component classification in Canada includes four levels [94]:

- Category 1: high safety significance
- Category 2: moderate safety significance
- Category 3: low safety significance
- Category 4: no safety significance

Category 1 aligns well with the NRC's safety-related classification. However, the other classification categories align with the IEC SILs.

Table 5-4 Safety Categories in Canada and Alignment with Standards [94]

Standard	Category 1 (high safety significance)	Category 2 (moderate safety significance)	Category 3 (low safety significance)	Category 4 (no safety significance)
IEC 61508-5	SIL 4 and 3	SIL 2	SIL 1	Non-safety–related
IEC 61513, system classes	Class 1	Class 2	Class 3	Non-safety–related
IEC 61226 and IEC 61513, functions	Category A	Category B	Category C	Non-safety–related
COG-95-264-1	Category I	Category II	Category III	Category IV (also known as *commercial grade*)

In Canada, software and digital devices are organized into four types—Real Time Process Computing (RTPC), Scientific Engineering and Safety Analysis (SESA), Managed Systems, and Business IT. Digital devices used in safety applications in the nuclear plant fit into the RTPC type. Within RTPC there are four categories; I, II, III, and IV.

The first step of the qualification activity is to determine the appropriate category for digital item. This determination sets the requirements to be used for determining if the digital item is suitable for the intended safety application. It is a standardized method for implementing a graded approach.

In addition to all these methods, the Canadian qualification process also includes environmental, seismic, and electromagnetic compatibility assessments that are similar to what is done for U.S. nuclear plants.

AECL CE-1001-STD [251] specifies requirements and a minimum set of software engineering processes for safety-critical software development for CANDU® nuclear generating stations. Software tool requirements are limited to high-level requirements to identify necessary resources for tool development, identify and document tools in plans and procedures, identify personnel required to maintain and manage the tools, and identify the qualification requirements for software tools. AECL CE-1001-STD does not distinguish between different types of software tools, does not use software tool categories or classifications, and does not contain any specific software tool qualification requirements tailored to the type of tool.

Overall, the Canadian approach to justifying the use of digital devices is an interesting case study because it correlates nuclear safety classifications directly to IEC 61508 SILs, it provides a path for accepting items based on SIL certifications issued by an independent third party, it does not include 10 CFR 50 App B or 10 CFR 21 requirements, and it also includes a standardized approach to ranking the complexity of a digital item. These aspects make the Canadian regulatory structure important to maintain awareness of since many of these aspects provide valuable approaches for dealing with issues currently being dealt with in the U.S. nuclear industry.

Numerous countries are evaluating the use of IEC SILs for CGIs. Note however, that in Canada the CGIs still undergo a certification process similar to the CGD.

5.2.2 France

The French Atomic Energy Commission, created in 1945, was later renamed the French Alternative Energies and Atomic Energy Commission (CEA) in 2010. CEA (French: Commissariat à l'énergie atomique et aux énergies alternatives), is a French public government-funded research organization in the areas of energy, defense and security, information technologies and health technologies. All commercial nuclear reactors in France have been and continue to be built and operated by the licensee Électricité de France (EDF). In 2006, the Autorité de sûreté nucléaire (ASN) was created as the independent French nuclear safety regulator, replacing the General Direction for Nuclear Safety and Radioprotection. On behalf of the state, ASN regulates nuclear safety and radiation protection. ASN issues regulatory decisions (general technical rules) that are to be endorsed by the government and issues technical rules and prescriptions. Not legally binding, ASN also provides guides that explain how to consider the corresponding regulation.

In France, certain types of EDDs are referred to using the related terms intelligent devices, simple devices, digital device of limited functionality, and smart devices. Regulatory guidance is broadly based on the IAEA standards [252]. Other relevant standards include the IEC 45A standards (mainly IEC 61513, IEC 60880), and French basic safety rule II.4.1a.

The system/component classification in France for the N4 plants (the current generation of nuclear power plants being built and operated in France) is five levels [162, 173]:

- 1E
- 2E
- SH
- Systems important to safety
- Not important to safety

The safety categories do not align well with the NRC's safety-related classification.

The system/component classification for the older plants in France is four levels [159, 161]:

- F1A: the safety functions needed to demonstrate that the plant can reach a controlled state for any design basis condition
- F1B: the safety functions needed to demonstrate that the plant can reach and be kept in a safe shutdown state up from design basis condition, for at least 24 hours
- F2: the safety functions needed to demonstrate that
  - the plant can be kept in a safe shutdown state up to 72 hours from any design basis conditions,
  - the plant can deal with the design extension conditions up to 72 hours,
  - the plant can withstand the internal and external hazards considered in the design over and beyond those included in the design basis analysis
- Non safety function: any other function

These safety categories also do not align well with the NRC's safety-related classification. These levels are systems and equipment are not in contradiction with IEC 61226, but are more precisely defined following the defense-in-depth principle as well as design extension corresponding to post accident conditions after 24 hours.

The French regulators define what they mean by *digital device of limited functionality* [14]:

- The device is a preexisting digital device that contains predeveloped software or programmed logic.
- The primary function performed is well defined and applicable to only one type of application within an I&C system.
- The primary function performed is conceptually simple and limited in scope.
- The device is not designed so that it is reprogrammable after manufacturing.
- If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process.

Up until 2000, no framework for regulating a smart device or devices of limited functionality existed, and the procedure for computer-based systems had to be used. Even a simple smart device with a good operational experience record could not be qualified if it was not developed to IEC 61513 with IEC 60880 or IEC 62138.

Since 2016, the current qualification framework in France for *digital devices of limited functionality* is as follows:

- All digital devices of limited functionality follow IEC 62671
- Already certified digital devices of limited functionality follow IEC 61508 with audit

Examples of digital devices of limited functionality include digital electrical off-the-shelf equipment such as a sensor, an actuator, an electrical protection device, etc., that is functionally simple.

RCC-E [253] provides guidance on industrial digital devices of limited functionality and introduces alternative qualification methods that credit IEC 61508 certifications. For the I&C aspects, the RCC-E relies heavily on IEC standards but clarifies an interpretation at a national level. The RCC-E identifies what is and is not relevant in a standard such as IEC 62671 within the context of equipment qualification.

The approach to qualification of software and programmed digital aspects of smart devices in France relies on the idea that smart devices are pre-existing components bought off the shelf and that requirements cannot therefore undermine previous design choices [176]. Requirements essentially address QA processes, including V&V activities as implemented by the design, and the way smart devices are used and implemented within a system. According to the qualification method, suppliers may be subjected to audit; such audits are likely to require more if there are no third-party product certifications available.

It is mportant to note that France recognizes that certifications by themselves cannot be used as a basis for qualification because licensees are responsible for what is installed in their plant [176]. This is the same as the requirements for plants in the United States.

Suppliers are required to inform EDF of any changes to a device and EDF then analyses whether the change is major or minor and what action to take [176]. This is also the same as the requirements for plants in the United States.

5.2.3 Germany

In Germany, certain types of EDDs are most likely referred to using the related terms digital device of limited functionality (synonym for device of dedicated functionality) or industrial digital device based on IEC terminology. Regulatory guidance is primarily based on the requirements defined by the German government [254] and nuclear regulator [255], which refer to the dedicated national standards relevant for hardware and software qualification. The approach is based on IEC standards such as IEC 61513, IEC 60880, and IEC 62138. DIN EN 61226 is the German version of IEC 61226. VDI/VDE 3528 [256] sets the regulatory expectations for COTS products.

The standards establish the criteria and methods to be used to assign the I&C functions of an NPP to three categories A, B, and C, which depend on the importance of the function for safety, and an unclassified category for functions with no direct safety role. The system/component classification in Germany, based on the definitions in IEC 61226, includes three levels for function:

- Category A: denotes the functions that play a principal role in the achievement or maintenance of NPP safety to prevent DBE from leading to unacceptable consequences.
- Category B: denotes functions that play a complementary role to the category A functions in the achievement or maintenance of NPP safety, especially the functions required to operate after the non-hazardous stable state has been achieved, to prevent design basis events (DBE) from leading to unacceptable consequences, or mitigate the consequences of DBE.
- Category C: denotes functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Category C includes functions that have some safety significance, but are not category A or B.

The safety categories do not align well with the NRC's safety-related classification.

The German equipment qualification applies to the approach prescribed by VDI/VDE 3528 [256]. This guideline describes the basic approach and boundary conditions for equipment qualification of commercial grade products, by intended use in nuclear I&C technology. The aim of VDI/VDE 3528 is to realize or preserve an I&C system with required reliability by use of components that are qualified according to industrial standards.

The most commonly used route for qualification of a digital system is to build on an existing commercial certificate of compliance to an industrial standard such as IEC 61508 and have the device certified by an assessor such as TÜV. When an already-qualified device is to be re-used in another application, the qualification process can claim credit for an existing pre-qualification. Generic qualification is also possible, which can be used as a basis for an application-specific qualification [176].

When a COTS product is to be used for a category A or B function, an independent expert appointed in accordance with German law also performs a suitability assessment, focusing on te development process, testing, and proven performance/experience.

5.2.4 India

In the Indian nuclear domain, Atomic Energy Regulatory Board (AERB) is the agency that certifies safety-critical software for NPPs.

In India, certain types of EDDs are referred to using the related term smart devices. Regulatory guidance is primarily from IEC 60880 for safety-critical software [257]. AERB safety guide (SG) D-25 [258] deals with the computer-based systems of pressurized heavy water reactors (PHWR). It provides guidelines for development of computer-based systems and explains the Standard Regulatory Review Process (SRRP) for computer-based I&C systems covering both hardware and software. IAEA standards, or other acceptable codes, are used to review specific areas for which AERB documents have not been prepared.

India's regulatory agency also require QA and cite ISO-9001. India also uses IEEE standards IEEE Std. 603 , IEEE Std. 7-4.3.2, and IEEE Std. 323.

In the Indian nuclear domain, the system classifications provided in AERB SG D-25 are:

- IA: I&C Safety Class A includes those computer-based systems that prevent postulated initiating events (PIEs) from leading to a significant sequence of events or that mitigate the consequences of a PIE. This class also applies to those computer-based systems the failure of which could directly cause a significant sequence of events.

- IB: I&C Safety Class B applies to computer-based systems that play a complementary role to the class IA systems in the achievement or maintenance of NPP safety. The operation of class IB computer-based systems may avoid the need to initiate class IA systems. Class IB computer-based systems may improve or complement the execution of class IA systems in mitigating the effects of a PIE. Class IB also applies to computer-based systems the failure of which could initiate or worsen the severity of a PIE.

- IC: I&C Safety Class C applies to computer-based systems that play auxiliary or indirect role in the achievement or maintenance of NPP safety. Class IC includes those computer-based systems that have some safety significance but do not belong to class IA or IB. They can be part of the total response to an incident but not be directly involved in mitigating the physical consequences of the incident.

The safety category IA aligns well with NRC's safety-related classification, but the other categories do not align well.

At present, regulatory guidance in India does not explicitly include/identify smart devices [259]. That said, the qualification of smart devices in India consists of two steps [260]:

- Generic qualification of product
- Qualification of smart device for specific application

Before a smart device can be used, a review is performed to ensure that the device is qualified for use in an NPP. This review requires that the device

- meets functional and performance requirements that are evaluated with testing (e.g., accuracy, EMI/EMC, seismic, etc.),

- has extensive operating experience, both inside and outside of the nuclear industry for the same model and software version of the device,

- has a well-established design process that was used throughout the lifecycle, the HRA and FMEA have been performed, and failure modes are predictable, and

- the manufacturing process was dependable, including ISO-9001 certification, version control, history, and problem reporting.

If the device has networking features, then the devices are evaluated for cyber security concerns.

The evaluation, which uses a graded approach, evaluates software to IEC 60800, IEEE Std. 603, IEEE Std. 7-4.3.2, and India's AERB SG-D-25. AERB SG-D-25 refers to IEC standards.

Additional (and practical) requirements for software in smart devices include the simplicity of the software without additional features, secondary function, and no unused code or features.

Not surprisingly, regulators have found that receiving source code and design documentation is difficult if at all possible, and the limited diagnostic information makes demonstration of software self-supervision difficult. Nuclear Power Corporation of India Limited (NPCIL), which is administered by the Department of Atomic Energy (DAE), proposes extensive black box testing and CCF analysis of systems with smart transmitters because of the unavailability of the source code [260]. Qualification of software tools is also an issue due to unavailability of reports detailing the qualification of the tools.

Similar to other countries, India recognizes that most requirements, guidance, and standards are given at a system level, which is difficult to apply at the component/device level.

The challenges faced by regulators in India are the same as those faced by other countries. An excellent compilation of challenges for qualifying smart devices is provided by Singh [259]:

- Digital devices are being used in large scale due to advantages of smart features.
- Smart features increase complexity and functionality.
- Uncertainties in assessment exist at the design stage.
- Validity of evidences are provided for assessment due to faster improvement and obsolesce of technologies.
- Sometimes it is difficult to know of the presence of smart devices in equipment in absence of internal details.
- Nuclear needs are not a priority for many commercial device manufacturers.
- Gap areas exist with respect to nuclear safety requirements for higher safety class.
- There is limited access to information on processes and design due to IP concerns.
- Design, development and manufacturing involves multiple vendors, so there is insufficient traceability and ownership of the original supplier.
- There is a greater chance of introduction of counterfeit, fraudulent, and suspects items and security vulnerabilities.
- Consideration of complementary testing and operating experiences could compensate for gap areas.

- Security assessment is challenging without knowing vulnerabilities.
- Diversity can prevent CCF v/s maintainability.
- Quality of documentation is lacking.
- Information is in pieces and is not written in compliance of justification needed for NPPs.
- Third-party assessors might not be aware of nuclear requirements.
- Documentation is available in different languages.
- Ensuring continuation of justification for future supplies is challenging.
- Suppliers continue to desire to upgrade products.
- Suppliers may not be proactive and may not consider that minor changes in design/component are important enough to record and report.
- Changes in manufacturing process are important.
- May require frequent requalification/revalidation exercises.

The experience in India in applying standards developed for systems at the component level can be useful in developing device specific guidance.

5.2.5 Japan

Prior to the Fukushima Daiichi accident, the requirements and guides for the licensing review process of establishment/permit for existing Japanese nuclear power plants were established by the Nuclear Safety Commission (NSC). After the Fukushima Daiichi accident, a new nuclear regulatory body, the nuclear regulation authority (NRA) was established to improve its nuclear safety management and regulation in 2012.

In Japan, certain types of EDDs are referred to using the related term smart devices. Japan does not currently have regulations specific to the use of smart devices; I&C systems important safety were built on the assumption of using only nuclear qualified products and are regulated using the same requirements. [19].

The safety system/component classification in Japan is three levels in accordance with the importance of their safety function [153]:

- Class 1: Secure and maintain as high as reasonably achievable level of reliability.
- Class 2: Secure and maintain a high level of reliability.
- Class 3: Secure and maintain a level of reliability equal to or higher than that for general industry.

Those SSCs of which loss of the function could cause an abnormality of the nuclear reactor facility, which causes excessive radiation exposure to the general public or the working personnel (the system for preventing the occurrence of abnormalities), are referred to as PS.

Those SSCs that have the function to prevent the propagation of abnormality or terminate it quickly in an abnormal situation of a nuclear reactor facility, and to protect the general public or the working personnel from possible excessive radiation exposure (the system for mitigating the impact of abnormalities), are referred to as MS.

The classification based on PS/MS and the three classes are:

- PS1 (prevention system)/MS1 (mitigation system)
- PS2/MS2
- PS3/MS3

The NRA defines safety functions as the functions of SSCs necessary to ensure the safety of nuclear reactor facilities. SSCs are categorized based on whether they can cause or prevent an AOO or DBA [261]:

(1) Functions that may cause, when lost, AOOs and DBAs in nuclear reactor facilities, potentially leading to undue radiation exposure of the public or site personnel

(2) Functions that prevent, in case of AOOs and DBAs in nuclear reactor facilities, the escalation of such conditions or put such conditions under control immediately, thereby preventing or mitigating potential undue radiation exposure of the public or site personnel

Importance of safety functions refers to the degrees of the importance of safety functions of the safety system/component from the viewpoint of ensuring the safety of nuclear reactor facilities to address or prevent the escalation of AOOs and DBAs.

Standards, codes, and acceptance criteria for regulatory authorization are established by legislation and regulation; the guidance is provided by selected U.S. NRC guidelines.

Three paths are provided in IEC 61513 on the functional validation stage—application software development, equipment (software and hardware) procurement, and development of novel system software and hardware features. Japan assumes that the procurement path provided in IEC 61513 will be adopted for smart devices [19].

The experience in Japan for regulating smart devices is similar to that of other countries [19]:

- *Basically the smart devices are designed to be applicable for various industries. Many selectable functions are designed and many software (program and Data) modules are implemented.*
- *The interconnectivity between each program, data structure, etc. are generally not disclosed*
- *The configuration data which defines the available functions of the smart devices are set by the vender or the purchaser*
- *The program update may be submitted as a functional improvement with new version and revision numbers without prior notice.*

Configuration management (CM) is essential for the successful use of smart devices. Watanabe recommends the following [19]:

- *The licensee need to decide information level according to the safety grade of smart devices (graded approach).*
- *The licensee need to request the smart device venders to disclose the device information.*
- *Considering the trouble investigation, CM of the smart devices is needed to cover all device information including every program and data for superfluous functions*
- *The licensee is needed to keep information matching with the implemented smart devices through the CM system.*

Japan does not specifically provide guidance on the use of smart devices but relies on the quality and function of the device application. Japan uses both IEC and IEEE standards as a safety basis.

5.2.6 Korea

In 1981, the Nuclear Safety Center was founded as part of the Korea Advanced Energy Research Institute (KAERI). In 1985, the Nuclear Safety Center branched off as an auxiliary organization KAERI. In 1990, the Korea Institute of Nuclear Safety (KINS) was independently established. Then in October 2004, the National Nuclear Control Agency (NNCA) was installed as an auxiliary organization of KINS, and the Korea Institute of Nuclear Nonproliferation and Control (KINAC) branched off in 2006.

In Korea, certain types of EDDs are referred to using the related term smart devices. Regulatory guidance is provided in KINS/GE-N001 [262], which is the Standard Review Plan for LWR in Korea. The Korean SRP based reviewsof CGIreference EPRI NP-5652, and EPRI TR-106439. Other U.S. NRC guidance documents used for guidance or required incude SRP BTP 7-19, SRM on SECY-93-087, NUREG/CR-6303, IEEE Std. 603, and IEEE Std. 7-4.3.2.

One of the missions of the KINS is to review and inspect nuclear installations including commercial NPPs, nuclear fuel cycle facilities and research reactors in Korea. KINS was established under the Korea Institute of Nuclear Safety Institute Law in February 1990. The regulatory experiences of KINS regarding the use of EDDs for safety I&C systems and the future work for them are discussed below.

These licensing requirements are intended to be implemented by the regulatory agency as binding requirements within the national legal framework. This document is supplemented by detailed guidance in reference G-RG-CP, “Preparation and Review of Applications for Construction Permits,” and G-RG-OL, “Preparation and Review of Applications for Operating Licenses,” (not yet published). These are supported by information in IAEA Safety Guides, NRC RGs, and guidance from other international sources.

The regulatory structure is that KINS and KINAC support the Nuclear Safety and Security Commission (NSSC) and the NSSC reports to the prime minister of Korea.

The system/component classification in Korea has three levels:

- IC-I (IC-1)
- IC-II (IC-2)
- IC-III (IC-3)

The safety categories do not align well with the NRC's safety-related classification.

The Shin Kori-3&4 Nuclear Power Reactors (SKN 3&4) are the first NPPs in Korea that adopted safety grade smart transmitters. SKN 3&4 also used digital relays for EDGs; these digital relays are EDDs that are composed of digital devices with firmware.

Specific to the review of smart transmitters, KINS [12] reviewed the use of smart transmitters against IEEE Std. 7-4.3.2-2003 [263] and IEEE Std. 1012-2004 [209]. IEEE Std. 7-4.3.2-2003 was used to evaluate software CCFs, including use of manual action and non-safety-related systems, or components, or both, to provide the means to accomplish the function that would otherwise be defeated by the CCF. IEEE Std. 1012-2004 was used to evaluate theto determine if it met the V&V requirements. The software was developed as IEEE SIL Level 4 or equivalent according RG 1.168 [319]. The equipment was qualified by IEEE Std. 323-2003 [158]. Also, SRP Appendix 7.0-A [264] and SRP BTP 7-19 [227] provided additional guidance on the assessment of the diversity and the defense-in-depth for the digital I&C systems.

KINS reviewed the digital relays for the EDGs as CGIs that must be commercially dedicated for use; EPRI TR-106439 was used for the dedication process. Also, KINS reviewed the QA program, problem reporting, the maintenance and troubleshooting process, and the operating experiences for the digital relays.

The major review points for the use of EDDs at KINS are as follows:

- Quality and reliability (QA program and V&V process)
- CCFs via software errors
- EMC
- CGI dedication (procurement planning, review, test, and control, etc.) [12]

KINS observed that EDDs might exist in safety grade procured equipment without explicit identification. Undetected defects of EDDs might be the potential safety concerns. EDDs should meet certain specific requirements in order to be selected and used in a safety I&C system.

KINS plans to develop technical positions for identification and qualification of EDDs; its technical position will address, but may not be limited to, quality and reliability, CCFs via software errors, EMC, and CGD for EDDs.

For devices that are used in safety systems such as the ultrasonic level transmitter in the APR1400, diversity is achieved using different, diverse manufacturer's designs for safety-related and non-safety–related applications [265].

The Korean regulatory framework is largely modeled on the U.S. NRC. However, the use of EDDs in Korean NPPs should be monitored for possible guidance and applications as they appear to be leading in this regard.

5.2.7 Pakistan

The Pakistan Atomic Energy Commission (PAEC), established in 1956, is an independent governmental agency and a scientific research institution, concerned with research and development of nuclear power, promotion of nuclear science, energy conservation and the peaceful usage of nuclear technology. In 2001, the PAEC was integrated with the National Command Authority (Pakistan), which is under the prime minister of Pakistan. Currently, the

PAEC is held responsible for design preparation and proper operational function of commercial nuclear power plants, and the safety regulations and protections of the nuclear power facilities are managed by the Pakistan Nuclear Regulatory Authority (PNRA).

In Pakistan, certain types of EDDs are referred to using the related term smart devices. The only regulartory guidance found for Pakistan was IEEE Std. 1012.

The use of smart devices is not yet recommended by PAEC for nuclear systems because of cyber threats. However, indigenous systems with smart devices may be candidates for use in non-safety class systems after rigorous V&V. The PAEC's concerns regarding the use of smart devices include [266]:

- Difficulty of system V&V
- Risk of cyber-attacks (currently no wireless controls are being installed at nuclear facilities in Pakistan)
- Anticipated problems for wireless-based smart systems

5.2.8 Romania

The National Commission for Nuclear Activities Control (CNCAN) is the nuclear safety and security regulatory authority of Romania that is responsible for the regulation, licensing and control of nuclear activities, ensuring the peaceful use of nuclear energy and the protection of the public and workers from the harmful effects of ionizing radiation.

In Romania, certain types of EDDs are referred to using the related term smart devices. Regulatory guidance is primarily from IEC 61511, EPRI 106439, and ANSI/ISA-S75.13.01.

Romania defines a smart device as [267]:

- an electronic device, generally connected to other devices or networks, that can operate to some extent interactively and autonomously
- a context-aware electronic device capable of performing autonomous computing and connecting to other devices by wire or wirelessly for data exchange
- devices such as sensors and valve actuators that contain computer-based technologies and are configurable to be suitable for a variety of applications
- devices with the capacity to generate elaborate data in addition to that strictly required by their main function

Pakistan recognizes that smart devices can provide self-diagnostics and improved capabilities. However, the cons of smart devices are their added complexity, additional failure modes, cyber security issues, and radiation sensitivity.

At the Cernavoda NPP, smart devices are used in transmitters, sensors, valves, pneumatics, valve positioners, relays, and controllers. The devices transmit data through the use of data diodes to communicate with an IoT, providing secure data transfer to IT systems (external or cloud based). Data communication uses the HART protocol.

Smart CANDU tools are an integrated set of software tools that facilitate online monitoring, self-diagnostics and analysis of systems to optimize performance and maximize plant life. This information management software application allows for system and component health monitoring.

The level of connectivity of smart devices is much greater than that of other countries, as shown in Figure 5-2.

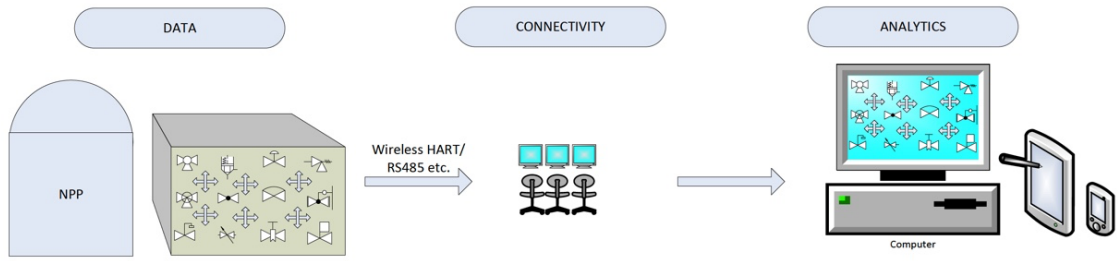


Figure 5-2 Interconnectivity of Smart Devices at Cernavoda NPP [268].

There were two presentations from Romania during the IAEA Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Systems Important to the Safety of Nuclear Power Plants. The first presentation [269] dealt with cyber-security guidance of digital applications and was not specific to smart devices. No unique information was presented.

The second presentation [267] described the use of smart devices at the CANDU-based NPP. There are three levels within the Cernavoda I&C architecture in which smart devices are employed: (1) analytics (system level – essentially the sense, command, and monitoring aspects of systems, (2) connectivity and communication, and (3) field devices. The first level involves digital platforms and software. The example given is the SMARTCANDU tools used for monitoring (ThermAND and ChemAND). This is not technically a smart device example, but rather it is a digital system that can be treated as such (i.e., assessed under typical digital system review guidance). No further information was presented on how this system-level equipment/system was licensed.

The second level is identified in terms of the communications equipment. Specific examples given are gateways and data diodes. No specific information was given on how these devices were assessed, but the other presentation on cyber-security assessments identified the regulatory approach to computer security (IAEA NSS-17, IAEA NSS-13, IEEE 7-4.3.2-2010, and IEC 62645).

The third level involves smart sensing and autonomous controllers. Two specific valve positioners (controllers) were identified: (1) Emerson Fisher digital valve controller (DVC) 6000, and (2) Emerson Fisher DVC 6200. These digital valve controllers are microprocessor-based current-to pneumatic instruments (microprocessor executes a digital control algorithm to establish a drive signal to the I/P converter based on the input demand). The DVC receives feedback of the valve travel position plus supply and actuator pneumatic pressure. This allows the instrument to diagnose not only itself, but also the valve and actuator to which it is mounted. In addition to the traditional function of converting a current signal to a pressure signal, DVCs use HART communications protocol for digital access to device information. The main difference between the two positioners is linkage. The DVC 6200 has a magnetic linkage, whereas the DVC 6000 has a mechanical linkage.

The justification for using the two smart positioners was based on CGI dedication guidance from EPRI TR-106439 (with emphasis on operating experience from Ginna, Vogtle and EdF) and vibration testing as defined in ANSI/ISA S75.13.01 [270]. Fatigue testing included 3 million cycles. No specific considerations were identified to address the smart characteristics of the devices other than citing the treatment of digital equipment under the EPRI CGI dedication guidance.

In summary, Romania simply follows the CGI dedication from EPRI TR-106439 and does not have specific guidance or practices for smart devices. They do, however, perform the typical vibration tests (based on ISA S75.13.01) and cite operating experience from Ginna, Vogtle, and EdF.

Regarding communications, there was no indication that they performed anything special for their gateways or data diode other than typical testing and following computer security guidance (IAEA NSS-13, IAEA NSS-17, IEC 62645, and IEEE 7-4.3.2-2010).

Essentially, Romania relies on IAEA and EPRI guidance, as well as the QA of the suppliers.

5.2.9 Russia

The Rosatom Nuclear Energy State Corporation is the agency responsible for fuel cycle and nuclear energy production activities, nuclear scientific and research centers, and Rosatom's nuclear weapons complex.

The Russian Research Institute for Nuclear Power Plant Operations (VNIIAES) is the organization that assists in NPP startup, operations, and training and that manufactures full-scope and analytical simulators.

Gosatomnadzor (GAN) is the state committee for nuclear and radiation safety and is responsible for regulating the safety of Russia's civilian nuclear reactors and fuel cycle enterprises. (The Ministry of Defense is responsible for all military nuclear facilities.) GAN licenses all civilian facilities that use radioactive materials, develops rules and standards governing the safe use of these materials, and inspects all facilities that use these materials, including NPPs. GAN is also charged with approving the design and construction of all nuclear plants.

In Russia, certain types of EDDs are referred to using the related term smart devices.

In the Russian Federation, Rostekhnadzor's regulatory activity in the area of I&C systems is based on the following regulations [248]:

- OPB-88/97, General Safety Provisions for NPPs (Sections 4.4, 4.5)
- NP-082-07, Nuclear Safety Rules for Reactor Installations of NPPs (Chapter 3)
- NP-026-04, Requirements to Control Systems Important to Safety of NPPs
- NP-006-98, Requirements to the Content of the Safety Analysis Report for VVER-type NPPs (chapter 7)

GOSTs are the Russian National Standards. Many GOSTs are adopted IEC standards:

- GOST R IEC 61513-2011
- GOST R IEC 60880-2010
- GOST R IEC 62138-2010
- GOST R IEC 60987-2011
- GOST R IEC 62340-2011
- GOST R IEC 61500

For those areas not covered by national regulations in due detail, such as digital I&C implementation, the provisions of internationally recognized documents such as IAEA standards are considered. IAEA standards that are part of the regulatory review include:

- IAEA Safety guide No. NS-G-1.3
- IAEA Draft Safety Guide DS-431

The system/component classification in Russia includes four levels [271]:

- Safety Class 1: includes fuel elements and elements of the NPP the failure of which would represent initiating events preceding BDBAs leading to damage of fuel elements with limits exceeding those established for DBAs on normal functioning of safety systems.

- Safety Class 2: includes elements the failure of which would be initiating events leading to damage of fuel elements within limits established for DBAs on proper functioning of safety systems with allowance for a specified number of failures in them for DBAs and safety systems elements, single failures of which lead to non-performance of functions by the relevant systems.

- Safety Class 3: includes systems important to safety that are not included in safety classes 1 and 2; elements containing radioactive substances release of which to the environment (including NPP rooms) on failures would exceed values specified in radiation safety standards; and elements performing control functions of radiation protection of personnel and the population.

- Safety Class 4: assigned NPP normal operating elements not affecting safety and not included in safety classes 1, 2, 3.

The classification categories for safety class 2 align well with the NRC's classification structure for *safety-related*, safety class 3 aligns well with *important to safety*, and safety class 4 aligns well with *nonsafety*. Safety Class 1 is related to BDBAs and does not align well with other regulators classification structure.

In discussing the safety aspects of using smart digital devices in nuclear systems important to the safety of NPPs, Sivokon discussed the challenges of digitizing I&C systems [272].

Russia recognizes the differences between analog and smart devices and uses technology in between—hardwired logic. IEEE Std. 610.10 1994 defines *hardwired* as "pertaining to a circuit or device whose characteristics are permanently determined by the interconnections between components." Hardwired logic is defined as "a group of logic circuits permanently interconnected to perform a specific function." Their hardwired logic uses components with CMOS ICs (AND, OR, NOT gates, flip-flops, counters, multiplexers, etc.), analog-to-digital converters (ADCs) without microcontroller cores, EEPROMs, solid state relays, transistors, diodes, resistors, capacitors,

fuses, etc. They do not use processors, microcontrollers, FPGAs, or CPLDs because they recognize that only very simple devices are thoroughly testable.

Advantages of hardwiring include [273]:

- Software errors and malfunctions are not a problem because there are no software controls in the algorithm processing.
- Behavior is predictable, and in-depth testing can be performed without the complicated ICs (microprocessors, FPGAs, CPLDs) inside, simple standard logic ICs allow detailed analysis during development, even with the multimeter or oscilloscope, and equipment behavior is much more predictable even in malfunction.
- Hardwiring is cyber secure by design.
- There are no abundant or unused elements and no hidden functions.
- Hardwiring ensures easier qualification.

Disadvantages include [273]:

- Difficult to incorporate online proof testing in a single nonredundant device (monitoring still possible).
- Difficult to implement some time domain processing such as PID control

This hardwired logic platform (HLP) has or is being implemented in the following plants and systems:

- Novovoronezh NPP unit 6 Diverse Actuation System (DAS)
- Leningrad NPP 2 unit 1 Additional Diverse Actuation System (ADAS)
- Novovoronezh NPP unit 7 Diverse Actuation System (DAS
- Rostov NPP unit 4 ESFAS channel
- Leningrad NPP 2 unit 2 Additional Diverse Actuation System (ADAS)
- Rostov NPP unit 3 ESFAS channel
- Kalinin NPP unit 1 ESFAS channel

Many of the regulations used in Russia apprear to be based on IEC standards. Thus, a review of IEC standards should cover the regulatory basis in Russia.

5.2.10 United Kingdom

The Office for Nuclear Regulation (ONR) is the United Kingdom's (UK's) independent nuclear safety and security regulator. ONR's inspectors use the safety assessment principles (SAPs), together with supporting technical assessment guides (TAGs), to guide their regulatory judgements and recommendations when undertaking technical assessments of nuclear site licensees' safety submissions.

In the UK, certain types of EDDs are referred to using the related term smart devices.

In the United Kingdom, smart devices are defined as [11]:

- COTS
- Based on microprocessors/microcontrollers running software/firmware, or a hardware description language (HDL)-programmed device
- User configurable but not user programmable (user cannot add new functionality)

Regulatory guidance is primarily from ONR SAPs, ONR TAG-046, TGN 032, IEC 61508, and the suite of (IEC) BS EN standards such as BS EN 61513, BA EN 61226, etc. Company Technical Standard CTS 214, mandates processes for C&I modification and replacement, and Technical Guidance Note (TGN) 032 outlines processes for the justification for the use of smart devices [11]. This guidance along with input from external standards such as IEC 61508, BS EN 61513, IEC 61226 feed into the Regulatory framework of ONR SAPs and TAG 046.

In evaluating a component or system, the UK first identifies the safety function of the device and then evaluates how the SSCs deliver those safety functions and their significance to safety. The basic safety requirements for UK nuclear facilities are identified in the SAPs issued by the Nuclear Safety Division of the Health and Safety executive which provides a framework for the consistent application of the principles. The nature of the UK regulatory regime is not prescriptive; however, the UK does support international standards that may be prescriptive.

The safety categorization scheme employed links with the licensee's design basis analysis. The three-safety system/component classifications are [124, ONR SAP ECS.1]:

- Category A: any function that plays a principal role in ensuring nuclear safety
- Category B: any function that makes a significant contribution to nuclear safety
- Category C: any other safety function contributing to nuclear safety

SSCs that have to deliver safety functions are identified and classified on the basis of those functions and their significance to safety [124], ONR SAP ECS.2]:

- Class 1: any SSC that forms a principal means of fulfilling a Category A safety function

- Class 2: any SSC that makes a significant contribution to fulfilling a Category A safety function or forms a principal means of ensuring a Category B safety function

- Class 3: any other SSC contributing to a categorized safety function

The expectation in the UK is that the extent of the justification required is according to the safety significance of the device according to its safety class. Three safety classes are recognized in accordance with the relevant SAP (i.e., Class 1 to 3). As a minimum (e.g., Class 3), demonstrated good commercial quality of the production excellence of the device may be sufficient, with commissioning test results and prior use as ICBMs. At the higher safety class (e.g., Class 1), it is necessary to assess a wide range of manufacturer documentation, including source code. Extensive ICBMs are also expected at Class 1 compared to Class 3, sufficient to make an adequate case for safety in the intended application.

Safety-related systems are distinct from safety systems in that, while they often have a significant influence on safety, they do not provide the primary means of protection for fault sequences. In an I&C context, safety-related systems include facility control systems, indicating and recording instrumentation, alarm systems, and communications systems.

The definition in ONR TAG 046, which is taken from the IAEA Safety Glossary, is a little different:

SAFETY RELATED SYSTEM – An item important to safety that is not part of a safety system (IAEA Safety Glossary). Safety-related systems are therefore systems in place to perform an operational function but which also provide a safety benefit. Safety related systems do not provide the primary means of protection for fault sequences. This is distinct from safety systems which are systems that do not perform any operational functions and are included solely because of the safety functions they perform.

ONR TAG 046 also uses the term *computer based systems important to safety* (CBSIS). A *system important to safety* is a safety system or safety-related system that implements safety functions at categories A–C and hence is assigned a corresponding class 1–3. The term *CBSIS*, therefore, encompasses both safety systems and safety-related systems that are computer based.

The classification categories do not align well with the NRC's classification structure, and this could lead to confusion with NRC regulations and guidance in that ONR considers safety-related systems to be distinct from safety systems. However, the basis of classifying based on safety function could provide potential avenues to explore for classification of devices.

Specific to the use of COTS smart devices, the UK recognizes the following challenges[11]:

- The risk from systematic failure must be sufficiently low.
- The device must always fail [safe] when triggered by a systematic failure (e.g., due to design flaws, human error, logic errors).
- A sufficiently low safety claim (class 3/2/1, $10^{-2}/10^{-3}/10^{-4}$ PFD) is inherited from the system safety case.

ONR TAG-046 identifies limits to the reliability claims that can be placed for a single smart device for the different safety classes. Modifications at the I&C architecture level may be an effective way to reduce the claim on each smart device if supported by a suitable CCF analysis. SAP ESS 27 [124] states that for computer-based systems,

Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.

ONR TAG-046 provides additional guidance for supporting clause SAP ESS.27 and outlines a two-legged approach for demonstrating the suitability of a smart device. The two legs consist of [274]:

1. Production excellence (PE) includes proof that the technical design practice is consistent with current accepted standards for the development of software for computer-based safety systems, implementation of a modern standards quality management system, and an application of a comprehensive testing program formulated to check every system function. This is a demonstration of excellence in all aspects of production from the initial specification to the finally commissioned system.
2. ICBMs include complete, preferably diverse checking of the finally validated production software by a team that is independent of the system's suppliers, and an independent

assessment of the comprehensive testing program covering the full scope of the test activities.

Production excellence for smart devices is typically assessed using the EMPHASIS approach (see Adelard below). The Emphasis assessment is used to provide evidence of the QA, design and development processes used by manufacturers of smart devices.

While the application of specific standards is not mandatory, "...the case for production excellence is greatly assisted by evidence of the systematic application of national and international ... standards, coupled with a case by case justification of non-compliances" [126]. IEC 61508, IEC 61513, and IEC 60880 are typical of the standards recommended for this role [176].

ICBMs are generally carried out by the licensee independently from the manufacturer, with specialized technical support where needed. To maximize the value added, they are generally expected to be diverse from the compensating measure used in the PE leg.

Licensees are responsible for ensuring that their use of COTS devices complies with SAP ESS.27 and TGN 046. The level of justification required for a smart device depends on a number of factors, but it broadly aligns with the safety function categories and system classes of IEC 61226.

In its guidance on COTs smart devices in ONR TAG-046 Revision 5, compensating activities are allowed to make up for the gaps in production excellence information. No attempt is made to define the compensating activities (compensatory measures), as these would be determined on a case by case basis.

5.2.10.1 Sellafield

Sellafield is a nuclear site involved in fuel reprocessing, nuclear waste storage, and decommissioning.

The actual reliability of instruments used at Sellafield, both "smart" and "dumb," have been catalogued over many years in the Sellafield Reliability Database (SRdB). However, the SRdB had little data on new models (mostly smarts) being offered by manufacturers. Their original intent was to use these new smarts on basic plant control systems (non-safety) and thus establish figures in the SRdB to show the reliability of these new smarts.

Sellafield's experience on the use of smart instruments [50] is described in the following:

- *It was often very difficult to even tell if an instrument was Dumb or Smart. Manufacturers' data sheets never specified if microprocessors were used. O&M manuals often never went to this level of detail on component parts, and visual examination often proved inconclusive.*

- *Existing models became Smart over-night. An instrument purchased just two years before was known to be dumb and purchasing an identical instrument with exactly the same part number now delivered an identical Smart Instrument. Manufacturers thought this was a good thing!*

- *It became clear that the introduction of Smarts was proceeding faster than Sellafield staff could gather SRdB data on them in non-safety systems.*

Realizing there was a knowledge gap around the subject of smart instruments in SISs, Sellafield formed a nuclear industry working group (NISIWG) [50]. Members consist of Sellafield Ltd., British-Energy, Magnox Generation, Urenco, BAE Systems, Atomic Weapons Establishment,

Devonport Dockyard Management Limited, Rolls-Royce Naval Marine, and GE Healthcare. NISIWG had several objectives that include a common understanding of the technology, identification of potential problem areas, sharing of substantiations, spreading of costs, production of individual company standards and procedures based on a common substantiation methodology, and of course some market advantage with manufacturers.

At first, most manufacturers cooperated enthusiastically, but as the scope of the data NISIWG required became clear, only a very few were able to deliver. It is worth reviewing why many manufacturers withdrew from helping NISIWG further, as it is a clear indication of the way the market economy is influencing the whole IEC 61508/61511 issue.

Most manufacturers' support waned as a consequence of the following issues [10]:

- A lack of understanding of IEC 61508 by the manufacturer.

- The UK nuclear industry process instrument market is only around 3% of the turnover of a large UK-based manufacturer. The nuclear industry is not a "big player" anymore. Pressure transmitters, for example, were sold at 1.8 million annually, of which just 540 were purchased by the whole UK nuclear industry.

- The average purchase price of a smart instrument is around £1,000, with small profit margins.

- When IEC 61508 was first published, both potential users and manufacturers of 61508 type equipment had no previous experience with it and early offerings reflected this lack of experience. Manufacturers had already paid considerable funds to third parties to issue certificates, which NISIWG was now questioning. Typical examples included certificates stating SIL3 compliance, with NISIWG erring toward an SIL1 rating. Manufacturers were therefore concerned that NISIWG's work would undermine the existing certificates. In recent times however, there has been a noted improvement in certification quality.

- It became demonstrably obvious that other industries were simply not as concerned about this issue as the nuclear industry. Indeed, NISIWG was often the only source of enquiries the manufacturer ever received for further details on the certification process.

6 STANDARDS AND GUIDES

National and international standards provide normative criteria and guidance on the use and regulation of a host of components, including those pertinent to EDDs. United States and international standards were reviewed to learn how others regulate and implement EDDs and to possibly leverage this experience into the framework of NRC regulations and guidance (Table 6-1). Guidance on the development and assessment of EDDs were evaluated for EPRI, IEEE, ISL, and NIST. The use of the standards and guides by country is cited in the review of how each specific country addresses the use of EDDs in NPPs.

Table 6-1 Standards Development Organizations (SDOs) and Organizations with Guidance Documents Cited by National and International Industries

SDO or organization
Adelard
AIChE – American Institute of Chemical Engineers
API – American Petroleum Institute
Automotive
CSA Group – formerly, Canadian Standards Association
CSB – Chemical Safety Board
EPRI – Electric Power Research Institute
EUROCAE – European Organisation for Civil Aviation Equipment
IAEA – International Atomic Energy Agency
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronic Engineers
ISA – International Society of Automation
ISO - International Organization for Standardization
NEA – Nuclear Energy Agency
NEI – Nuclear Energy Institute
NIST – National Institute of Standards and Technology
ONR - UK Office for Nuclear Regulation
In-house developed standards

From a standards perspective, both the nuclear IEEE (e.g. IEEE 603) and the nuclear IEC (e.g. IEC 61513) standards suites use system-level requirements that are not easily synthesized down to component- or EDD-level requirements.

How other standards are used to classify and regulate systems and devices can be useful in identifying differences in regulatory philosophy and potential modifications that could be incorporated into the NRC regulatory structure. Many of the standards are based on the IEC suite of standards. For example, Adelard, API, ASIL, CSA Group (Canada), DOE, ISA, ISO, MDEP, NEI, ONR, OSHA, and FRA use IEC standards. The IAEA standards are the basis for the first tier of IEC standards for safety for nuclear I&C (IEC 61513). Feeding into IEC 61513 is IEC 61508 for functional safety (non-industry specific). Several are based on IEEE standards, such as (of course) IEEE and NIST. The EPRI reports provide a solid basis for evaluating specific aspects of safety.

The IAEA's approach to the safety classification of SSCs considers safety classification (important to safety and not important to safety), functionality, and consequences that result if the function fails when it is required to perform, and it is also related to the consequences in the event of a spurious actuation. The classification typically begins with categorization of the functions to be performed by I&C systems, which are assigned to categories according to their importance to safety. The safety importance of a function is related to the consequences.

Standards and their associated regulations can be either prescriptive or performance based. Prescriptive requirements specify features, actions, or programmatic elements to be included in the design or process as the means for achieving a desired objective. Performance-based requirements rely upon measurable (or calculable) outcomes (i.e., performance results) to be met but provide more flexibility to the licensee as to the means of meeting those outcomes. A performance-based approach establishes performance and results as the primary basis for decision-making and incorporates the following principles: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee, performance; (2) objective criteria to assess performance are established based on risk insights, deterministic analyses, and performance history; (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not, in and of itself, constitute or result in an immediate safety concern [275].

Many of the standards are performance based, including those cited by DoD, DOE, ISA, ONR, and OSHA. Many of the standards reviewed also recognize and take into account that certain types of EDDs are dedicated devices of limited, specific functionality, that contain or may contain components driven by software or digital circuits designed using software-based tools. In fact, EUROCAE allows the system architectural features, such as redundancy, monitoring, or partitioning (the separation of critical from non-critical functions) to reduce the degree to which components contribute to specific failure conditions. Thus, a partitioned device can have different Design Assurance Levels (DALs) within the same component.

Because many regulations and standards are based on IEC SILs, it is important to learn from those that have evaluated the implementation of IEC SILs and those that have cited some shortcomings of the standards. The objective of EPRI 3002011817 [276] is to demonstrate that equipment certified to non-nuclear safety standards (more specifically, IEC-61508/61511) can meet or exceed nuclear power safety and reliability requirements without further analysis or verification. For the suitability of an item, EPRI 30020118186 states that IEC SIL certification to IEC 61508 may provide evidence of product or platform suitability. An NEI working group is leveraging EPRI 3002011817 to specify a third-party IEC 61508 SIL certification as an alternate approach to determining the acceptability of some of the dependability critical characteristics as defined by EPRI TR-106439. Adopting IEC SIL certifications would allow NPPs to use the same supply chain and structures that non-nuclear safety related industries use. This broadens the supplier base, promotes competition, and allows the harvesting of economies-of-scale arising from other safety industries.

Determining how IEC SIL certifications fit within the U.S. NRC regulatory structure would be a difficult task. Because quality and safety are related, certification to meet IEC SILs has quality implications, and it is be expected that as the SIL increases, the quality requirements would also increase. As written, the 10 CFR 50 Appendix B/CGD approach for safety-related components is not readily transferrable to cross-walking quality standards to the different SILs.

Before determining how the IEC SIL certification would fit within the NRC regulatory structure, it is important to note the limitations of applying standards for the process industry to the nuclear industry.

IEC 62671 [17] states that “IEC 61508 can be used as complementary guidance for the evaluation and assessment of components [for use in the nuclear industry], but it is recognized that certification to non-nuclear standards alone is insufficient.” This statement most likely recognizes the lack of clear mapping between the prescriptive nuclear requirements and the performance-based requirements of IEC 61508. It also reflects the concept that IEC 61508 requirements may not address nuclear-specific environmental concerns. Similarly, Summers notes that “Following a careful review of a significant variety of product safety manuals, it appears that many field devices are achieving higher safety integrity level (SIL) claims than can be supported by process industry data [123].”

Of note are those countries or agencies that use standards and guidance beyond the IEC suite of standards. More specifically, in addition to IEC standards, Canada uses CAN CSA-N290.14 and CSA-N290.8 and the UK uses ONR SAPs, ONR TAG-046, and TGN 032, respectively. DoD uses MIL-STD-882E, which is focused on providing performance criteria and does not prescribe specific design criteria or even specific design techniques. The main goal of MIL-STD-882E is to eliminate hazards when possible and to minimize risks when hazards cannot be eliminated. NASA uses a consequence-based approach in NASA-GB-8719.13 to evaluate the consequences of the device failure and its impact on the system. The EMPHASIS tool used by Adelard uses a claims-based approach that is designed to demonstrate that the behavior and functionality of the product is sufficient for its intended application and that the products will behave accordingly throughout its design lifetime.

Industrial control equipment manufacturers, railway equipment, automobiles, medical devices, and airborne software use some type of SIL that can be 3, 4, or 5 levels (a SIL 0 or DAL E is not included in the number of levels). BS EN 50128 does not use all five levels of safety integrity. Instead, the requirements for SIL 1 and SIL 2 are the same for each technique or measure. Similarly, each technique or measure has the same requirements at SIL 3 and SIL 4. Therefore, effectively, there are recommendations for techniques and measures for only three SILs in BS EN 50128 [67]. Translating the integrity levels to safety/not safety for the NRC has not been performed but the categorization of these levels may provide insight to the NRC regulatory structure by providing information on how components are categorized compared to safety/not safety.

One benefit of using IEC SILs is that the SILs correlate the probability of failure on demand-average (PFDavg) or risk reduction factor (RRF) to safety. The U.S. DOE is like the NRC in that it does not currently use probabilistic classification methodologies for components. However, regulators within and outside the nuclear industry do use probability of failure as a measure of safety. ONR, through ONR TG-046 [126], relates the safety class to the probability of failure on demand for standby and frequency of failure per year for active components. The U.S. DoD assesses and documents risk based on the severity category and probability level of the potential mishap(s) for each hazard across all system modes.

The -2018 version of ISO 26262 includes guidance for software tool selection, use, documentation, and qualification. NASA expects that automatically generated code be treated at the same level as hand-generated code.

Although there are four integrity levels, the newer version of IEEE-1012-2016 no longer uses the "SIL" terminology to avoid confusion with the much more widely used IEC-61508 context; rather, IEEE 1012-2016 refers to integrity levels.

Insights and lessons to be learned could be gleaned from detailed reviews of the IEC standards (which covers most applications), Canada, UK, NASA, and DoD. Standards from each of these have a different philosophy for addressing safety. Many of the standards use a claim-based approach or consider the functionality of the device in performing a safety assessment. Others, such as ASIL, have a qualitative measurement of risk, whereas IEC SIL is quantitatively defined as probability or frequency of dangerous failures depending on the type of safety function.

The documents in Table 6-2 are the most similar works identified that are related to the comparison of industries that mitigate significant risk using digital instrumentation and controls equipment.

Table 6-2 Most Similar Works

Existing Work	Summary of Evaluation
Nuclear Use of I&C Equipment Certified for Commercial Safety Use [85]	Johnson recognizes that new technology will first appear in commercial markets because there is a larger market. The one exception is for nuclear specific functions and equipment. The commercial industry now has certification processes for safety systems and equipment based upon IEC 61508, UL 1998 and others.
Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety [277]	The collections of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, certain IEC standards deal with specific I&C functions, a topic area where IEEE standards are largely mute. This paper considers how the two sets of standards may be used in a complementary fashion to achieve broader topic coverage than is possible using only one or the other standard suite.
Comparison of the Software Safety Criteria between IEC and IEEE Standards for the Digital Instrumentation and Control System [278]	The paper also compares the safety lifecycle and planning activities defined in IEC 61508 with those in IEC 60880 for the software safety lifecycle, IEEE 7-4.3.2 for the computer safety system lifecycle, and IEEE 1228 for the software safety lifecycle. Most of the IEC and IEEE standards consist of three main phases—planning phase, the realization phase according to the plan, and the validation phase. This paper shows the differences in the safety lifecycles between the IEC and IEEE standards. A major difference is that the safety lifecycles in the IEEE standards require a direct safety analysis at each phase of the lifecycle.
The Potential for a Generic Approach to Certification of Safety Critical Systems in the Transportation Sector [23]	The concept is similar to the present work, but the focus is on railway, automotive, and aerospace sectors. This paper investigates the potential for common treatment of certification of safety critical programmable electronic systems in the transportation industries. It contains a comparative review of new, emerging international standards that are likely to influence certification procedures in the railway, automotive and aerospace sectors in the future. These include the EUROCAE/SAE aerospace guidelines, the CENELEC railway standards, and IEC-61508. The review identifies the common and divergent requirements for certification among these standards.

6.1 Adelard

The development of the Evaluation of Mission imperative, High-integrity Applications of Smart Instruments for Safety (EMPHASIS)[15] assessment tool is based on a questionnaire derived from IEC 61508 [229]. The EMPHASIS assessment tool for "smart" instruments is intended for use in nuclear safety-critical applications in the UK [279].

EMPHASIS can be used with different target IEC SILs. For components with a lower integrity aim, other processes may be used that do not typically reach the same level of detail as an Emphasis assessment. Third-party product certifications (e.g., commercial certificates of compliance to IEC 61508) can be taken into account in the assessment of production excellence but are neither necessary nor sufficient for successful assessment. Compensatory activities must be carried out if the production excellence leg falls short of the standard expected.

The EMPHASIS approach has been accepted by ONR and licensees in the UK to dedicate the use of components with smart devices. Thus, the approach to justifying the use and application of smart devices in the UK nuclear industry is a mature process.

The EMPHASIS tool is based on IEC 61508 and is used by licenses, and an increasing number of suppliers. EMPHASIS's methodology is to examine a series of criteria that includes the company, its core competencies, the tools and techniques used in the design and production of the product, and the testing requirements. More specifically, the types of evidence sought in the assessment stage of EMPHSAIS include product certificates, equipment manuals, company policy documents, design documentation, documentation of safety-related functions, and configuration management procedures.

The EMPHASIS tool is used to meet the production excellence leg of the two-legged approach in TAG-046. EMPHASIS consists of approximately 300 questions structured in four phases, and is inherently graded due to being based on IEC 61508 with its four SIL levels:

- Phase 1 covers QA and safety management.
- Phase 2 covers generic programmable electronic aspects and development process for the device as a whole.
- Phase 3 covers hardware development process and verification activities.
- Phase 4 covers software development process and verification activities.

15 EMPAHSIS was initiated by Moore Industries and the Control and Instrumentation Nuclear Industries Forum (CINIF, UK) in 2003/4 to address concerns regarding smart sensors. One of the projects funded by the CINIF, entitled "COTS Goal-based Safety Assessment" (COGS), was aimed at developing an approach to the safety justification of COTS products like devices dedicated to a single function, user-programmable and control equipment, or certain software-only products such as operating systems. COGS is a claim-based approach that is designed to demonstrate that the behavior and functionality of the product is sufficient for its intended application and that the products will behave accordingly throughout its design lifetime. According to CINIF, the key advantage of a claim-based approach is that there is greater flexibility in making a justification while ensuring that all safety relevant attributes of the COTS product are justified. The EMPHASIS tool is now owned by CINIF and has subsequently been developed further and supported by Adelard LLP on behalf of CINIF.

EMPHASIS is typically performed by considering the device independently of the application where it will be used. This allows for reuse of the justification in a number of applications, provided that the behavior of the device and any restrictions identified during the assessment are suitable for each application.

Many regulators and industries use IEC SILs for components with different safety requirements. The EMPHASIS questionnaire can be configured for different IEC SILs by including more techniques and measures at higher SILs, as defined in IEC 61508.

The depth and breadth of the questions in EMPHASIS are directly linked to the level of detail in the wording of the requirements of IEC 61508. This standard is fairly long because the issues in assuring the software and hardware in computer-based systems are inherently complex. An analysis with significantly less depth is likely to trivialise or brush over essential aspects of the standard. IEC 61508 was chosen because many suppliers already claim compliance with its requirements, and UK regulators (e.g., ONR, HSE) recognize it as relevant good practice forming a benchmark for legal adequacy.

Adelard, working with Emerson, used EMPHASIS to assess the Rosemount 3051 Pressure Transmitter and the Rosemount 644 Temperature Transmitter using Emphasis at SIL 3 and 2 respectively [31]. The Rosemount 3051 pressure transmitters and Rosemount 644 temperature transmitters are the nonnuclear versions of the transmitters and are not qualified for nuclear plant use. Over 8 million pressure transmitters and 1.5 million temperature transmitters have been installed worldwide [31]. At present, the nuclear qualified pressure transmitters are 3051N [280].

Emerson answered over 300 assessment questions and provided over 150 archived documents as evidence for each individual product. Demonstrating production excellence requires the manufacturer of the smart device to show that all aspects of design, development and production are consistent with best practice and are performed in the context of an adequate quality management system. Additionally, the manufacturer must demonstrate that they have performed a testing program that verifies all functions of the device. Adelard visited Rosemount's premises for seven days to discuss and understand the development procedures and the approach to design and verification and to review the answers provided.

The Rosemount 3051 transmitter's capabilities include power advisory diagnostics and temperature alerts. Power advisory diagnostics detect issues such as corroded terminals and wiring, grounding, and power supply issues. Temperature alerts can be set to notify if the process temperature reaches a trip high alert or low alert value, the total time the value was reached, and more. The transmitter is optimized with a local operator interface (LOI) and power advisory diagnostics to reduce installation and commissioning time. With wireless capabilities, these devices enhance monitoring and can operate in remote and hard-to-reach locations.

The Rosemount 644 can use 4-20 mA /HART® protocol, FOUNDATION™ fieldbus protocol, or PROFIBUS® PA protocol. It has an LCD Display or LCD Display with LOI. The device performs basic diagnostics, has Hot Backup™ capability, sensor drift alert, thermocouple degradation, and min/max tracking. (A hot backup means the backup controller is running. A hot backup controller is not considered to be independent of the primary controller because it is subject to common cause failure [195]. Furthermore, hot backup controllers may have components that are common to both the primary and the backup controller, such as the backplane, firmware, diagnostics, and transfer mechanisms which could have undetected dangerous failures.)

Emerson's feedback on the assessment of its transmitters using EMPHASIS is that the analysis was rigorous, beyond what they had been previously subjected to in other third-party certifications, but that it was well targeted and focused on issues relevant to product quality [281]. Emerson considered its self-funding of the assessment costs to be money well spent (usually the assessment is funded by the licensee). Note also that one of the Emerson assessments found the instrument to have fulfilled the production excellence criteria for class 1 / SIL3.

According to Adelard, safety demonstrations of commercial products can be challenging because of insufficient support from suppliers (products are sold as a black-box, design documentation constitutes intellectual property, etc.), unclear guidance documents, and inapplicability of known analysis techniques among others [282, 226]. However, creating justifications for higher classes will require access to code and development documentation (IP) to reach appropriate conclusions with sufficient confidence, but this IP does not leave the company and should not be carried into the safety case [281].

It is recognized that it is not easy to use the EMPHASIS tool to qualify the digital devices because (1) the assessors need special training on how to use the EMPHASIS tool; (2) the assessors have to have a very good understanding of IEC 61508; (3) the assessors should have a good knowledge of the digital devices to be qualified; (4) the current nuclear market for such digital devices is very small. Thus, there are not many qualified assessors available to do the qualification. The process, because of its complexity and completeness, seems to be greater than current reviews; however, if a vendor undertakes such as review and it is approved by ONR, the NRC ought to be able to substantially leverage those reviews.

The EMPHASIS assessments can be used to inform and support other safety cases so they can be used in other regulatory activities. In the United Kingdom, there is no problem in piecing together a case using parts from other assessments [281]. In fact, reusing an EMPHASIS assessment is just this on a large scale: reusing the whole production excellence leg. Claims, arguments, and evidence are ideal mechanisms for doing this while ensuring that the claims, arguments, and evidence are appropriately used in the new application.

Several devices have been assessed following the methodology in ONR TAG-046 by Adelard. Examples of smart devices justified for nuclear application in the UK include:

- Temperature transmitters
- Pressure transmitters
- Radiation monitors
- Protection relays
- Gas analyzers
- Voltage regulators

The majority of this has been done at Class 3. Only a limited number of devices have been assessed to Class 1 and 2.

6.2 American Petroleum Institute (API)

American Petroleum Institute API standard RP 554, Part 1 [283] provides a discussion of general functional communications that exist in a process control system; API RP 554, Part 2 [284] describes a number of common implementations of these communications functions described in Part 1.

API RP 554, Part 2 discuses smart devices along the traditional sense of industrial practice—these smart instruments communicate directly with the process control systems or with each other. These instruments not only transfer information about the basic process measurement, but they also communicate diagnostic information about the health of the device or other secondary information derived from the primary measurements.

The overall risk of a plant may be managed by focusing inspection efforts on the process equipment with higher risk. API 581 [285] provides a basis for managing risk by making an informed decision on inspection frequency, level of detail, and types of nondestructive examination (NDE). IEC 61511 is an informative reference to API 581.

None of the regulators reviewed cited an API standard. In addition, the application of smart devices in the petroleum industry, with their communication capabilities, is beyond what is in use in most industries, including the nuclear industry.

6.3 Automotive

Automotive Safety Integrity Level (ASIL) is a risk classification process defined by ISO 26262 [72]. ISO 26262 is an international standard that is an automotive specific implementation of IEC 61508. ISO 26262 does not provide normative nor informative mapping of ASIL to SIL. While the two standards have similar processes for hazard assessment, ASIL and SIL are computed from different points. Whereas ASIL is a qualitative measurement of risk, SIL is quantitatively defined as probability or frequency of dangerous failures depending on the type of safety function.

ASIL has 4 SILs—A, B, C, and D. ASIL A represents the lowest degree, and ASIL D represents the highest degree of automotive hazard.

ISO 26262 calculates ASIL based on the severity of the injuries that could result from an event, the likelihood the event will occur in normal operation, and how many drivers could control the situation to avoid the injury. The standard defines functional safety as “the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical or electronic systems.” ASILs establish safety requirements based on the probability and acceptability of harm for automotive components to be compliant with ISO 26262.

Because ASIL is a relatively recent development, discussions of ASIL often compare the SILs to levels defined in other well-established safety or quality management systems (Table 6-3). In particular, the ASILs are compared to the SIL risk reduction levels defined in IEC 61508 and the design assurance levels used in the context of DO-178C and DO-254. While there are some similarities, it is important to also understand the differences.

Table 6-3 Approximate Cross-Domain Mapping of ASILs [286]

Domain	Domain-specific safety levels				
Automotive (ISO 26262)	Quality management	ASIL-A	ASIL-B/C	ASIL-D	—
General (IEC 61508)		SIL-1	SIL-2	SIL-3	SIL-4
Aviation (ED-12/DO-178/DO-254)	Design assurance level (DAL) -E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	—	SIL-1	SIL-2	SIL-3	SIL-4

6.4 CSA Group

IEC standards adopted by Canada as national standards are published as CSA standards by the CSA Group (formerly the Canadian Standards Association). CAN/CSA-C22.2 NO.61511 adopted IEC 61511 with Canadian deviations. Because CAN/CSA-C22.2 NO. 61511 is essentially the same as IEC 61511, it is reviewed under IEC standards below.

The Canadian Nuclear Safety Commission (CNSC) regulates the use of nuclear energy and materials in Canada. The CNSC is currently in a transition period regarding its standard applicable to digital devices. The previous licensing basis referenced CSA N290.14-07 [250], but now all new licenses and re-licensing activities are referencing the second edition of this standard—CSA N290.14-15 [94]. The scope of CSA N290.14-15 expanded the scope of CSA N290.14-07 to include hardware and a broader range of software.

The qualification activities specified in CSA N290.14-15 include the performance of a design review that focuses on several specific concerns that would potentially impact the digital item's ability to perform its safety function. These topics are silent for undetected failure, flooding, determinism, and performance (execution timing), common mode (systematic integrity), security, power interruption or restart, time-dependent behavior, modal behavior, shared resources, upgrades, maintainability issues, extra functionality, communications (wired of wireless), coexistence, user interface, and other postulated failure modes.

CSA N290.14-07 provides a systematic approach to qualifying predeveloped software for use in safety-related applications, and there is an extensive amount of experience with using the standard.

The qualification activities specified in CSA N290.14-15 also include guidance for performing a failure analysis. Several references are provided for performing this analysis. Those references are IEC 62502 for event tree analysis, IEC 60812 for failure mode and effects analysis, IEC 61882 for hazard and operability studies, IEC 61025 for fault tree analysis, and EPRI 3002000509 for hazard analysis. Two complementary methods are required to be used for category 1 applications, and one method is required to be used for category 2 and 3 applications.

A product that has been pre-certified (e.g., using IEC 61508) assists in demonstrating compliance to some of the requirements in CSA N290.14. Then there are qualification activities specified in CSA N290.14-15 that are dependent on pre-developed software (and digital items) or custom software (and digital items). For pre-developed software/digital items, four methods identified for

qualification are identified as being available for use that are dependent on the category of the digital item. This category appears to be similar to what the NRC considers CGIs. Table 6-4 identifies the methods and their availability for each of the categories.

Table 6-4 Applicable Methods for Qualification of Predeveloped Software [94]

Method	Applicable categories		
	Category 1	Category 2	Category 3
Recognized program	✓	✓	✓
Mature product method		✓	✓
Proof through testing			✓
Preponderance of evidence	✓	✓	✓

The recognized program method may be applied to pre-developed software digital items to be used in Category 1, 2, or 3 applications (Table 6-5). This method involves verifying that the process used to produce the digital item or the digital item itself conforms to one of the appropriate standards identified in Table 6-5. Conformance may be verified during the qualification activities, or it may be verified by an audit report or certification that was generated by an independent third party (separate from the OEM).

Table 6-5 Acceptable Standards for the Recognized Program Method [94]

Category	Acceptable software development standards
1 (High safety significance)	1. OPG/AECL CE-0100-STD and OPG/AECL CE-1001-STD; 2. IEC 61508 (SIL 3); or 3. IEC 61513, Class 1 and IEC 60880
2 (Moderate safety significance)	1. OPG/AECL CE-1002-STD; 2. IEC 61508 (SIL 2) 3. IEC 61513, Class 2, and IEC 62138, Category B; or 4. IEEE 828, IEEE 830, IEEE 1012, and ISO/IEC 12207
3 (Low safety significance)	1. OPG/AECL CE-1003-STD; 2. IEC 61508 (SIL 1) 3. IEC 61513, Class 3 and IEC 62138, Category C; 4. ISO 9001 using the guidance in ISOIEC 90003; or 5. ISO/IEC 12207

The mature product method can be used for Category 2 and 3 applications and requires a minimum amount of successful operating history and minimal details on the item's complexity. This approach cannot be used for Category 1. Table 6-6 identifies the required operating history in years.

Table 6-6 Minimum Unit Years of Required Operating History [94]

Pre-developed software digital item complexity	Operating history, minimum unit years		
	Category 1	Category 2	Category 3
Low	n/a	200	100
Medium	n/a	500	200
High	n/a	1,000	500
Very high	n/a	2,000	1,000

The proof-through-testing method may be applied to pre-developed software digital items and items that are to be used in Category 3 applications. For a pre-developed software digital item that runs with discrete executions (e.g., software that runs only during system startup, such as boot firmware), the complexity of the pre-developed software digital item should be low (< 1,000 lines of code, < 20 internal modules, < 5 interface complexity index); the pre-developed software digital item should performs the same steps (i.e., not responding to varying external stimuli) on each execution in the given configuration; and the pre-developed software digital item should be tested in a configuration representative of its final installed configuration, without any failure, meeting the minimum number of test executions. For a pre-developed software digital item that is used continuously while the system is online (e.g., a disk controller), its complexity should be determined to be low (see above); it should continuously loop through a consistent set of steps, and it should be dynamically tested in a configuration representative of its final installed configuration, through all operational modes and a representative range of input values, without any failure, and meeting the minimum number of test hours. See table 4-6 for further detail on how the standard evaluates complexity.

The preponderance-of-evidence method may be applied to pre-developed software digital items to be used in Category1, 2, or 3 applications. This method consists of one or more of the following elements:

a. proven-in-use arguments;

b. partial compliance with applicable industry standards or guidelines, or other equivalent documents;

c. evidence from a previous qualification or a generic pre-qualification (e.g., certification to the relevant standard of IEC 61508) of the pre-developed software digital item, with consideration of the limits of applicability to the current application;

d. complementary testing;

e. analysis of the candidate product (e.g., design test coverage review); and

f. use of software modules, objects, libraries or components that have been verified.

CSA N290.14-15 allows a graded approach based on safety significance, operating history, complexity, functionality, and continuous or standby operation.

6.5 Chemical Safety Board (CSB)

The Chemical Safety Board (CSB**)** is an independent federal agency charged with investigating industrial chemical accidents. The CSB conducts root cause investigations of chemical accidents at fixed industrial facilities. Root causes are usually deficiencies in safety management systems but can be any factor that would have prevented the accident if that factor had not occurred. Other accident causes often involve equipment failures, human errors, unforeseen chemical reactions or other hazards.

The CSB does not issue citations or fines, but it does make safety recommendations to facility management, industry organizations, labor groups, and regulatory agencies such as OSHA and EPA. After conducting an investigation, the CSB identifies any need for improvements and modernization to OSHA's PSM and to the Environmental Protection Agency's (EPA's) Risk Management Plan (RMP) program. Both OSHA and EPA have safety management regulations.

6.6 Department of Defense (DoD)

DoD has a large range of different applications for safety systems and mission critical computer applications. DoD expends extensive effort into developing those systems in a manner that allows them to have a very high level of correctness, reliability, and security. DoD uses MIL-STD-882E [83] to focus on providing performance criteria and does not prescribe specific design criteria or even specific design techniques. MIL-STD-882E states that its main goal is to eliminate hazards when possible and to minimize risks when hazards cannot be eliminated. The process for achieving this goal involves 8 elements. Those elements are:

1. document the system safety approach,
2. identify and document hazards,
3. assess and document risk,
4. identify and document risk mitigation measures,
5. reduce risk,
6. verify, validate, and document risk reduction,
7. accept risk and document, and
8. manage life-cycle risk.

During the process of assessing and documenting risks, the risks are categorized by severity and probability (frequency of occurrence). The probability levels can be defined as either qualitative or quantitative. Additionally, it is acknowledged that software risks must be assessed differently. Due to inherent differences between the ways that hardware and software fail, predicting the probability of software failure is very difficult and cannot be based on historical data. Instead, software risks are assessed using software control categories, along with the severity categories to determine a software criticality index (SwCI). The SwCI is then correlated into a level of rigor (LOR) that can be used to define what the safety requirements are for the software.

Concerning classification of equipment, some specific terms are described in MIL-STD-882E. Those terms are *safety-related*, *safety-critical*, and *safety-significant*. *Safety-related* is a term applied to a condition, event, operation, process, or item whose mishap severity consequence is either marginal or negligible. *Safety-critical* indicates a condition, event, operation, process, or item whose mishap severity consequence is either catastrophic or critical. *Safety-significant* is a term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related. DoD recognizes that even though these terms have been defined, their specific meaning will vary based on the nature of each specific application.

Hazard analysis is a significant aspect of the methodology prescribed in MIL-STD-882E. The sequence of hazard analyses is the preliminary hazard analysis (PHA), system requirements hazard analysis (SRHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), operating and support hazard analysis (O&SHA), health hazard analysis (HHA), functional hazard analysis (FHA), system-of-systems (SoS) hazard analysis, and environmental hazard analysis (EHA).

The assessment of risk for software, and consequently software-controlled or software-intensive systems, cannot rely solely on the risk severity and probability. Determining the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application-specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. Therefore, another approach shall be used for the assessment of software's contributions to system risk that considers the potential risk severity and the degree of control that software exercises over the hardware. The degree of software control is defined using the Software Control Categories (SCC) in Table 6-7 (or approved tailored alternative) [83].

Table 6-7 The Software Criticality Matrix Shows how the Severity and Software Control Categories are Correlated to Determine a Software Criticality Index for the DoD

Severity → SCC	Catastrophic	Critical	Marginal	Negligible
AT Autonomous	1	1	3	4
SAT semi-autonomous	1	2	3	4
RFT redundant fault tolerant	2	3	4	4
Influential	3	4	4	4
NSI no safety impact	5	5	5	5

In summary, MIL-STD-882E does not prescribe the use of any specific design architectures or methodologies to achieve safety. Instead, it is focused on the elimination and management of the risks involved and drives documentation of the specific methodologies that are implemented. It also prescribes the verification steps to ensure the implementations comply with the safety requirements that were derived from the hazard analyses.

The *Software System Safety Engineering Handbook* [84] is not a standard like MIL-STD-882E, but it is intended to provide additional guidance for achieving software system safety (SSS) as a subset within the overall concepts of system safety engineering. Appendix D of this handbook is specifically focused on use of COTS and NDI software. The approach presented in this handbook for evaluating a COTS item for selection and use in a safety system consists of the use of three criteria: confidence, influence, and complexity. The confidence aspect is focused on achieving strong evidence that indicates the COTS item will successfully perform its critical functions when installed within the full range of possible operating environmental parameters. The influence aspect focuses on understanding the safety significance of the role of the COTS item within the host safety system. Finally, the complexity aspect focuses on a combination of safety factors, testability factors, and integration factors. With these three criteria—confidence, influence, and

complexity—evaluations can be performed to make decisions about whether or not certain COTS items should be used within a particular safety system.

6.7 U.S. Department of Energy (DOE)

The U.S. DOE is like the NRC in that it does not currently use probabilistic classification methodologies. As a result, DOE-STD-1195 prescribes a deterministic approach based on the independent protection layers (IPLs) analysis methodology. Appendix B of the DOE standard contains a table that correlates the number of IPLs to either a SIL 1 or SIL 2 (reproduced as Table 6-8). The SILs are derived from ANSI/ISA 84.00.01-2004, which itself is based on the IEC SILs. During the establishment of the safety basis for a DOE facility, the number of IPLs existing to prevent a hazardous event from occurring are counted and used to determine the SIL in accordance with the IPLs.

Table 6-8 SIL Determination Methodology in DOE-STD-1195-2011 [187]

Number of IPLs		
	3	SIL-1
	2	SIL-2
	1	SIL-2

Hardware fault tolerance (HFT) is defined as the ability of a functional unit to continue to perform a required safety function in the presence of a fault. This ability is expressed in the minimum number of required redundant sensors. The requirements per SIL expressed in Table 6-9 are from IEC 61511-1 [195]. This table is read by first looking for the SIL and then looking at the fault tolerance minimum. For example: A SIL 2 application requires one sensor and one redundant sensor. A SIL 4 application requires one sensor and two redundant sensors.

Table 6-9 Minimum Hardware Fault Tolerance Requirements According to SIL (IEC 61511-1 Table 6)

SIL	Hardware fault tolerance (minimum)
0	0
1	0
2	1
3	1
4	2

The HFT requirement is not affected by the selection of either certified or prior-use sensors.

The HFT is comparable to redundancy in the nuclear sector. The safe failure fraction (SFF) and associated hardware fault tolerance requirements are intended as a way of preventing manufacturers from claiming high SILs for non-redundant devices simply based on the PFD calculation. The SFF tables were intended to ensure fault tolerance through required redundancy.

6.8 Electric Power Research Institute (EPRI)

EPRI provides guidance on the CGD process, configurability, SIL, and identification of an undeclared digital device in a component.

Many regulations and standards are based on IEC SILs. The objective of EPRI 3002011817 [276] is to demonstrate that equipment certified to non-nuclear safety standards (more specifically, IEC-61508/61511) can meet or exceed nuclear power reliability requirements without further analysis or verification at what EPRI describes as the "platform" level which refers to products and equipment versus levels involving how those are applied or integrated into the plant. This would allow NPPs to use the same supply chain and structures that non-nuclear safety related industries use. This broadens the supplier base, promotes competition, and allows the harvesting of economies-of-scale arising from other safety industries.

EPRI 3002011816 [154], the Digital Engineering Guide (DEG), applies systems engineering as the foundation to conduct a facility change that adds or modifies digital technologies, whether it is a new plant design, a major analog to a digital facility change, or a minor update to a software module in an installed digital system. The guidance uses a graded approach to match the rigor of each activity with the commensurate risks. Of interest is its applicability to EDDs. The DEG does not use the term embedded digital device, but EDDs would fit straightforwardly within the scope of the DEG. The DEG also uses the related term *digital configuration item*. The report states that "A digital configuration item is an aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process." It also notes that digital configuration items can be found in mechanical or electrical equipment (i.e., not just I&C equipment). Equipment information items such as technical manuals, data sheets, specifications, etc., should be examined carefully to determine if the equipment contains digital content. Equipment inspections may aid in this determination. Embedded programs, data and operating systems (firmware) and application software are considered digital configuration items.

For the suitability of an item, the DEG states that IEC SIL certification to IEC 61508 may provide evidence of product or platform suitability. If SIL certification is used as a method for demonstrating product or platform suitability, then the restrictions or conditions specified in the safety manual shall be integrated with related activities.

Some EPRI reports complement NRC regulatory guides by providing guidance for meeting the CGD requirements of 10 CFR 21 and the QA requirements of 10 CFR 50, Appendix B. EPRI NP-5652 [73] and EPRI TR-102260 [74] focus on CGD of hardware components. EPRI TR-106439 [54] and EPRI TR-107339 [77] provide guidance for accepting commercial-grade digital equipment. EPRI TR-1025243 [165] provides guidance for the CGD of safety-related design and analysis software tools.

In 1988, EPRI published EPRI NP-5652 to address industry concern over an effective methodology to ensure the proper dedication of CGIs used in safety-related applications. EPRI NP-5652 was the first guidance document to provide a detailed acceptance methodology specific to CGD for items used in NPPs. Industry's use of the CGD process has significantly increased over time as the number of suppliers with nuclear QA programs has decreased. However, the previous industry dedication guidance was developed in the late 1980s, and the NRC had only previously endorsed EPRI dedication guidance in Generic Letter 89-02 [287] and Generic Letter 91-05 [288].

EPRI NP-5652 defines the basic process for CGD: a technical evaluation, definition of critical characteristics for acceptance, and use of any of four acceptance methods to verify the characteristics. The key points of EPRI NP-5652 are the basic premise of CGD and the four acceptance methods for dedication. EPRI NP-5652 contains a generic procedure for acceptance of CGIs, as well as four alternative acceptance methods to provide flexibility. These four alternative acceptance methods are:

Method 1 — Special Tests and Inspections

Method 2 — Commercial-Grade Surveys of Suppliers and Vendors supplying CGIs

Method 3 — Source Verification

Method 4 — Recording of Acceptable Supplier/Item Performance

The report describes the implementation of each method and reviews examples of situations in which it could be beneficial to use more than one acceptance method.

EPRI TR-102260, which is not endorsed by the NRC, provides supplemental guidance to EPRI NP-5652 regarding the implementation of the process for dedicating CGIs for nuclear safety-related applications.

Digital equipment utilizing software presents new challenges in commercial dedication. However, the same basic approach still applies. Key elements of the dedication process are:

- An up-front technical evaluation to define the requirements for the device
- From these requirements, selecting a set of critical characteristics for acceptance
- Applying the methods described in NP-5652 (as endorsed by Generic Letter 89-02 and supplemented by Generic Letter 91-05) to verify the critical characteristics (or using the revision to NP-5652 as conditionally endorsed by RG 1.164).

With digital equipment, there are new critical characteristics and additional verification activities that need to be performed compared to analog equipment.

EPRI TR-106439 states that the following:

> *It is important to remember that when the final set of critical characteristics has been identified, all of these characteristics must be verified including physical, performance and dependability characteristics.*

Although a prescriptive list of critical characteristics for each application of each device type may be useful, such a list could be easily misused. The list would become a check list rather than considering the device, its design, and use. It is the opinion of the ORNL researchers that a generic list of critical characteristics would not be a good solution, as they would be used as a checklist, and the result would not be adequate. Advances in I&C technology and functionality would require frequent updates to the check list otherwise the check list would become quickly outdated. An analogy is the migration from analog to digital systems. The first digital systems mimicked the analog systems. As experience with digital systems increased so did the

complexity, functionality, communications, etc. of the systems. The same is likely to occur with EDDs.

If appropriate verifiable critical characteristics cannot be identified, then commercial grade dedication cannot be used.

EPRI TR-102260 evaluated industry activities that occurred since the publication of EPRI NP-5652 and provides updated information that can be used to reduce engineering and procurement costs associated with CGD. Key points that should be considered when using this document in discussing software tools is that its primary focus is on materials and equipment and that no specific discussion is provided for digital equipment or software.

EPRI 3002002982 [53] is conditionally endorsed by RG 1.164. The NRC participated in the development of these methods [289]. EPRI 3002002982 describes a methodology that can be used to dedicate CGIs for use in safety-related applications. The scope of applications for which CGI dedication is used has evolved significantly since EPRI published EPRI NP-5652 and EPRI TR-102260. The guidance in this final report reflects lessons learned and addresses challenges that were identified through the expanded use of the original guidance.

EPRI TR-106439 [54] provides guidance for the dedication of commercial-grade digital equipment for use in safety systems. The guidance provided in EPRI TR-106439 addresses (1) application of the preexisting nondigital CGD guidance to digital systems, (2) identification of applicable codes and standards, (3) a process to perform the evaluation of commercial-grade digital equipment, and (4) acceptance criteria for using commercial-grade equipment in a safety system. This guideline is intended to help utilities evaluate, design, and implement digital upgrades involving commercial software-based equipment. The NRC's safety evaluation of EPRI TR-106439 concluded that "TR-l06439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plants." Furthermore, SRP BTP 7-18 [290] states that "EPRI TR-106439 and EPRI TR-107330 describe an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides additional information on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors for purchased PLC software."

EPRI TR-107330 [291] is a specification for qualifying a commercially available PLC for use in a safety application. The specifications are for evaluating a PLC for a safety-reated application, establishing a suitable qualification test program, and confirming that the manufacturer has an adequate QA program. The specification include requirements for QA measures to be applied, documentation to support the qualification, and documentation to provide the information needed for applying the qualified PLC platform to a specific application. EPRI TR-107330 emphasis that qualifying a particular platform for a different range of applications can be accomplished by making appropriate adjustments to the requirements. The NRC's safety evaluation of EPRI TR-107330 [292] concluded that the TR-107330 guidance "is applicable to the generic qualification of a PLC as a component for safety-related applications....Because TR-107330 is generic, licensees referencing TR-107330 will need to document the details regarding the use of this specification in plant specific applications."

EPRI TR-107339 [77] is a supplement to EPRI TR-106439. EPRI TR-107339 provides more detailed guidance for evaluating commercial digital equipment through tailoring of the guidance in EPRI TR-106439 consistent with the importance of the digital equipment to safety and economics. EPRI TR-107339 provides guidance for each of the phases of the CGI dedication process, including project definition, defining the detailed requirements, defining the critical characteristics

for acceptance, formulation of an acceptance strategy, and verification of critical characteristics. Unlike EPRI TR-106439, EPRI TR-107339 is not endorsed by the NRC. The primary focus of EPRI TR-107339 is on the differences in the technical evaluation and acceptance process required for digital, software-based equipment and systems.

EPRI TR-1011710 [78] updates the methodology provided in EPRI TR-107339. This handbook provides updated design, analysis, and critical digital review guidance. The document was written by Electricité de France (EdF) and a U.S. consulting firm. The handbook combines the similar methods used in both countries for reviews of digital equipment (critical digital review and reinforced functional qualification [QFR]), incorporating the lessons learned and best practices from both countries. This documentation is not required to perform CGD, nor is it endorsed by the NRC, but it provides extensive updated guidance for documented design analysis of digital I&C as part of CGD.

EPRI TR-1025243 provides guidance for using its CGD methodology to accept commercially procured computer programs that perform a safety-related function. EPRI TR-1025243 provides a methodology that can be used to perform safety classification of non-process computer programs, such as design and analysis tools, that are not resident or embedded (installed as part of) plant systems, structures, and components. The report also provides guidance for using CGD methodology to accept commercially procured computer programs that perform a safety-related function. Included in EPRI TR-1025243 is a clarification of CGIs as related to computer programs. EPRI TR-1025243, Rev. 1 is endorsed by NRC Regulatory Guide 1.231 with the following exception: “the NRC staff does not accept the use of Revision 1 of EPRI Technical Report 1025243 dedication methodology for process (installed or embedded) computer programs or software tools associated with process computer programs.”

EPRI 3002002289 [167], which is not endorsed by RG 1.231, supersedes EPRI 1025243. As with hardware, when a computer program having the functional safety classification of *safety-related* is furnished as a commercial item, it should be procured as commercial grade and dedicated for use as a basic component in a safety-related application. Guidance for accepting software integral to a plant’s SSCs is not included in the scope of EPRI 3002002289 because this type of software has been evaluated for use by the NRC. Guidance for accepting devices with integral computer programs may be found in the EPRI TR-106439 and EPRI TR-107330.

There is one important point to note in the discussion of CGD of the software portions of I&C systems described above: the difficulty in using testing as a tool to determine the quality of the software is that testing does not normally take into account software behavior under abnormal conditions and events. This differentiates system software from software tools, which are normally used under ideal conditions. Any abnormal event or condition that occurs during the testing or use of software tools can be eliminated simply by retesting or reprocessing.

Other EPRI documents not specific to the CGD process that are of interest for using and replacing EDDs include EPRI TR-1001503, EPRI 1008256, EPRI 3002005326, and EPRI 3002008010, which are described below.

The objective of EPRI TR-1001503 [34] is to identify and document existing systems and components that can be used for the modernization of I&C equipment in nuclear power plants and to make utilities more aware of alternative ways to modernize obsolete and costly-to-operate equipment. A database application consisted of a vendor’s database containing vendor information, a systems database capturing the capabilities of the product line, and a utilities

database containing data about specific implementations of a platform at NPPs. The database application was not maintained and is no longer available.

EPRI 1008256 [293] (formerly EPRI NP-6406), which is not endorsed by the NRC, provides detailed guidance for the technical evaluation of replacement items. This includes determining whether a replacement item is an equivalent or like-for-like replacement or if it is sufficiently different that a design change is required. It also includes guidance on defining safety-related functions and design requirements from which critical characteristics are identified.

EPRI 3002005326 [294], which is not endorsed by the NRC, recognizes that potential vulnerabilities can be managed using a combination of preventive and mitigative measures. This report provides practical guidance for addressing a full range of potential digital failure and CCF contexts. It includes steps for identifying and qualitatively assessing susceptibilities in terms of their likelihood, failure effects, and the measures in place to protect against them. The report also includes guidance on using susceptibility and coping analyses to screen and prioritize potential vulnerabilities. The guidance also includes the application of risk insights. The guidance provided in EPRI 3002005326 draws from industry standards and practices, lessons learned, and related EPRI products published over the last several years. It addresses both safety and non-safety applications. Technical considerations include factors that affect the likelihood of both latent software defects and the activating conditions that can trigger them—factors such as software development practices, test coverage, system and functional complexity, and designed-in defensive measures. The guide recommends using a safety-significance–based graded approach that considers the context of the I&C in the plant, the likelihood of failure, and the failure consequences in assessing the adequacy of the implemented preventive and mitigative measures.

Undeclared digital content is a concern in components with EDDs. EPRI 3002008010 [57], which is not endorsed by the NRC, was prepared to assist EPRI members and their suppliers in detecting digital content embedded in electrical and electronic equipment and to prevent undeclared digital content from being installed. The report addresses the attributes associated with digital content including the type of processor, if the item supports data communication, and if the item is configurable. The report also provides signs of digital content (supplier literature, external, and internal) and how to identify them.

EPRI documents for CGD have evolved since first publishing EPRI NP-5652 in 1988. Although EPRI 3002002982 supersedes the original versions of EPRI reports EPRI NP-5652 and EPRI TR-102260 in their entirety [289], many CGI dedications cite EPRI NP-5652.

Of particular importance to EDDs is EPRI's document on undeclared digital content (EPRI 3002008010).

6.9 European Organisation for Civil Aviation Equipment (EUROCAE)

EUROCAE (European Organisation for Civil Aviation Equipment) ED-79/ARP-4754 [295] is focused on the railway, automotive, and aerospace sectors.

System safety requirements are established by a functional hazard assessment. The safety requirements of each function are defined by the most severe failure condition associated with this function. Table 6-10 shows the relationship between the five classes of failure conditions with the quantitative functional safety requirements (maximum rate of failure per flight hour) and the development assurance level for the system.

Table 6-10 Relationship Between Severity of Failure Condition, Safety Requirement, and Development Level [237]

Failure condition class	Quantitative safety requirements (failure/h)	Development assurance level (DAL)
Catastrophic	$P < 10^{-9}$	A
Hazardous	$P < 10^{-7}$	B
Major	$P < 10^{-5}$	C
Minor	None	D
No safety effect	None	E

DAL A is comparable to IEC SIL 4, DAL B to IEC SIL 3, DAL C to IEC SIL 2, and DAL D to IEC SIL 1 [286].

While quantitative assessments can be used to assess whether safety requirements have been met for hardware, as far as systematic safety (hardware design and manufacturing/ software/installation errors) is concerned, qualitative techniques must be applied, and judgements must be made to demonstrate that a system meets the target safety levels.

The verification of safety requirements in a complex system would be problematic if these requirements were only expressed quantitatively [296]. The DALs (referred to as *integrity levels* by other SDOs) provide a qualitative indicator that a system meets its safety objectives. Its principal role is to relate a level of assurance about system safety to the application of an appropriate combination of quantitative and qualitative techniques during the system lifecycle.

Similar to other standards and guidance, when a function or a system is implemented using an architecture with more than one component, all the components inherit the system development level.

System architectural features such as redundancy, monitoring, or partitioning (the separation of critical from non-critical functions) can reduce the degree to which components contribute to specific failure conditions. Appropriate architectures can, therefore, reduce the necessary assurance activity, and as a consequence, the component DALs. The guidelines specify a number of such architectures and specify the potential reductions. A list of architectures is presented in Table 6-11.

Table 6-11 Architecturally Derived (and Reduced) Development Levels [237]

Architecture	Most severe system failure condition / system development level	
	Catastrophic/A	Major/B
Partitioned design	Level A for the partition. Each partitioned portion can take a level corresponding to the most severe failure condition within the partitioned portion	Each partitioned portion can take a level corresponding to the most severe failure condition within the partitioned portion
Two dissimilar, independent design implementing a function	Level B for each portion	Level C for each portion
Two independent, partitioned designs implementing a function	Level A for the partition, level A for the primary portion, level B for the secondary portion	Level B for the partition, level B for the primary portion, level C for the secondary portion
Active/monitor parallel designs	At least one portion to level A, the other portions to level C	At least one portion to level B, the other portion to level C
Backup, parallel design	Primary portion to level A, backup portion to level C	Primary portion to level B, backup portion to level D

Thus, ARP 4754 allows credit for partitioning, diversity, and redundancy for reducing the severity of system failure.

6.10 International Atomic Energy Agency (IAEA)

The top layer of the IEC standards derives from IAEA standards:

- IAEA SSR-2/1 [297] and IAEA SSR-2/2 [298] for the safety of nuclear power plants
- IAEA SSG-39 [16], which superseded IAEA NS-G-1.3 [172], for I&C systems important to safety in NPPs

These standards are the basis for the first tier of safety for nuclear I&C: IEC 61513. Feeding into IEC 61513 is IEC 61508 for functional safety (non-industry specific).

The glossary for the IAEA [299] defines an item important to safety as “an item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.” Safety systems, safety-related items, and safety features (for design extension conditions) are all items important to safety:

- Safety system: a system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents
- Safety-related system: a system important to safety that is not part of a safety system
- Systems not important to safety

The term *safety feature* (for design extension conditions) refers to an "item that is designed to perform a safety function for or that has a safety function for design extension conditions."

IAEA SSG-39 [16] provides recommendations on the design of I&C systems to meet the requirements established in IAEA Safety Standards Series No. SSR-2/1 [297]. IAEA SSG-39 is a revision and combination of IAEA safety guide IAEA NS-G-1.1 and draft safety guide IAEA DS-431. I&C systems important to safety are identified on the basis of the identification of necessary I&C safety functions and the definition of systems that perform certain combinations of these functions. The classification using IAEA SSG-39 aligns philosophically with the NRC classification.

IAEA SSG-39 provides guidance on the preparation of documentation used to adequately demonstrate the safety and reliability of computer-based systems important to safety. This safety guide applies to all types of software: pre-existing software or firmware, software to be specifically developed for the project, or software to be developed from an existing pre-developed equipment family of hardware or software modules. The safety standard requires software tools to be verified and assessed consistent with tool reliability requirements, the type of tool, the potential of the tool to introduce fault or fail to make the user aware of existing faults, and the extent to which the tool may affect redundant elements of a system or diverse systems. Tools that can introduce faults or fail to detect faults need to be verified to a greater extent than other tools; however, verification is not necessary if the tool output is systematically and independently verified.

IAEA SSG-39 [16] states that

> *Commercial off the shelf devices tend to be more complex, may have unintended functionalities and often become obsolete in a shorter time. They will often have functions that are not needed in the NPP application. Qualification of a commercial off the shelf device could be more difficult because commercial development processes may be less transparent and controlled than those described in this Safety Guide. Often, qualification is impossible without cooperation from the vendor. The difficulty associated with acceptance of a commercial off the shelf device may often lie with the unavailability of the information to demonstrate quality and reliability.*

The IAEA recognizes that SSG-39 is focused on the safety system. A new IAEA Nuclear Engineering (NE) Division series document will focus on smart devices and how the devices are used in an application [300]. Efforts on this new safety report began in 2018.

The IAEA is also working on Safety Report NSNI-18-23 [301] to address concerns specifically related to the use of smart devices. The IAEA recognizes that industrial or commercial grade smart devices are typically developed according to non-nuclear industry standards. Some of these devices are certified by non-nuclear organizations using those non-nuclear standards for the use in industrial safety applications (e.g. oil and gas industries, railways, aircraft). The qualification of an industrial or commercial smart device for applications in NPPs may be more difficult than a device specifically developed for the nuclear application. Similar to the nuclear industry, the availability of the information to demonstrate quality and reliability of a device is difficult to obtain. Currently there is limited regulatory guidance on the safe use of smart devices in nuclear safety systems, namely to select and evaluate smart devices for their use in NPPs, make use of a third-party certification within the framework of the assessment process, and adequately implement safety design criteria based on a graded approach.

IAEA SSG-39 provides limited, high-level guidance on the qualification of digital devices with limited functionality in order that they can be used in I&C systems important to safety. IEC 62671 provides guidance on the selection and use of industrial digital devices with limited functionality.

IAEA NSNI-18-23 specifically focuses on the selection and evaluation of devices of limited, specific functionality and limited configurability, for use in NPPs. Additional details on techniques and measures expected at different safety levels are available in IEC 61508.

IAEA COTS Guide NR T 3.31 [7] recognizes (1) the gradual decrease of market availability of nuclear qualified products, (2) the worldwide transition to digital technology, and (3) the increasing dependence on integrating commercial I&C products within new development or modernization projects. COTS devices are produced in large quantities, with varied widespread use and significant operating experience, providing a large, user-based test bed in which problems are identified and fixed. COTS devices may also offer benefits such as an extensive history of operation, a large installed user base, improved reliability with a proven operating history, proven technology, self-monitoring, and a larger group of technical personnel experienced with using them.

The use of COTS devices in systems important to safety raises concerns because their quality and integrity is not commonly developed in accordance with nuclear standards. Prior to use in NPPs, there is a need to demonstrate that digital COTS devices adhere to the functional, safety and environmental requirements (including heat, humidity, vibrations, electromagnetic interference/radiofrequency interference [EMI/RFI], seismic, etc., requirements as appropriate) with a level of quality and reliability comparable that of a nuclear product. When COTS devices are used in NPPs, it is important that a suitable process is in place to gather sufficient evidence and confidence to demonstrate that these products will meet specific quality, functional and non-functional requirements expected in the intended application.

The COTS guidance from the IAEA recognizes that COTS devices that are used in mechanical or electrical systems may not be considered as an I&C device. Users and assessors of these COTS devices may not be aware that these devices could be considered as an I&C device or that the device has an embedded digital component. Because the device function remains the same, the product literature and part number for the device may not be revised to reflect this change. If the digital subcomponent(s) are not identified, its (their) digital/software quality would not be assessed, and the component (i.e. COTS device) may have new failure mechanisms and modes that were not considered. This may also be referred to as *COTS with undeclared content*. This challenge is beyond the scope of the digital COTS justification process, but the IAEA COTS document cites NRC RIS 2016-05 and EPRI 3002008010 as two sources of information associated with this challenge.

6.11 International Electrotechnical Commission (IEC)

The IEC leverages IAEA safety guides to provide overall design principles for I&C systems. IEC standards must account for the regulations of all member states (62 full members, 26 associate members, 88 total members).

IEC standards are integral in the development of other standards in many industry standards as many industries have adopted the IEC standards outright or modified the standards to meet their specific needs. Table 6-12 and Figure 6-1 provide a listing of some industry standards and their relationship to IEC 61508.

Table 6-12 Industries that Use IEC Standards as a Basis

Standard	Industry	Use
IEC 61508	Non-Industry Specific	IEC 61508 provides guidance for safety-related systems. Large market sectors for sub-system/system suppliers conform to IEC 61508. Compliance with the standards in other sectors facilitate consistency with the requirements of IEC 61508.
IEC 61511	Process industry	IEC 61511 has been developed as a process sector implementation of IEC 61508
IEC 61513	Nuclear power	IEC 61513 provides an interpretation of the general requirements of IEC 61508-1, IEC 61508-2, and IEC 61508-4 for the nuclear application sector
IEC/EN 62061	Control systems for machinery	IEC/EN 62061 is an industry-specific adaptation of IEC 61508
IEC 62671	Nuclear power	IEC 62671 provides requirements for determining whether digital devices of industrial quality, that are of dedicated, limited and specific functionality and limited configurability, are suitable for use in a nuclear application.
EN 5012X	Railways	EN 5012X is an industry-specific adaptation of IEC 61508
ISO 26262	Automobile	ISO 26262 is a derivative of IEC 61508 and is an industry-specific adaptation of IEC 61508
ISO/IEC 62304	Medical devices	ISO/IEC 62304 is an industry-specific adaptation of IEC 61508
ISO 13482	Robots	ISO 13482 adopts the approach in IEC 62061 to formulate a safety standard for robots and robotic devices in personal care to specify the conditions for physical human- robot contact. ISO collaborates closely with the IEC on all matters of electrotechnical standardization
ISO 13849	Control systems for machinery	ISO 13849 Part 1 and IEC 62061 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. ISO collaborates closely with the IEC on all matters of electrotechnical standardization
ISO/TR 23849	Control systems for machinery	ISO/TR 23849 provides guidance on the application of ISO 13849 Part 1 and IEC 62061 in the design of safety-related control systems for machinery

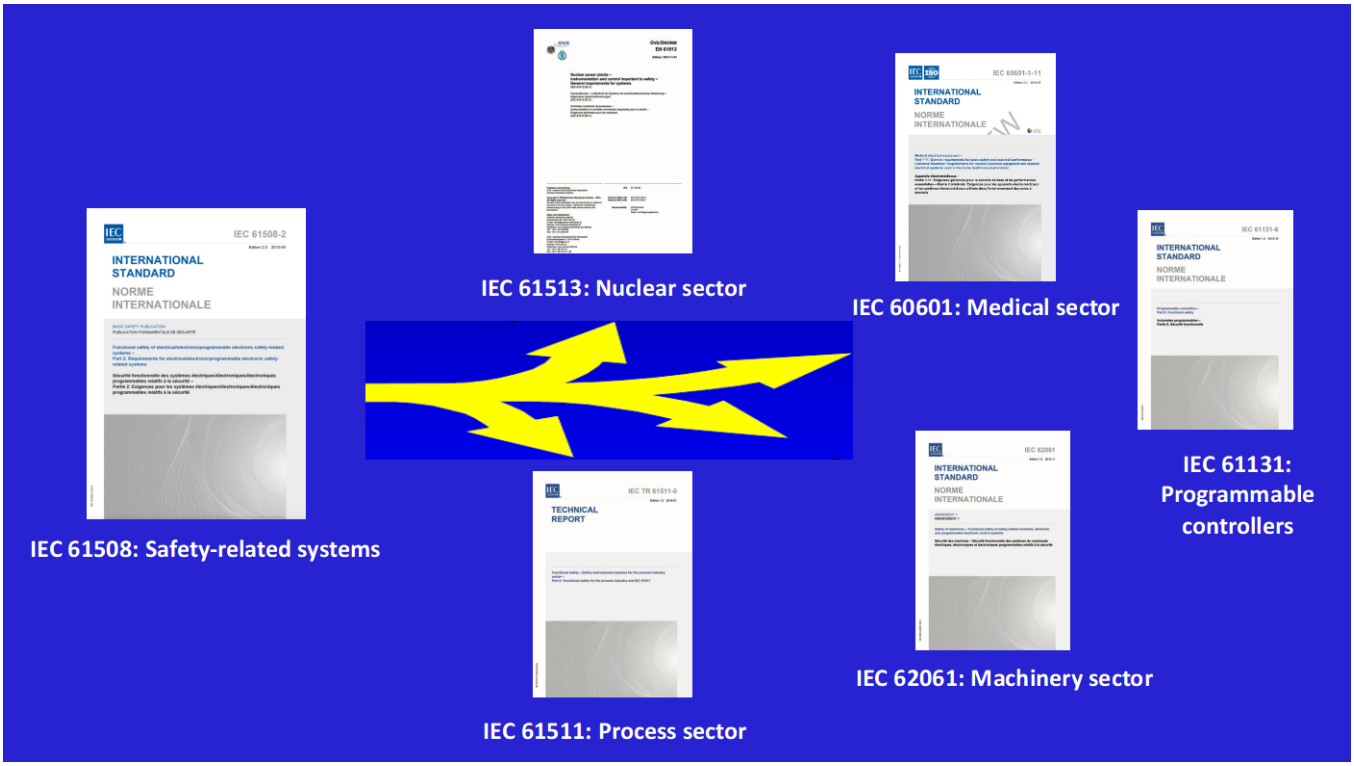


Figure 6-1 Generic and Application Sector Standards for IEC Standards Cover the Entire Lifecycle of I&C Systems in Many Industries

The IEC standards, and standards based on the IEC standards, used in process industries and foreign NPPs, are performance based and can provide a graded approach at the device level. More specifically, IEC 61511-2 [202] states that "IEC 61511 series is performance based, and that many approaches can be used to achieve compliance." IEC 61508 is considered to be performance-based because it avoids prescriptive rules, such as redundancy and self-test capability standard for the functional safety of equipment [276]. Similarly, ISA TR84.00.02-2015 [205] states that "The approaches outlined in this document are performance-based; consequently, the reader is cautioned to understand that the examples provided do not represent prescriptive architectural configurations or MI requirements for any given SIL." Conversely, the U.S. nuclear industry has traditionally used a prescriptive method to determine the safety significance of a system and its impact on the severity of risk. As written, the 10 CFR 50 Appendix B/CGD approach for safety-related components is not readily transferrable to cross-walking quality standards to the different IEC SILs or to the application of a graded approach. However, reviewing the use of probabilistic, performance-based system analysis and the graded approach for achieving functional safety provided in the IEC standards can provide insights into the use of IEC SIL certified components and how they could fit into the NRC regulatory structure.

The guidance provided in key international IEC standards constitutes the basis for an overall approach to designing I&C systems important to safety. IEC 61508 [194] provides guidance for safety-related systems. Large market sectors for sub-system/system suppliers conform to IEC 61508. Compliance with the standards in other sectors facilitate consistency with the requirements of IEC 61508. The process industry uses IEC 61511 [195]. IEC 61513 [79] represents the high-level guidance addressing I&C system architecture considerations in the nuclear sector; IEC 60880 [81] supplements that guidance by specifically addressing software-based system considerations; IEC 62340 [302] provides a framework for establishing a CCF

coping strategy that is consistent with the high-level requirements in IEC 61513 and complementary to the software requirements in IEC 60880.

IEC 61508 is based on two fundamental concepts [276]:

- safety lifecycle, which uses probabilistic, performance-based system analysis and design to minimize random failures and an engineering process to minimize systematic faults resulting from design and documentation errors

- SILs, which are used to implement a graded approach to achieving functional safety (with respect to both random and systematic failures)

IEC 61508-7 [303] provides a risk-based approach for determining the required performance of safety systems and provides generic requirements that can be used directly by industry or can be used as a basis for developing application-specific sector standards. This is arrived at by determining the severity of the risk associated with the hazard and assessing the frequency of the hazard and the protection to be provided by the system to reduce the risk from the hazard to a tolerable level.

IEC 61508 defines *safety* as a freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly, as a result of damage to property or to the environment. IEC 61508 defines *functional safety* as that part of safety that depends on a system or equipment operating correctly in response to its inputs. The safety lifecycle includes activities necessary to achieve the required functional safety for the functions executed by the electrical, electronic, and programmable electronic (E/E/PE) safety-related systems.

The use of IEC SILs allows correlation of expected quality standards to each SIL. A categorization framework or methodology is needed to map specific applications and equipment functions to the appropriate SIL. IEC 61508-5 [304] provides examples of how this can be accomplished. Once this framework is established, the QA sufficiency can be determined through the following approach:

- A specific SIL has been determined to be appropriate for the application.

- The equipment selected for the application has been determined to meet the requirements of that same SIL.

- Since meeting the requirements of the SIL includes satisfying the systematic integrity requirements, and since QA is an aspect of systematic integrity, it can be concluded that the QA used by the manufacturer to design and produce the equipment is adequate.

Components based on IEC 61508 are not directly applicable to NPPs. Differences in dedication also need to be understood. IEC 62671 [17] provides requirements for determining whether digital devices of industrial quality, that are of dedicated, limited and specific functionality and limited configurability, are suitable for use in a nuclear application. IEC 62671 states that “IEC 61508 can be used as complementary guidance for the evaluation and assessment of components [for use in the nuclear industry], but it is recognized that certification to non-nuclear standards alone is insufficient.” It is also important to remember that devices addressed by IEC 62671 are dedicated devices of limited, specific functionality. This statement most likely recognizes the lack of clear mapping between the prescriptive nuclear requirements and the

performance-based requirements of IEC 61508. It also reflects the concept that IEC 61508 requirements may not address nuclear-specific environmental concerns.

Although IEC 61508-1 does not require that the competence of personnel involved in functional safety assessments be formally authorized or accredited [276], most end-users who purchase IEC 61508 certified equipment demand that product certifications be done by a highly competent technical organization with accreditation from an Accreditation Body (AB) that is a member of the International Accreditation Forum (IAF) [305]. IAF membership includes more than 70 countries that are signatories of the IAF Multi-Lateral Agreement (MLA), which recognizes the equivalence of other member's accreditations. There is a designated International Accreditation Forum (IAF) member entity in each country that performs accreditation. In the United States, ANSI is the national accreditation body. In the Federal Republic of Germany, it is the Deutsche Akkreditierungsstelle (DAkkS). Thus, IAF member accreditations are valid in most countries of the world.

The body for certifying items to IEC 61508 is accredited by a national accreditation body. Accreditation bodies must meet ISO/IEC 17011 [306], which specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies. ISO 17065 [307] specifies requirements, the observance of which is intended to ensure that certification bodies operate certification schemes in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of certified products, processes and services on a national and international basis and so furthering international trade.

IEC 60880 [81] specifies requirements for achieving highly reliable software, covers all software life cycle activities, and together with IEC 61508, it can serve as the basis for certification of safety critical software for use in NPPs. It addresses each stage of software generation and documentation, including requirements specification, design, implementation, verification, validation and operation. Like other IEC standards, IEC 60880 is results oriented (i.e., performance based) rather than prescriptive, with a minimum set of V&V activities to be performed for each phase of development. Criteria within this standard are the resulting characteristics of the safety system.

With respect to the use of software tools, IEC 60880 requires documentation of tool use, adequate training on tool use, and verification of software tools to a level consistent with its reliability requirements, the type of tool, and the potential of the software tool to introduce faults. IEC 60880 and IEC 62138 [82] identify types of software tools that require different levels of verification and assessment. IEC 60880 does not require qualification of a software tool if the tool cannot introduce faults into the software, if the tool output is always systematically verified, or if tool faults are mitigated. IEC 62138 considers software tools to be support system software that is part of the system software in a typical I&C system and is either off-line or on-line (i.e., embedded in nonsafety support systems). Its requirements for software tools are consistent with but less rigorous than the IEC 60880 requirements. IEC 62138 focuses efforts on tool certification and the certification of the tool development process rather than a rigorous tool qualification process.

IEC 60987 [80] for computer hardware recognizes that software that is not firmware should be developed or assessed according to the requirements of the relevant software standard (that is, IEC 60880 for Class 1 systems and IEC 62138 for Class 2 systems).

IEC 61226 [175] establishes a method of classification of I&C systems and equipment according to their importance to safety. The classification of I&C functions depends on their contribution to

the prevention and mitigation of postulated initiating events. The resulting classification is then used in IEC 60880 and IEC 62138 to determine relevant specification and design requirements including qualification requirements for software tools used to develop I&C software and systems important to safety.

IEC 61513 [79] addresses hardware robustness and provides requirements for security at the level of the I&C architecture and of an individual I&C system. IEC 61513 allows I&C systems important to safety of classes 1, 2 and 3 to be implemented using conventional hard-wired equipment, digital technology equipment (computer based or programmed hardware) or by using a combination of both types of equipment. This international standard provides the acceptance criteria for the selection, evaluation, and use of certain digital devices that have not been developed specifically for use in these nuclear I&C systems.

IEC 61513 has been implemented by the nuclear industries in some countries, mostly in Europe, but this standard breaks from the performance-based requirements for systematic integrity and the probabilistic approach to reliability [308]. It points to other standards such as IEC 60880, IEC 62138, and IEC 60987 that implement a very prescriptive and deterministic approach that is very similar to the IEEE suite of standards (e.g. IEEE 603, IEEE 379, IEEE 7-4.3.2).

IEC 62671 [17] provides requirements for determining whether digital devices of industrial quality that were not developed specifically for use in nuclear I&C sytems are of dedicated, limited, and specific functionality and limited configurability are suitable for use in a nuclear application. This standard recognizes that devices addressed by this standard are dedicated devices of limited, specific functionality that contain or may contain components driven by software or digital circuits designed using software-based tools. Examples are smart sensors, valve positioners, and electrical protective devices or inverters that contain or may contain components driven by software or digital circuits designed using software-based tools. The IEC 62671 standard focuses on addressing the evaluation process, the elements of functionality and other requirements that shall be evaluated, the criteria for providing confidence in the correctness of the design and manufacture of the device, criteria for the integration of the device into a plant I&C system, and considerations for preserving the acceptability of the device. Thus, this standard is similar to a CGD facility dedicating a CGI for use in an NPP.

IEC 62671 [17] does not address the software aspects of complex general-purpose devices that are addressed by other standards such as IEC 60880 and IEC 62138 for software. This standard addresses the issues that should be considered when evaluating the suitability of these dedicated devices of limited, specific functionality for use in an NPP. The intent is to apply a graded approach to these issues, with more demanding requirements applied for higher classes.

Two other IEC standards are worth mentioning. The first, IEC 62098 [309], covers evaluation methods for microprocessor-based instruments. The second, IEC 60770-3 [310], provides guidelines for the evaluation of intelligent transmitters, including fault-injection testing.

The same components are typically certified for use in many other countries. For example, a specification sheet may list, among others, CSA (Canadian Standards Association, Canada), ATEX (equipment for potentially explosive atmospheres, Europe), KGS (Korea Gas Safety, Korea), etc., to indicate that the product is certified for use in those countries. These certifications are generally the same as the IEC certifications. IEC certification can include specifying one of the four IEC 61508 SIL levels or classifying the component based on its safety in accordance with IEC 61226. A product assessment performed according to the requirements of IEC 61508 must include hardware probabilistic failure analysis, quality system evaluation, and an assessment of all

fault avoidance and fault control measures during hardware and software development. Because many vendors also supply many other industries, they also cite compliance with ISO 9001 [311] for its QA program. Thus, it can be assumed that manufacturers that can achieve IEC SIL 2, 3, or 4 certifications can be assumed to have a complete, fully implemented QA program [157]. Although not necessarily a QA program that fully meets the requirements of Appendix B as per SECY-03-0117 which reviewed ISO 9001-2000 against the existing framework of Appendix B and concluded that ISO 9001 does not meet the requirements of Appendix B [52].

6.11.1 Process Industries

IEC 61508 [194] and IEC 61511 [195] are currently the most widely used standards addressing the use of software in the process industry. IEC 61508 is used by manufacturers and suppliers to certify platforms and equipment, and IEC 61511 is used by designers, integrators, and end-users to certify applications of safety instrumented system. These standards address sensor software, even though its inclusion in the introduction of IEC 61508-7 [303] is rather indirect:

> *In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with E/E/PE [electrical, electronic, and programmable electronic] safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.*

Opposed to this, IEC 61511-1 [195] is very clear in its introduction:

> *The SIS [safety instrumented system] includes all devices necessary to carry out each SIF [safety instrumented function] from sensor(s) to final element(s).*

Thus, IEC 61511 addresses the application of safety instrumented systems for the process industries, including sensors, logic solvers, and final elements.

Part 3 of IEC 61511 (ISA 84.00.01) and Part 5 of IEC 61508 describe methodologies that can be used to classify safety equipment. These methodologies all correlate an increase in requirements (higher IEC SIL) with the importance of the specific safety system to the overall safety of the plant (risk based, probabilistic). There are both qualitative and quantitative methods that are appropriate for certain types of systems and situations.

The IEC standards provide for device ratings by manufacturers. IEC 61508 has 4 SIL levels that are based on the probability of failure per hour (PFH) of operation. Each higher SIL value is a factor of 10 improvement in reliability. SIL-1 defines a probability of failure on demand (PFD) range of 10^{-1} to 10^{-2} or a risk reduction factor of 10 to 100. Table 6-13 and Table 6-14 show what this means in failures per year.

Table 6-13 Maximum Accepted Failure Rates Based on SIL for Low Demand Systems

SIL	PFD	Failure rate of safety system
SIL 1	10^{-2} pfd 10^{-1}	One failure in 10 years
SIL 2	10^{-3} pfd 10^{-2}	One failure in 100 years
SIL 3	10^{-4} pfd 10^{-3}	One failure in 1,000 years
SIL 4	10^{-5} pfd 10^{-4}	One failure in 10,000 years

Table 6-14 Maximum Accepted Failure Rates Based on SIL for High Demand Systems

SIL	PFH (per h)	Failure rate of safety system
SIL 1	10^{-6} pfh 10^{-5}	One failure in 100,000 h
SIL 2	10^{-7} pfh 10^{-6}	One failure in 1,000,000 h
SIL 3	10^{-8} pfh 10^{-7}	One failure in 10,000,000 h
SIL 4	10^{-9} pfh 10^{-8}	One failure in 100,000,000 h

A low demand mode on a safety system translates to a demand on the safety system not more frequently than once per year. Exida relates low demand mode to the proof test interval where the demand interval for operation made on a safety-related system is greater than twice the proof test interval [312]. Low demand mode (on demand) is typically found in the process industry [188]. A typical example is an emergency shutdown system that only becomes active when the process becomes out of control. This normally occurs less than once a year.

A high demand mode (i.e., high demand rate or continuous demand) on a safety system translates to a continuous demand on the safety system or a demand that occurs more frequently than once per year.

Exida has a different definition of high demand mode that is intended to give credit to frequent diagnostics. High demand mode is where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safety state is part of normal operation [312]. High demand mode (continuous mode) is mainly used in production engineering [188]. Continuous monitoring of working processes is frequently required to guarantee the safety of the workers and the environment.

Many industries use IEC SILs for meeting probability of failure on demand-average (PFDavg) or risk reduction factor (RRF). IEC SIL-1 represents the lowest risk-reduction level of performance; SIL-4 represents the highest risk-reduction level of performance. ISA 84.00.01 notes that SIL-4 is not used in the process industry sector because it requires elaborate systems and is difficult to support because of the high level of reliability required of the hardware. SIL-4 systems are not expected to be used for safety system controls in DOE facilities or in the process industries. For the process industry, SIL 4 is not to be required for a SIS. Non-process control measures are needed to reduce the risk to at least SIL 3 [313].

The following passages discuss the approaches used by IEC 61508 and IEC 61511, respectively.

Rating in accordance with IEC 61508: the definitions of IEC 61508 cover the complete product lifecycle from initial concept up to discontinuation of a product. In order to develop a component according to this standard, appropriate procedures and additional technical measures must be taken and verified from development through production. This often makes the development of a failsafe product more expensive than that of a standard component without SIL certification.

Rating in accordance with IEC 61511 (operational proof): currently there is only a limited number of devices which have been certified in accordance with the IEC 61508 standard. In order to allow a practicable selection of devices, the possibility of operational proof for devices has been permitted in IEC 61511.

Operational proof in IEC 61511 means that evidence must be provided to show a sufficient number of units in the field and include data on the operating period and conditions of use. A minimum period of use is 1 year, with a specified number of operating hours. The operational proof only applies to the version/release of the product for which the proof has been provided. All future modifications of the product must subsequently be carried out in accordance with IEC 61508.

The IEC SIL standard requires a functional safety assessment to be carried out on all parts of the safety-related system and for all phases of the lifecycle (see clause 8 of IEC 61508-1). The level of independence required of the assessor ranges from an independent person in the same organization for SIL 1 to an independent organization for SIL 3 / 4 (Table 6-15). In all cases, there is a specific requirement that the assessor be competent for the activities to be undertaken.

Table 6-15 Review Independence Based on IEC SIL [188]

IEC SIL 1	Independent person
IEC SIL 2	Independent department
IEC SIL 3	Independent organization
IEC SIL 4	Independent organization

Instruments that are fully compliant with IEC 61508 address systematic faults through a full assessment of fault avoidance and fault control measures during hardware and software development. There are three main parts to IEC 61508 which specify these requirements:

- Part 1 addresses the overall functional safety management of the product.
- Part 2 covers the hardware requirements, including achievement of failure rates and diagnostic coverage, as well as specific techniques and measures for avoidance of systematic failures.
- Part 3 covers the software requirements and is primarily focused on the process used when developing the software, including specific use of techniques, design, and coding standards and analysis and testing techniques.

Guidance from IEC 61511/IEC 61508 would place EDDs/components that perform HMI, diagnostics, and monitoring as IEC SIL 1, 2, or 3 based more on the system the component is in

rather than its functionality. This is consistent with how regulators in foreign countries assess IEC SIL levels. That is, the lower IEC SILs are applied to low risk situations.

Most smart sensors/actuators have a minimal operating system that handles interrupts and performs simple task scheduling; sometimes features such as priority scheduling, logging into files on flash, or emulating virtual memory are added. The application software layer, using these basic capabilities, implements the application-specific functionality, which of course varies considerably. These limited functionality EDDs may be referred to as simple devices in the process industry.

It is interesting to note that a smart device may be certified to different SILs depending on its use. For example, the Fisher FIELDVUE DVC 6200 digital valve controller can meet the hardware requirements of IEC SIL 3 and the position monitor can meet the hardware requirements of IEC SIL 2 [312]. The software for the diagnostic function and transmitter / limit switch configurations are limited to SIL 2.

Basing the classification of the device on the safety class of the system in which it is installed may not match the consequences of its failure for those devices with limited functionality (i.e., monitoring, diagnostics, or HMI), especially if its failure does not impact the functionality of the component or system.

6.11.2 SIL Comparisons

Safety-critical software requires a robust process of development, verification, configuration management, and QA processes. These processes are regulated by standards such as IEC 61508 [194] industrial control equipment manufacturers, EN 50128 [314] for railway equipment, ISO 26262 [72] for automobiles, ISO/IEC 62304 [315] for medical devices, and RTCA DO-178C [316] for airborne software. Many standards base the integrity of the software to the safety integrity level (Table 6-16).

Table 6-16 Comparison of SILs for Different Industries [327]

Safety level	Safety Level			
	IEC 61508 Automotive SIL	EN 50128 Software SIL	ISO 26262 SIL	ISO/IEC 62304 Class
highest	4	4		
	3	3	D	C
			C	B
	2	2		
		1	B	A
lowest	1		A	
	0			

ISA 84.00.01 (the process industry daughter standard to IEC 61508) notes that the application of SIL 4 criteria is considered very unusual in the process industry and recommends redesigning the system to reduce its safety significance to a lower SIL before continuing on an effort to implement a system at SIL 4. It is further noted that SIL 4 is considered to be very difficult to achieve and maintain.

Translating the IEC SILs to safety/not safety for NRC has not been performed. The approval of the RadICS platform shows the difficulty in licensing and approving a digital control system platform solution for safety-related applications in NPPs that was based on IEC 61508 SIL 3. In its review [144], that NRC states "Though functional safety assessments were performed to demonstrate RadICS platform compliance with IEC 61508 SIL 3 certification requirements, the NRC's regulatory framework does not include the SIL compliance approach." Where possible, the NRCs review compared the IEC methods to endorsed IEEE standards. For example, the SER stated that "The SER recognizes that the FMEDA methods used were found to be consistent with IEEE Standard 379 2000 as endorsed by RG 1.53 Rev. 2." In other parts, the NRC required CGD of the platform because "the RPC Radiy QMS [Quality Management System] has not been assessed by the NRC staff to be compliant to 10 CFR Part 50, Appendix B." It would be interesting and likely helpful to understand how the IEC SIL 3 conforms to the NRC's safety classification.

6.12 Institute of Electrical and Electronics Engineers (IEEE)

IEEE has more than 419,000 members in over 160 countries. IEEE standards may be required by the NRC by regulation (i.e., IEEE Std. 603-1991) or endorsed as providing an acceptable method for for complying with the Commissions' regulations (i.e., 43 IEEE standards are endorsed by NRC Div. 1 regulatory guides [317]).

The clauses in IEEE standards are applicable at the component and system levels, depending on the clause. For EDDs, the most applicable standards are IEEE Std. 603, IEEE Std. 7-4.3.2, and IEEE Std. 1012 (currently endorsed in their 1991, 2003, and 2004 versions respectively).

IEEE 7-4.3.2-2016 [26] provides specific requirements for programmable digital devices to supplement the criteria and requirements of IEEE Std. 603-2009 [318]. Subclause 5.17 in IEEE 7-4.3.2-2016 requires that previously developed systems be qualified using a dedication process for a CGI. Annex C (informative) provides guidance for dedicating a CGI, including consideration of hardware, software, or firmware failures (i.e., hazards that could interfere with accomplishing the safety function). IEEE 7-4.3.2-2016 requires that software be developed, modified, or accepted in accordance with an SQA plan and that the plan shall address the software tools used for system development and maintenance.

IEEE Std. 1012-2004 [209], endorsed by Regulatory Guide 1.168, Rev. 2 [319], defines four software integrity levels (IEEE SILs (Table 6-17), not to be confused with the IEC safety integrity levels [SILs]. NRC endorses this standard for V&V, reviews, and audits of software used in safety systems. However, RG 1.168 states that software used in NPP safety systems should be assigned SIL 4 or the equivalent, as demonstrated by a mapping between the applicant or licensee approach and SIL 4 as defined in IEEE Std. 1012-2004. Thus, although four IEEE SILs exist, only SIL 4 is applied to safety systems in NPPs. Although not currently used in the licensing of NPPs, the different IEEE SILs provide a graded approach to software development.

Although there are four integrity levels, the newer version of IEEE-1012-2016 no longer uses the "SIL" terminology to avoid confusion with the much more widely used IEC-61508 context; rather, IEEE 1012-2016 refers to integrity levels. IEEE 1012-2016 is part of a much larger portfolio of lifecycle standards and using a V&V standard in isolation without a full discussion of the lifecycle may have unintended consequences. Lastly, IEEE 1012-2016 adopts modern systems engineering that includes an integrated view of hardware and software. IEEE 1012-2016 is currently not endorsed by NRC, but the differences between the -2004 and -2016 version are noted in the -2016 version to avoid confusion.

Table 6-17 Four-level Software Integrity Scheme in IEEE Std. 1012-2004

IEEE Std. 1012 SIL	Consequences	Mitigation
4	Grave	No mitigation
3	Serious	Partial to complete mitigation
2	Minor	Complete mitigation
1	Negligible	Mitigation not required

Annex B (informative; not endorsed) of IEEE Std. 1012-2004 provides an example of a risk-based, four-level integrity scheme. The risk-based scheme, shown in Table 6-18, assigns a software integrity level based upon the combination of an error consequence and the likelihood of occurrence of an operating state that contributes to the error. Some table cells reflect more than one software integrity level, indicating that the final assignment of the software integrity level can be selected to address the system application and risk mitigation recommendations. For some industry applications, the definition of *likelihood of occurrence categories* may be expressed as probability figures derived by analysis or from system requirements.

Table 6-18 Graphic Illustration of the Assignment of Software Integrity Levels (*Source*: IEEE Std. 1012-2014, Table B.3)

Error	Likelihood of occurrence of an operating state that contributes to the error (decreasing order of likelihood)			
Consequence	Reasonable	Probable	Occasional	Infrequent
Catastrophic	4	4	4 or 3	3
Critical	4	4 or 3	3	2 or 1
Marginal	3	3 or 2	2 or 1	1
Negligible	2	2 or 1	1	1

This standard applies to software being acquired, developed, maintained, or reused (legacy, modified, COTS, non-developmental items [NDIs]). The term *software* also includes firmware, microcode, and documentation. In many instances, the consequence/mitigation SIL definitions are applied, while the risk-based SIL levels are informative.

It is unknown if and to what extent IEEE standards are used in industry outside the nuclear arena. Many of the standards, such as IEEE Std. 1012, are used for software development at NPPs. However, the IEEE Std. 1012 working group stakeholders include vendors that supply both the nuclear industry and other entities in DOE, DoD, NASA, aerospace, NNSA, and universities.

When conducting V&V of a system, software, or hardware element, IEEE Std. 1012 states that it is important to examine the interactions with the system of which the element is a part. When performing V&V of an EDD, one should ask how it fits into the system.

The V&V processes for the software in an EDD will be similar to that for the software in a system.

As far as licensing is concerned, the software in EDDs presents many aspects similar to those for the development of software or the use of pre-existing software. Thus, several issues, common positions, and recommended practices for software in general also apply to the development of software in EDDs.

When validating the software in an EDD, assessments will be performed on a specific version of the device and the associated software. However, if the supplier changes its product (e.g., the software version), then the EDD should undergo another validation process. Thus, similar to system software, a process must be established to ensure that the software installed in the EDDs is the same version as those subjected to the validation process. In addition, a supplier could upgrade a product from a conventional device to one with embedded software without the end user being aware of this change. A process must be established to ensure that such changes are detected and that the EDD is subjected to assessment.

Quality of the software development process, such as using IEEE SILs as defined in IEEE Std. 1012, are used by Korea in evaluating EDDs.

6.12.1 IEEE WG 6.6

IEEE working group WG 6.6 “Intelligent Digital Devices,” was formed in 2012 as part of an effort by the IEEE Power and Energy Society (PES), Nuclear Power Engineering Committee (NPEC), Subcommittee 6 “Safety Related Systems,” to identify areas for development of new standards. WG 6.6 was formed to develop guidance on the use of intelligent digital devices (IDDs) in NPPs.

WG 6.6 started work on IEEE P1891 [320] with the scope of addressing IDDs in safety-related applications. The scope of P1891 evolved over the years to also cover simple and complex IDDs in augmented quality and nonsafety related applications, using a graded approach. WG 6.6 has recently narrowed the scope of their activities to focus on simple devices or devices of limited functionality for use in safety-related applications. The new standard will address certain devices that contain embedded software or electronically-configured digital circuits used in systems and equipment important to safety in nuclear power plants. It will provide requirements for the selection and evaluation of such devices where they have dedicated, limited, and specific functionality and limited configurability. There are similarities in scope between the current WG6.6 work and IEC 62671. WG6.6 is currently engaging IEC to pursue a Dual Logo standard with IEC 62671.

6.13 International Society of Automation (ISA)

ISA has adopted several IEC standards for use in automation and control systems. ISA has over 150 consensus industry standards.

ANSI/ISA-84.00.01-2004 is an identical adoption of IEC 61511, with the addition of a grandfather clause to accommodate existing SIS installations. The only modification to IEC 61511 for adoption as a U.S. standard (i.e., ANSI/ISA-84.00.01-2004 [IEC 61511-1 Mod]) was reference to the United State's handling of legacy systems (i.e., the grandfather clause).

DOE and OSHA cite the ANSI/ISA 84.00.01-2004 standard rather than IEC 61511.

ANSI/ISA 84.00.01-2004 Part 1 (IEC 61511-1 Mod) [76] provides several methods for determining SILs, such as layer of protection analysis, which uses frequency of the event as a basis, or safety layer matrix, which uses available information of IPLs as a basis for selection of SILs for the SISs.

ANSI/ISA 84.00.01-2004 is used by the process industries for designing reliable SISs that are commensurate with the level of hazard mitigation or prevention strategy.

The evaluation approaches outlined in ISA-TR84.00.02-2002, Part 2 [321] are performance-based approaches and do not provide specific results that can be used to select a specific architectural configuration for a given SIL.

6.14 International Organization for Standardization (ISO)

ISO collaborates closely with the IEC on all matters of electrotechnical standardization.

With respect to quality, many industries cite compliance with ISO 9001:2015. This standard includes requirements for leadership, planning, support, operation, performance evaluation, and continual improvement.

The automotive industry cites compliance with ISO 26262 [72]. ISO 26262 is an international standard for functional safety of electrical and/or electronic systems in production automobiles. ISO 26262 is a derivative of IEC 61508, and similar to IEC 61508, is risk-based, where the risk of hazardous operational situations is ***qualitatively*** assessed, and safety measures are defined to avoid or control systematic failures and to detect or control random hardware failures or mitigate their effects.

ISO 26262 contains requirements for software integration and testing to demonstrate that the software architectural design is realized by the embedded software. ISO 26262 also contains requirements for the verification of software safety requirements to demonstrate that the embedded software fulfils the software safety requirements. The -2018 version of ISO 26262 includes guidance for software tool selection, use, documentation, and qualification.

Unlike the IEC standards with SILs 1–4, ISO 26262 uses four ASILs, A through D, to tailor the requirements of ISO 26262 to avoid unreasonable residual risk. ISO 26262 requires software to be assigned to one of four ASIL categories on the basis of the system ASIL and the level of risk associated with the use of the software in the system.

6.15 The National Aeronautics and Space Administration (NASA)

The consequence-based approach in NASA-GB-8719.13 [208] (NASA-GB-8719.13 supersedes NASA-GB-1740.13) evaluates the consequences of the device failure and its impact on the system. NASA-GB-8719.13 encourages the use of simulators or an in-circuit emulator (ICE) system for debugging in embedded systems because these tools allow the programmer or tester to find some subtle problems more easily. However, the guidebook does not discuss simulator or ICE system verification, validation, qualification, review, or approval practices.

NASA-STD-7009 [242] provides an approved set of requirements, recommendations, and criteria with which models and simulations (M&S) may be developed, accepted, and used in support of NASA activities. NASA does not provide specific verification, validation, or qualification

requirements for most COTS, GOTS, or MOTS software tools and expects automatically generated code to be treated to the same level as hand-generated code [67].

6.16 Nuclear Energy Agency (NEA)

The NEA is an agency within the Organisation for Economic Co-operation and Development (OECD). The NEA's current membership consists of 33 countries in Europe, the Americas, and the Asia-Pacific region. The goal of the NEA in the area of nuclear safety technology and regulation is to assist member countries in ensuring high standards of safety in the use of nuclear energy by supporting the development of effective and efficient regulation and oversight of nuclear installations and by helping to maintain and advance the scientific and technological knowledge base. All NEA members are also IAEA members.

MDEP was established in 2006; the nuclear regulatory authorities of 16 countries participate in MDEP. The NEA facilitates MDEP activities by providing technical secretariat services. This is a multi-national initiative to leverage resources and knowledge of national regulatory authorities tasked with regulatory design review for new reactors.

MDEP Common Position CP-DICWG-07 [15] (MDEP Generic Common Position #7) addresses using industrial digital devices of limited functionality in systems important to safety but that have not been developed specifically for use in nuclear power applications. The definition of a *digital device of limited functionality*, taken from IEC 62671, excludes PC, PLCs, etc. MDEP recognizes that the worldwide nuclear power industry is increasingly interested in using industrial digital devices of *limited functionality* [emphasis added] in systems important to safety, but that have not been developed specifically for use in nuclear power applications. Some of these devices are found embedded in plant components and actuating devices such as sensing instrumentation, motors, pumps, actuators, and breakers. MDEP does not consider complex devices such as those that use commercial computers (PCs, PLCs) to be industrial digital devices of limited functionality.

MDEP's Vendor Inspection Cooperation Working Group (VICWG) [322] is focused on evaluating opportunities to maximize the use of results from international regulator efforts at vendor facilities [323] that includes

1. Developing a common QA quality control (QC) criteria document for use by multi-national regulatory bodies conducting joint inspections

2. Developing an inspection protocol for implementation of multi-national inspections

3. Completing several inspections with support by international regulators (both domestically and abroad)

Its first multi-national inspection was scheduled for July 2014 using the protocol and common QA/QC criteria documents with Valinox in Montbard, France (SG tube manufacturer).

NEA/CNRA/R(2014)7 [248] reports on the survey on the design review of new reactor applications. These are to serve as guides for regulatory organizations to understand how technical design reviews are performed by member countries. The licensing process surveys are based on IAEA Safety Guide GS-G-4.1. This volume—Volume 1—is focused on I&C. Survey responses were provided by 11 countries—Canada, Finland, France, India, Japan, Republic of Korea, Russian Federation, Slovak Republic, Slovenia, Sweden, and the United States.

Standards cited by the various countries for regulating NPPs include those by CSA, ISO, IEC, IAEA, IEEE, and AERB.

6.17 Nuclear Energy Institute (NEI)

The NRC is currently evaluating the sufficiency of the NEI's proposed guidelines for digital modifications, cyber security controls, and CCFs:

- NEI 96-07, Appendix D [224]
- NEI 13-10, Rev. 5 [90]
- NEI 17-06 (still in draft) [308]

NEI 96-07, Appendix D may eventually supersede the supplemental RIS 2002-22. [Regulatory Guide 1.1.187, Rev. 2, published in June 2020, endorses NEI 96-07, Appendix D, Revision 1, as a means for complying with the requirements of 10 CFR 50.59 when conducting digital I&C modifications, subject to clarifications.]

The Nuclear Energy Institute (NEI) has a working group focused on Modernization Plan (MP) #3-Commercial Grade Dedication. This working group is leveraging EPRI 3002011817 [276] to specify a third-party IEC 61508 SIL certification as an alternate approach to determining the acceptability of some of the dependability critical characteristics as defined by EPRI TR-106439. NEI is proposing this alternate method in a new document identified as NEI 17-06. Note that NEI 17-06 is still in draft form and the information in this report may become inaccurate.

Dependability critical characteristics are a special type of characteristic that are specifically associated with programmable digital devices (PDDs), which includes the scope of EDDs. This alternate method is being proposed to be used in lieu of the traditional verification methods of commercial grade surveys (EPRI method 2). The proposal also asserts that the IEC 61508 certification also removed the need for a detailed design review such as a Critical Design Review (CDR) as defined by EPRI 1011710 [78]. The primary basis for this proposal is that the development, manufacturing, and third-party review process involved in a SIL certification encompasses the requirements and activities involved in the performance of a design review and in the use of commercial grade surveys.

The intent of NEI's proposal is to use an existing ecosystem of dependable safety equipment in a manner that reduces lead time and procurement cost.

None of the other regulators reviewed cited an NEI white paper. However, EPRI 3002011817 was written to demonstrate that equipment certified to non-nuclear safety standards (more specifically, IEC-61508/61511) can meet or exceed nuclear power safety and reliability requirements without further analysis or verification; this EPRI document is related to the proposed NEI 17-06.

6.18 National Institute of Standards and Technology (NIST)

NIST special publication (SP) 500-234 [324] contains only a few high-level software tool requirements that deal with V&V and training associated with the health care industry. Both NIST SP 500-234 and IEEE 1012-2012 recommend that an independent V&V (IV&V) team execute qualification tests on tools (e.g., compilers, assemblers, and utilities) shared with the development environment and recommend that the IV&V team should use or develop its own set of test and analysis tools when possible. Both NIST SP 500-234 and IEEE 1012-2012 also state that the

V&V plan should include details for acquiring tools and for training personnel. However, NIST SP 500-234 does not discuss software integrity levels or provide minimum V&V activities as a function of integrity level. NIST SP 500-234 does not distinguish between different categories of tools or use safety as a measure to determine tool qualification requirements.

NIST SP 800-161 [325] provides guidance to federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage their iformation and communications technology (ICT) supply chain risks.

6.19 Office for Nuclear Regulation (ONR)

The UK Office for Nuclear Regulation (ONR) is the regulatory authority that oversees the safety and security at 37 nuclear licensed sites in the UK [326]. The UK generally operates a goal setting regime . This means that ONR sets out broad regulatory requirements, and it is for licensees to determine and justify how best to achieve them, referencing relevant good practice [300]

The key principles considered by ONR inspectors in the review of safety submissions are set out in the SAPs [124]. The key SAP applicable to computer based safety systems is clause ESS.27, which states:

> *Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design.*

The concepts outlined in the key SAPs are then expanded in more detailed TAGs.

The purpose of ONR TAG-046 [126] is to provide additional guidance for applying SAP ESS.27. ESS.27 presents the elements of a multilegged procedure that should be used to demonstrate the adequacy of a computer-based safety system. An important distinction between smart devices and other computer-based systems is that the end user cannot modify or add device functionality to a smart device in any way, though they can usually perform limited configuration. Such devices are still considered as computer-based systems, and therefore their use in safety or safety-related applications should be justified according to SAP ESS.27.

For NPPs, TAG-046 states that IEC 61513 should be considered for assessing software aspects of computer-based systems important to safety as the general requirements for systems (all classes), IEC 60880 for software aspects for systems performing category A functions, and IEC 62138 for category B or C functions. While TAG-046 addresses some hardware-related topics, the IEC standard requirements for computer-based system hardware for NPPs are provided in IEC 61513 and IEC 60987 for class 1 and 2 systems and in IEC 61508 for class 3 systems.

TAG-046 recognizes that IEC 61513 does not provide an explicit link between safety class and IEC SIL as defined in IEC 61508. However, it does acknowledge that there are similarities between the assignment of SILs to safety functions in IEC 61508 and the classification of nuclear safety functions in IEC 61226. ONR has adopted the position outlined in NS-TAST-GD-003 [207] and NS-TAST-GD-094 [328], whereby the system class is aligned to probabilistic targets and deterministic expectations. However, based on the information provided in TAG-046, a relationship between class and IEC SIL can be determined (Table 6-19).

Table 6-19 Relationship Between Safety Class and IEC SIL

ONR TG-046 Class	IEC SIL
1	3 or 4
2	2
3	1

The relationship between safety class, SIL, and numerical integrity target can be subject to some variation. For category A / class 1, the techniques required by IEC 61508 for SIL 4 should be applied, but the licensee can only claim a risk reduction (e.g., in the PSA) of 1E-4 (despite the fact that IEC 61508 allows for down to 1E-5). (This is assuming the hardware reliability supports 1E-4 or better; if it does not, then the claim is limited by the hardware reliability.) For category B / class 2, the initial expectation is that the techniques required by IEC 61058 for SIL2 should be applied, but then the licensee can only claim 1E-2. If the licensee wants to claim 1E-3, it needs to do better than just meet IEC 61508 SIL2. The framework set out in the rest of TAG 46— production excellence represented by the best practice by manufacturer and ICBMs represented by the confidence-building activities performed by the licensee or their agent —is the mechanism to achieve this. (Likewise, for category C / class 3, SIL 1 gives 1E-1 by default; TAG 46 is applied to reach 1E-2.) In practice, the licensees almost always claim 1E-2 for a SIL 1 system, and this should be supported by a good production excellence / ICBM.

Clause 2.6 in TAG 046 describes an approach and references for risk informing. The key concept is that the safety class assigned is related to the risk reduction required. Therefore, identical systems could have very different safety classes due to the lack or presence of other independent systems to mitigate the hazard.

When determining the requirement for the system, ONR expects the deterministic analysis to be the primary means of determining the requirement, particularly for reactor protection, where these functions are well defined in IEC 61226. However, the PSA will often have some relevance in determining the requirement, especially if the system does not fit into the IEC 61226 framework. If the PSA requires lower than 1E-2 but not lower than 1E-3 (e.g., 9E-3), then this equates to a class 2 / SIL 2 system. Likewise, 9E-4 would be class 1 / SIL4, or possibly class 2 / SIL3, depending on deterministic arguments. (Note that ONR does not accept a claim better than 1E-4 for a computer-based system.)

If the PSA holds together with a claim of 1E-2, then, deterministic arguments aside, ONR would accept class 3 / SIL1 and expect good production excellence / ICBM. If the PSA holds together with a claim of 1E-1, TAG 46 states that ONR still expects class 1 / SIL1 (para 5.8); it is only when 3E-1 is needed that ONR would specify that TAG 46 compliance is no longer necessary. In practice, it appears that ONR may rely on third-party assessments and manufacturer pedigree arguments for 1E-1.

Best estimate is used when the PSA is being used to determine safety vulnerabilities and when the overall big picture could be distorted by conservatism just for the computer-based systems. It does not allow a reduction in the techniques expected to justify the numerical claim. When a PSA is driving the integrity requirement, then the PSA requires the high-confidence figures before being established as the requirement for the system.

Appendix 8 of ONR TAG-046 [126] outlines the ONR's expectations for the safety justification of COTS smart devices. Smart devices are instruments, sensors, actuators or other previously electromechanical components (e.g., relays, positioners and controllers), whose *functionality is limited* [emphasis added] and which feature built-in intelligence in the form of a microprocessor or hardware description language (HDL)-programmed device to help perform its function. An important distinction between smart devices and other computer-based systems is that the end user cannot modify or add device functionality in any way, although they can usually perform limited configuration. Such devices are still considered to be computer-based systems, so their use in safety or safety-related applications should be justified according to SAP ESS.27.

Table 6-19 relates the ONR TG-046 Clause 9.9 classes to IEC SIL levels, and Table 6-20 provides a link between categorization, classification, and IEC SIL.

Table 6-20 Link Between Categorization, Classification and SIL (TAG-046, Table 1 [126])

Category & class according to TAG94	IEC 61508 PFD range (high confidence)	IEC 61508 FF range (high confidence)	ONR initial expectation re application of techniques & measures per IEC 61508	Initial acceptable nuclear safety case PFD value or FF (high confidence)	Limit to reliability claim providing relevant assessment criteria was met (high confidence)
Category A / class 1	1E-5 PFD < 1E-3	1E-5 FF < 1E-3	SIL 4	1E-4 *	1E-4*
Category B / class 2	1E-3 PFD < 1E-2	1E-3 FF < 1E-2	SIL 2	1E-2	1E-3
Category C / class 3	1E-2 PFD < 1E-1	1E-2 FF < 1E-1	SIL 1	1E-1	1E-2

*Note the best (minimum) that should be claimed for a computer-based safety system is 1E-4 (high confidence). A claim of 1E-4 (high confidence) should always be delivered by a SIL 4 system.
FF = frequency of dangerous failure per year

One key part of the regulatory process, upon which NS-TAST-GD-046 [126] is based, is that the grading allowed in the guidance impacts the reliability claim that the licensee can take for the device. While ONR does use a best estimate PRA (called *PSA* within their regulatory infrastructure) for certain purposes, when it comes to determining the needed grade of a system, a high confidence value limited as in Table 6-20 must be used. This means that if one device is implemented at a lower grade, then it may result in others being required to be implemented at a higher grade.

Currently, no such reliability feedback mechanism as a consequence of using a graded approach exists within the NRC's regulatory infrastructure.

It should be noted that the high confidence numerical values in Table 6-20 start at 1E-1 and do not exceed 1E-4, even for a SIL 4 system with relevant assessment criteria having been met.

6.20 Occupational Safety and Health Administration (OSHA)

To help ensure safe and healthful workplaces, OSHA has issued the Process Safety Management of Highly Hazardous Chemicals standard (29 CFR 1910.119), that contains requirements for the management of hazards associated with processes using highly hazardous chemicals.

PSM is addressed in specific standards for general and construction industries. OSHA's standard emphasizes the management of hazards associated with highly hazardous chemicals and establishes a comprehensive management program that integrates technologies, procedures, and management practices. OSHA has PSM for different industries [329]:

- Process Safety Management for Petroleum Refineries. OSHA Publication 3918 (2017)
- Process Safety Management for Explosives and Pyrotechnics Manufacturing. OSHA Publication 3912 (2017)
- Process Safety Management for Small Businesses. OSHA Publication 3908 (2017)
- Process Safety Management for Storage Facilities. OSHA Publication 3909 (2017)
- PSM Covered Chemical Facilities National Emphasis Program. OSHA Directive CPL 03-00-021 (January 17, 2017)
- Process Safety Management - Small Business Advocacy Review Panel. OSHA is initiating a Small Business Advocacy Review Panel to get feedback on several potential revisions to OSHA's Process Safety Management Program (PSM) standard
- Petroleum Refinery Process Safety Management National Emphasis Program. OSHA Directive CPL 03-00-010 (August 18, 2009)

The PSM standards are performance-oriented. Therefore, employers have the flexibility in complying with the requirements of PSM, including, among other aspects, the use of recognized and generally accepted good engineering practices. Specific to this review, OSHA stated that ANSI/ISA 84.00.01-2004 Parts 1-3 (IEC 61511 Mod) may be applied under OSHA's PSM standard, 29 CFR 1910.119 [330]. OSHA considers the revised ANSI/ISA S84.00.01-2004 Parts 1–3 (IEC 61511 Mod) to be recognized and generally accepted good engineering practices for SISs. OSHA does not specify or benchmark S84.00.001-2004, Parts 1–3 as the only recognized and generally accepted good engineering practice.

6.21 Federal Railroad Administration (FRA)

The purpose of the Federal Railroad Administration (FRA) is to promulgate and enforce rail safety regulations, administer railroad assistance programs, and conduct research and development in support of improved railroad safety and national rail transportation policy.

The railway industry cites compliance with BS EN 50128 [171], a railway-specific implementation of IEC 61508 that specifies technical requirements for the development of safety-related software for railway control and protection systems. BS EN 50128 [171] and EN 50129 are two European standards (EN 5012x) that define safety-related software process standards, hardware, and approval processes for railway applications. EN 50128 provides process standards for software

for railway control and protection systems. EN 50129 covers safety-related electronic systems for signaling

Even though the safety lifecycles for industry-specific standards such as EN 50128[16] for a railway inherit the definition of *phases* from the generic IEC standard of IEC 61508, the detailed phases of the safety lifecycles for the specific industries are different from IEC 61508.

The railway industry uses a probabilistic risk–based process for safety-related system and software development. This standard requires a systematic approach for safety-related software development to identify hazards, assess risks, and identify risk reduction measures. BS EN 50128 requires software to be assigned to one of five SILs, from SIL 0 (lowest) to SIL 4 (highest), on the basis of the system SIL and the level of risk associated with the use of the software in the system. BS EN 50128 does not use all five levels of safety integrity. Instead, the requirements for SIL 1 and SIL 2 are the same for each technique or measure. Similarly, each technique or measure has the same requirements at SIL 3 and SIL 4. Therefore, effectively, there are recommendations for techniques and measures for only three SILs in BS EN 50128 [67].

The safety-related software SIL and the tables of recommendations for measures and techniques to satisfy the requirements of BS EN 50128 do not impact the selection, use, or qualification of software tools used in the safety-related software development processes.

BS EN 50128 contains requirements and guidance for software tool selection, use, documentation, and qualification. BS EN 50128 also provides a comprehensive process for determining the confidence level in software tools used in the software development process similar to the tool qualification level used in the civil aviation industry. According to ISL [67], BS EN 50128 provides comprehensive, well-organized software tool requirements and guidance.

BS EN 50128 contains several requirements for software tools used in the safety-related software development life cycle process that only depend on the tool functionality. Tools are assigned to one of three classes—T1, T2, or T3—and the tool requirements vary by class.

6.22 In-House Developed Standards

Companies such as Avanceon develop their own standards. According to Avanceon, its in-house developed standards “ensure consistent product and project results, make it easier to support and maintain systems, and provide for more flexible and productive systems.” If requested however, Avanceon can use specific industry standards. AutoGen™ is an Avanceon software application designed to rapidly and dynamically configure standard PLC code, HMI objects, electrical drawings, and system documentation to meet the clients’ specific set of standards and process design [331].

16 The international version of EN 50128, which is identical to EN 50128, is IEC 62279.

7 SUMMARY AND OBSERVATIONS

The key issues related to EDDs are (1) sufficient rigor in their procurement and control, (2) identification of EDDs in procured equipment, (3) dedication needs for appropriate quality and reliability, and (4) management of potential software-related CCFs.

A review of vendor component specifications and performance along with personal communication with selected vendors provided insights into the process of component development (including EDDs), manufacturing, testing and change, and configuration management.

Specifically, 18 instrument applications investigated in this project include EDDs associated with commonly used pressure, level, flow, and temperature control instruments. The functionality of these devices should be representative of other I&C applications in NPPs that are outside the 18 component types reviewed.

An initial survey of other other sectors and international regulatory practices was also performed to support future detailed work in this project.

ORNL also determined the potential safety implications—new hazards, vulnerabilities, failure modes, and triggering mechanisms, and other potential safety concerns—based on the use of digital instrumentation and controls (I&C) systems and components in safety-related or important to safety applications at NPPs. ORNL then identified existing practices and solutions to address the safety implications from other industries or from international organizations.

An evaluation of those existing practices and solutions was performed in order to support future decisions regarding regulations and guidance by the NRC, in particular the application of a graded approach.

A summary from the evalaution is provided in the areas of terminology, EDD related issues, operating experience, and existing practices which the NRC could use to address the EDD related issues.

An overall set of observations follows, including some observations related to emerging technologies identified during the review and the evaluations.

7.1 Summary

The installation of any EDD must be identified, reviewed, tested, controlled, and evaluated for the potential effects of hardware and software defects. Implementation of CGD, 10 CFR 21, and 10 CFR 50.59 processes, along with the NRC vendor inspection program, NUPIC (if five or more NUPIC members use their items and services) and NAIC evaluation of suppliers, and maintenance of the licensees' approved suppliers (vendors) list, should provide assurance that only components of appropriate quality are in use. However, none of these processes identified the design modification of the Allen-Bradley timing relays.

Of importance to this project is the RIS 2016-05 [1] that was written to clarify NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with EDDs. RIS 2016-05, which applies to equipment, instrumentation, and controls

that contain EDDs in safety-related systems, states that licensees should adequately address the following:

1. The quality and reliability of EDDs that exist in actuation equipment

2. The potential vulnerabilities to CCFs

3. Sufficient procurement planning and material control to identify, review, test, and control EDDs

Other issues related to the use of EDDs in safety-related systems include the potential for undeclared digital content in the devices, the difficulty in obtaining information about a device's design and operating history, the use of software tools, accepting certifications (similar to dedication) from other entities, new cyber security concerns, and the possibility that a graded approach may be beneficial for approving the use of EDDs.

In addition to meeting performance requirements, EDDs in safety-related systems should be designed for a reliability level that is commensurate with the safety significance of the function(s) to be performed. Design attributes for achieving a given level of functional reliability and robustness include those related to quality, knowing if digital content is in the EDD, the use of software tools and their pedigree, cyber security vulnerabilities, redundancy, diversity, failure detection, periodic testing (including the use of self-diagnostic features and surveillance tests), and failure data/failure modes. V&V should be included at appropriate stages of the design to confirm that the necessary safety functions have been identified and will operate as intended.

These issues, discussed below, can be used to guide regulatory judgements and recommendations when undertaking technical assessments of the use of EDDs in safety related applications. The supporting issues can be used to appropriately grade the review of the use of EDDs. In addition, the supporting issues can be used to guide assessments of proposed new nuclear facility designs.

7.1.1 Common Names

Because of the different names and functionality of EDDs, it is important for licensees and the NRC to understand exactly what is being installed. This is because some smart instruments in industry include communication devices.

The U.S. NRC uses the term EDD but throughout industry, other regulators, and foreign uses of EDDs, the most common related term is smart device. Other related terminology includes devices of limited functionality, or intelligent devices. Industry also uses the term IoT that signifies the devices are connected to a larger system that provides monitoring and information from those devices.

The standards community uses a larger set of related device names for types of EDDs including EDD, simple device, intelligent device, smart device, digital device, digital device of limited functionality, (synonym for device of dedicated functionality), industrial digital device, and programmable digital device.

An important distinction made by the UK's ONR between smart devices and other computer-based systems is that the end user cannot modify or add device functionality in any way, although the user can usually perform limited configuration. Such devices are still consideredto be

computer-based systems, so their use in safety or safety-related applications should be justified according to the United Kingdom's Office of Nuclear Regulation's SAP ESS.27.

7.1.2 EDD Related Issues

The introduction of EDDs can create new hazards, vulnerabilities, failure modes, triggering mechanisms, and other potential safety concerns at both the component level and system level. New vendors into the market may not be familiar with the quality requirements associated with the nuclear power industry. Other issues are the potential for undeclared digital content in the devices, the difficulty in obtaining information of the device's design and operating history, the use of software tools, accepting certifications (similar to dedication) from others, new cyber security concerns, and how a graded approach may be beneficial for approving the use of EDDs.

7.1.3 Operating Experience

Operating experience, although frequently used to determine failure rates, may be more appropriately used for lessons learned. The dc inductive kick on a relay reported in March 2015 (6 years after the design change) was not an original issue and was recognized as a CCF as far back as 1991. The difference between 1991 and 2015 is that devices are switching from analog to digital and digital components are more susceptible to a dc inductive kick failure mechanism. The review of operating experience for this report agreed with other reviews in that software errors can be CCFs that are likely the result from poorly defined, misunderstood, or not properly implemented requirements. Examples of both the undeclared digital content and the dc inductive kick failure mechanism highlighted in the review of operating experience are applicable to EDDs. Some regulators, such as the military, do not address CCFs per se, but rely on safety assessments based on the consequences (hazards) of a failure.

An issue with operating experience is that software issues may be reported differently. For example, operational experience based on returns under warranty may not capture software issues that were resolved via a call to the company and a patch or change in configuration without the actual item needing to be returned. Similarly design errors that can be resolved via a patch, either to resolve a software issue or compensate for some other design fault using software, may be reported differently in any system based on the number of reported issues. Such updates allow for fixing devices in the field resulting in no further reports or returns for that issue, as opposed to a manufacturing defect that could not be so resolved. A partial solution to this issue could be a requirement to know and examination of the number of updates or patches that have occurred for the product. Larger numbers of patches may indicate issues with the production quality of the design process and software development lifecycle.

It is generally accepted that operating experience can be used to prove the suitability and reliability of components and can therefore be used to support the confirmation of the regulatory requirements for the use of the device. However, the large volume of operational experience from industrial applications may not be applicable, and thus misused, because of a lack of documentation, uncertainty in the version of the device used, process conditions, operating environment, service history, proper failure reporting and recording of data, and any modifications to the device. That is, the failure rates are not sufficiently refined to reflect the use of EDDs in different environments or conditions. The limited data from operational experience in the NPP industry makes the use of reliability claims difficult to defend, although the non-nuclear industry has extensive operating experience and vendors claim increased reliability.

7.1.4 Existing Practices

Safety significance is a key characteristic of I&C systems at NPPs. Safety classification is one of the fundamental safety concepts used to ensure that NPPs pose minimal risk to public safety. The classification of an SSC identifies the importance to safety for that SSC and the consequence of its failure. The classification of SSCs is closely related to the plant states and the postulated initiating events.

10 CFR 50 establishes a classification approach for SSCs in a nuclear facility. 10 CFR 50.2 defines safety-related SSCs in terms of reliance on those SSCs to remain functional during and after design basis events to assure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain a safe shutdown condition, and (3) the capability to prevent or mitigate the consequence of accidents that could result in unacceptable offsite exposures.

There are notable variations in safety classification internationally. The classification of safety systems between countries, organizations, and even within the same organization may have a common term, but the terms may have different meanings. Although the classification of safety systems for other countries may not align well with the NRC's safety/not safety classification, a review of these other classifications provided insights into how to provide a graded approach to the review of safety-related EDDs which led to the categories in section 4.10. Understanding the specifics of different classifications could support regulators leveraging portions of each other's evaluations.

Another possible way to provide a graded approach would be to allow the use of IEC SIL certification used by industry and many regulators, both foreign and domestic, to support commercial graded dedication. Although this sounds simple, it would require much effort by the NRC to review and inspect the certification process, along with ensuring that any device meets the critical characteristics for its application.

7.1.5 Differences by Country

A summary of the terminology and standards used when evaluating the use of EDDs in NPPs is provided in Table 7-1.

Table 7-1 Summary of Terminology and Standards by Country for Evaluating the Use of EDDs

Country	Terminology	Standard Guidance/Guides
United States	Embedded digital devices (EDDs)	Appendix B/CGD RIS 2016-05 [1] RIS 2002-22 Supplement 1 [223]
Canada	Smart devices	CAN CSA-N290.14 CSA-N290.8 IEC 61508 (SIL) IEC 61513 (safety class) IEC 60880 IEC 62566
France	Intelligent devices Simple devices	IEC 62671 (applicable to all) IEC 61508 (previously certified)
	Digital device of limited functionality	RCC-E 2016

Table 7-1 Summary of Terminology and Standards by Country for Evaluating the Use of EDDs (Continued)

Country	Terminology	Standard/Guidance/Guide
Germany	Digital device of limited functionality (synonym for device of dedicated functionality) Industrial digital device (based on IEC terminology)	IEC 60880 IEC 61508 IEC 61513 IEC 62138 VDI/VDE 3528
India	Smart devices	ISO-9001 IEC 60880 IEEE Std. 603 [332] IEEE Std. 7-4.3.2-2003 [263] IEEE Std. 323 [158] AERB SG-D-25
Japan	Smart devices	Japan does not currently have regulations specific to the use of smart devices; I&C systems important safety were built on the assumption of using only nuclear qualified products and are regulated using the same requirements.
Korea	Smart devices	KINS/GE-N001 SRP BTP 7-19 SRM on SECY-93-087 NUREG/CR-6303 IEEE Std. 603 [332] IEEE Std. 7-4.3.2 [263] EPRI NP-5652 [73] EPRI TR-106439 [54]
Pakistan	Smart devices	IEEE Std. 1012
Romania	Smart devices	IEC 61511 EPRI 106439 ANSI/ISA-S75.13.01
Russian Federation	Smart devices	ISO 9001 certified Rostekhnadzor licensed
UK	Smart devices	ONR SAPs ONR TAG-046 TGN 032 IEC 61508 BS EN 61513, 61226…

Canada, Korea, and the United States refer to the IEEE standards as part of the basis for regulatory approval. IEEE Std. 603 and IEEE Std. 7-4.3.2 were most consistently identified as part of the basis.

India and Russia identified the use of IAEA safety standards related to their review of I&C. (The IEC standards are based on the IAEA standards.) In Russia, IAEA Safety Guide No. NS-G-1.3 and IAEA Draft Safety Guide DS-431 provide part of the technical basis for granting regulatory authorization in several technical topics. Also, in India, IAEA standards or other acceptable codes are used to review specific areas for which AERB documents have not been prepared.

Commonly used consensus standards are the IEC standards identified by Canada, France, and Russia as part of the technical basis for granting regulatory approval. The most commonly identified IEC standards were IEC 60880, IEC 61513, and IEC 62138.

France recognizes that certifications by themselves cannot be used as a basis for approval licensees are responsible for what is installed in their plant [176]. The United Kingdom uses IEC 61508 and Adelard's EMPHASIS tool, despite a reputable body being required for IEC SIL certifications above SIL 1.

In its guidance on COTs smart devices in ONR TAG-046 Revision 5, compensating activities (compensating measures) are allowed to make up for the gaps in production excellence information. No attempt is made to define the compensating activities (compensatory measures), as these would be determined on a case by case basis. TAG-046 indicates that there is no comprehensive guidance on the selection of independent confidence building measures for smart devices, beyond the details within the TAG itself. Some duty-holders have developed their own processes for justification of smart devices with ONR, however these are proprietay.

The UK and Canadian approaches to digital devices make for an interesting case study comparison. Both countries do not have a requirement for vendors to produce equipment in compliance with a nuclear-specific QA program such as 10 CFR 50 App B or ASME NQA-1, and they also do not include a 10 CFR 21 requirement that vendors must agree to comply with. As a result, both countries do not use the process commonly known as CGD. Both countries highly value the principles of IEC 61508 and implement a structured, graded approach using the defined SILs in conjunction with the classes and categories of IEC 61226. Despite these similarities, these countries have polar opposite perspectives on the value of third-party certifications. The CNSC is willing to rely heavily on these certifications, but the ONR has a significant skepticism of them. The ONR requires the certification process to be repeated through their EMPHASIS tool before having confidence in the digital device being suitable for the nuclear safety application.

7.1.6 Standards / Guidance

Outside of the nuclear industry, vendors typically use recognized and generally accepted good engineering practice. If the regulatory agencies in other industries or countries identify a standard for systems/components, they typically cite an IEC standard. In many cases, this leads to the use of IEC 61511/IEC 61508. That is, the supply chain and structures for non-nuclear safety related industries use IEC-61508/61511. Many use the same IEC standards but adopt them under a different number. For example, the international version of EN 50128 is IEC 62279, which is identical to EN 50128. Canada adopted IEC 61508 under the number of CSA 61508. Similarly, IEC 61511 is ANSI/ISA 84.00.01. However, IEC 62671 appropriately states that "IEC 61508 can be used as complementary guidance for the evaluation and assessment of components [for use in

the nuclear industry], but it is recognized that certification to non-nuclear standards alone is insufficient."

Many regulations and standards in use outside the U.S. nuclear industry are based on IEC SILs. Efforts are underway to change that in the United States. The purpose of NEI 17-06 [308] is to provide an acceptable approach for procuring and accepting commercial grade digital equipment that have an IEC SIL certification by an accredited third party SIL certification body for nuclear safety-related applications. The objective of EPRI 3002011817 [276] is to demonstrate that equipment certified to non-nuclear safety standards (more specifically, IEC-61508/61511) can meet or exceed nuclear power reliability requirements without further analysis or verification. EPRI 3002011816 [154] states that IEC SIL certification to IEC 61508 may provide evidence of product or platform suitability. If SIL certification is used as a method for demonstrating product or platform suitability, then the restrictions or conditions specified in the safety manual shall be integrated with related activities. Acceptance of components approved under IEC SIL certification to support the CGD process would require a proper review of IEC 61508, ensuring measures are in place so that only components that are used meet the form, fit, and function for its approved, and an inspection of the certification process and certification bodies.

Prior to acceptance, some deficiencies in the use of IEC SIL certifications have been expressed. More specifically, Summers notes that under IEC 61508 requirements, a product with a high total failure rate can achieve a high SIL claim limit as long as its failure is detected and annunciated [120]. This means that a device can have a high SFF and be highly unreliable. Possessing a high SFF does not necessarily mean that the device performance is adequate for safe service. Summers notes that "the SFF is not penalized by the choice to alarm rather than achieving the safe state. Therefore, the more failures that are detected, the higher the SFF becomes, regardless of the number of times, or the total amount of time, that the device is in the failed state, essentially dumping responsibility for process protection back on the operator." This approach would maximize the reliance on diagnostics and minimize the quality standards of the components. Summers also notes that "Following a careful review of a significant variety of product safety manuals, it appears that many field devices are achieving higher safety integrity level (SIL) claims than can be supported by process industry data [123]."

An alternative type of certification is that performed by Adelard. This method is accepted by the United Kingdom. That is, ONR has approved the use of EMPHASIS for dedicating components. It may be possible to leverage the ONR/EMPHASIS review for use in the United States.

Much of the guidance on EDDs and smart devices treat the devices as systems. For example, the U.S. requirements and guidance used to review the use of EDDs refer to safety systems. Guidance used by other regulators also review the devices like a system. Part of this is because the device is in a system. IEC 61511 defines *component* as "one of the parts of a system, SIS subsystem, or device performing a specified function" and states that a component may also include software. The components make up the system architecture. An impact analysis would be used to determine the effect that a change to a function or component will have to other functions or components in the system ***as well as in other systems***.

The approach of the IEEE SIL and IEC SIL are similar in that the requirements for meeting the standard increase as the SIL level increases. However, the IEC SILs directly relate to safety goals, whereas the IEEE SIL indirectly relate to safety through the presumption that high software integrity or quality will result in improved safety assurance. It seems clear that, given the extensive international use of IEC SIL certification in non-nuclear industries and the directly treatment of the primary objective of safety, the IEC SIL classification would form a very suitable

basis for characterizing the reliability/dependability, and thus the associated evidentiary requirements for the reliability/dependability, of EDDs.

The international standards allow more of a risk-based approach compared to the United States by ***qualitatively*** assessing the risks of hazardous operational situations. The V&V of the software tools is based on a graded approach and whether the software tool can or cannot introduce faults into the software or whether it can fail to make the user aware of existing faults.

Overall, the international standards appear to cover the same concerns as NRC's guidance and endorsed standards. For example, both use SILs for developing software, although the SILs are not a one-for-one match. Both recognize that software tools may be used and, depending on the standard development organization (either domestic or international), guidance differs on the acceptance of the software tools; however, domestic and international standards recognize the importance of the development process. In addition, the evaluation/acceptance process and supply chain are important topics in both international and domestic standards. The value of endorsing international standards is that vendors would not be required to design to different criteria and go through two evaluation/acceptance processes.

The software in an EDD may be developed using software tools or manually written. Vendors that were contacted indicated that they will manually write the code for the EDD but will use software tools if requested by the customer. If they manually write the software code for an EDD that can be used in a safety application it is written following an approved Appendix B program. With respect to software tools, some regulators assess software tools similar to support system software that is part of the system software in a typical I&C system and is either off-line or on-line (i.e., embedded in nonsafety support systems). Software tools may not need to be developed under an Appendix B program nor dedicated if V&V activities can detect defects not detected by or introduced by the software tool. Regulatory guidance is not consistant when that cannot be demonstrated. IEEE 7-4.3.2 2003 describes a test tool validation program or using tool operation experience and Regulatory Guide 1.152 and ISG-06 do not seem to contradict this; however BTP 7-14 and SRP Appendix 7.1-D clearly indicate that if such verification cannot be demonstrated the tool itself should be developed or dedicated as safety-related, with all the attendant requirements. Thus, insights into the V&V of the outputs of software tools may be needed to support future uses of software tools, particularlily commercial tools.

Countries and regulators are not the only organizations with terminology differences. Table 7-2 shows that the standards in use for providing guidance to designing I&C systems (and used for EDDs) typically use the terminology simple or smart device but many other names are also used.

Table 7-2 Summary of Terminology Used in Guidance/Standards Documents

Organization	Terminology	Guidance/Standard/Guide
AFCEN (French Society for Design and Construction rules for Nuclear Island Components)	Simple Smart device Digital device Digital device of limited functionality	• RCC E 2016 • IEC 60880 • IEC 62138 • IEC 62566 • IEC 62671 • IEC 60987
EPRI	Smart devices Embedded digital device	EPRI TR-106439 EPRI TR-107339 EPRI 3002008010
IAEA	Smart devices Embedded digital devices Industrial digital device	"Addressing Safety of Smart Devices for Use in Nuclear Power Plants" (first ever IAEA safety report on the subject, to be published later in CY2020) IAEA Nuclear Energy Series No. NP-T-X.XX, V2.25 (number to be determined) IAEA Nuclear Energy Series No. NP-T-1.13 IAEA Safety Standards Series No. SSG-39
IEC	Digital device of limited functionality (synonym for device of dedicated functionality) Industrial digital device	IEC 62671 IEC 61508
IEEE	Smart devices Programmable digital device	ONR SAPs ONR TAG-046 TGN 032 IEC 61508 BS EN 61513, 61226…
ISA	Smart devices intelligent devices	ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) ISA-TR108.1-2015
NEA	Digital device of limited functionality Programmable digital device	MDEP DICWG-07 NEA/CNRA/R(2014)7

7.2 Observations

Functionality/Terminology

The majority of EDDs in current use in the U.S. NPPs are stand-alone devices without communication connectivity beyond what may have been used in analog devices with a diagnostic output, such as being connected to other devices or in a system type architecture. EDD usage in NPPs around the world is similar to that in U.S. NPPs. Within the nuclear industry, EDDs are of limited functionality and are typically referred to as EDDs, smart devices, or devices of limited functionality. This is much different than EDD use in other industries. In fact, it is from other industries that EDDs have many different names and functions and it is expected that the increased functionality of EDDs in other industries will migrate to the nuclear industry.

Supply Chain and CGD related challenges

The ORNL review of the supply chain—front, middle, and back ends for EDD—did not identify gaps should a licensee and vendor follow the requirements and guidance as appropriate. This includes everything from secure development environments to purchase to integration at the plant. Many of these vendors that supply EDDs to NPPs are vertically integrated, or they specify the components to be used for the EDDs and are familiar with NRC regulations and guidance. NRC inspections of the CGD facilities provide assurance of the processes being followed.

Devices manufactured in a different time frame would not be considered identical per the guidance in IP 43004. An equivalency evaluation could include steps to ensure an EDD has not been added to a device that previously did not have one, or that a known EDD has not undergone a change.

Documentation shortcomings vary depending on manufacturer and when the product was developed. It is challenging to perform CGD without support from the supplier, including access to product information, company site visits, and discussions. Moreover, determining how much of the code to analyze can be challenging. Adelard recommends using flow graphs to reveal the internal structure of the code to find out exactly what code governs the main function of the smart sensor. From there, the assessor may concentrate only on the variables accessed from this critical code. Development of other approaches can be beneficial (i.e. other plugins, black-box techniques, assembly code analysis, architecture/system-level mitigations based on hazard analysis). However, determining how many techniques to use and how to combine them effectively can be troublesome, as well. The ONR SAPs and TAGs are goal-setting principles and guidelines, but they do not define what exactly needs to be done for device justification. There is a list of tools, approaches, and techniques known to the industry, but they are not technology independent, and not all are applicable to all devices.

Safety demonstrations of COTS products can be challenging. Products may be sold as a black-box, safety demonstrations may require the supplier's intellectual property, available guidance documents may be unclear, and known analysis techniques may not be suitable. Moreover, the nuclear industry is a relatively small customer and does not have much leverage with manufacturers.

A standards-based approach to EDD justification does not necessarily provide evidence that the I&C system and its software achieve the performance required at the desired level of reliability. One of the projects funded by the CINIF is entitled COTS Goal-based Safety Assessment (COGS) and is aimed at developing an approach to the safety justification of COTS products like devices dedicated to a single function, user-programmable and control equipment, or certain software-only products such as OSs. COGS is a claim-based approach, which uses the Claims-Arguments-Evidence (CAE) framework. A claim-based approach allows greater flexibility in making a justification while ensuring that all safety relevant attributes of the COTS product are justified. COGS is generally applicable to several types of products and is designed to demonstrate that the behavior and functionality of the product is sufficient for its intended application and that the products will behave accordingly throughout its design lifetime. Such an approach could provide some grading of the review of EDDs.

Operating and International Experience

Recent events show that operating experience can provide lessons learned (such as undeclared digital content or dc inductive kick failure mechanism) that can be used to provide additional guidance such as how to determine if a device has undeclared digital content to specifying in procurement documents the presence of such a device.

International experience with vendors is similar to that in the United States: manufacturers' data sheets may not state if microprocessors were used. O&M manuals may not go to the level of detail on component parts necessary for review, and visual examination often proved inconclusive. Instruments purchased just two years before now had microprocessors and purchasing an identical instrument with exactly the same part number would deliver an identical smart instrument.

Emerging Technology

In the future, if EDDs with communication capabilities are integrated into a safety system, the EDDs would need to consider independence between safety systems and other portions of a safety system, other systems, and the effects of design basis events, as required by Clause 5.6 in IEEE Std. 603. Care will need to be taken to ensure these requirements are not challenged in a particular implementation of an EDD as it may create new dependencies or make existing ones more significant.

As noted in Section 4.9.1, issues have been identified with the use of FMEAs with high complexity devices or within interacting systems. As EDDs are expected to increase in complexity and connectivity the use of FMEA to adequately address creating the critical characteristics needed for dedication becomes questionable. Modern methods and tools designed to deal with more complex and connected systems may be needed for such EDDs.

Licensing Review Guidance

The ORNL review found that while following all guidance for systems and the process regulatory guidance in support of Appendix B Quality Assurance should be sufficient, it may not be necessary. Graded approaches and commercial grade dedication could therefore improve the effeciancy of EDD reviews.

In reviewing EDDs, system level concerns for EDDs with increased functionality are reviewed to the extent that they impact the FSAR in existing plants or the areas of review in a new design as

appropriate. This will vary depending particularly on any communication features added. The issue of quality then remains. Addressing quality using 10 CFR 50 Appendix B and associated regulatory guidance documents related to quality should be sufficient for EDDs, but that may entail more effort than is necessary as these guidance documents were developed to support systems that may be more complex and involve more application specific code and customization than a particular EDD. Approval under CGD hinges on the ability to properly identify critical characteristics and then verify them. Currently this relies heavily on an understanding of the failure modes and FMEA especially in the absence of design documentation, therefore the controversies associated with the use of FMEA on digital systems as described in this report and leveraging different types of FMEA or other techniques for performing hazards assessments along with modern means of V&V could be a path forward in being able to resolve issues with future EDDs with more functionality and complexity.

The approach to smart devices in ONR guidance and ISG-06 both describe the use of measures (called compensatory in ISG-06 and compensating in ONR Nuclear Safety Technical Assessment Guide 046 Revision 5) given shortcomings in demonstrating the adequacy of the rigor of the development and production process. Neither gives particularly specific guidance on the nature of these measures. It may be possible to provide additional guidance to industry in a harmonized manner.

ISG-06 Revision 2 already has consideration of integrated design environmental tools stating: “It is acceptable for a licensee to adapt test documentation to reflect important process differences, technology differences, and exceptions related to the use of integrated design environment tools.” However, utilizing this flexibility may be challenging for model based engineering approaches or tools that do not produce outputs that can easily be put on the docket in any form.

Tests to indicate the presence of a digital device could be developed and instituted either at the vendor or plant. For example, EMC testing may indicate the presence of an EDD due to many EDDs having a vulnerability to EMI/RFI or high energy radiation or the signature on an oscilloscope may differ once a digital device is installed.

8 REFERENCES

1. RIS 2016-05, “Embedded Digital Devices in Safety-Related Systems,” April 29, 2016. (ADAMS Accession No. ML15118A015)

2. S. A. Arndt, “Embedded Digital Devices NRC Perspective,” Workshop on Qualification of Embedded Digital Devices Bethesda North Marriott Hotel, North Bethesda, MD, March 11, 2016.3.

3. Allen-Bradley Bulletin 700 -P, -R, -RTC, NEMA Industrial Relays. https://ab.rockwellautomation.com/Relays-and-Timers/700-RTC-NEMA-Solid-State-Timing-Relays#documentation

4. Emerson Process Management (2020), “FIELDVUEW DVC6200 Series Digital Valve Controller,” https://www.emerson.com/documents/automation/product-bulletin-fieldvue-dvc6200-digital-valve-controller-en-123336.pdf

5. B. Fitzgerald, M. Cheng-Newson, and F. Mercaldi, “Pickering Exploits Digital Valve Technology ,” Nuclear Engineering International, July 2015.

6. Editors R. de Lemos, C. Gacek, and A. Romanovsky, *Architecting Dependable Systems IV*, H. Sozer, B. Tekinerdogan, and M. Aksit, “Extending Failure Modes and Effects Analysis Approach for Reliability Analysis at the Software Architecture Design Level,” Pages 409-433, Springer-Verlag Berlin Heidelberg 2007.

7. IAEA Nuclear Energy Series No. NR-T-3.31, “Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, International Atomic Energy Agency, Vienna, 2020

8. R. Selega, “Smart Industry & Safety Instrumented Systems,” *Chemical Processing*, Feb 21, 2018. https://www.controlglobal.com/articles/2018/smart-industry-and-safety-instrumented-systems

9. K. McKay, OPG Canada, “Use of Smart Devices in Safety Related Computers,” *COTS Digital Devices in Safety Critical Industries, Use and Licensing*, Report 2019:627, Stockholm on 22 October 2019..

10. T. S. Nobes, “Smart Instruments in Safety Instrumented systems—Sellafield Experiences.” Measurement + Control, Vol 41/6, July 2008. https://journals.sagepub.com/doi/pdf/10.1177/002029400804100603

11. S. Kuball, “Experience with Justification of Smart Devices in EDF NG UK and issues for consideration,” IAEA Technical Meeting on Smart Devices, Vienna, 17-21 February 2020.

12. Kim, Y. M., Lee, H. K., & Park, H. S., “Regulatory Experience of the Embedded Digital Devices for Safety I and C Systems on NPPs,” Proceedings of the KNS 2016 Autumn Meeting, (pp. 1CD-ROM). Korea, Republic of: KNS, 2016.

13. International Society of Automation, “Intelligent Device Management—Part 1: Concepts and Terminology,” ISA-TR108.1-2015, Research Triangle Park, North Carolina, June 16, 2015.

14. E. Overling, “DDLF Qualification France, RCCE 2002-2012-2016,” EDF, March 2019.

15. Multi-National Design Evaluation Programme Digital Instrumentation and Controls Working Group, “Common Position on Selection and use of Industrial Digital Devices of Limited Functionality,” MDEP Common Position CP-DICWG-07, Version 3, 09 July 2014.16. IAEA Safety Standards Series No. SSG-39, “Design of Instrumentation and Control Systems for Nuclear Power Plants Specific Safety Guide,” International Atomic Energy Agency, Vienna, 2016.

16. IAEA Safety Standards Series No. SSG-39, “Design of Instrumentation and Control Systems for Nuclear Power Plants Specific Safety Guide,” International Atomic Energy Agency, Vienna, 2016.

17. International Electrotechnical Commission, “Nuclear Power Plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality,” IEC 62671 Ed. 1, Geneva, Switzerland, 2009-01-09.

18. EPRI 1002833, Final Report, “Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,” Electric Power Research Institute, EPRI, Palo Alto, CA, March 2002. (ML020860169)

19. Watanabe Nobumichi, “Considerations on Applying the Smart Devices,” Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Systems, IAEA Headquarters Vienna, Austria, 17 to 21 February 2020.

20. M. Rouse, DEFINITION embedded system, https://internetofthingsagenda.techtarget.com/definition/embedded-system

21. “Global Embedded System Market: Snapshot,” Transparency Market Research. https://www.transparencymarketresearch.com/embedded-system.html

22. M. Rouse, embedded system. https://internetofthingsagenda.techtarget.com/definition/embedded-system

23. “IIoT: Combining the Best of OT and IT,” Industrial Ethernet Book Issue 95 / 14. https://iebmedia.com/index.php?id=11673&parentid=63&themeid=255&hft=95&showdetail=true&bb=1

24. E. Dean, “When worlds collide: Understanding emerging IT/OT convergence.” 10 Sep 2018. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/When-worlds-collide-Understanding-emerging-IT-OT-convergence

25. B. Slusser, “Industry 4.0 is here – are you ready?,” March 16, 2018. https://avanceon.com/author/writer_30/

26. IEEE Std. 7-4.3.2-2016, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 29 January 2016.

27. *PumpSmart - ITT Pro Services* [Online]. Available: https://www.ittproservices.com/ittgp/medialibrary/ITTPROServices/website/Literature/Brochures/PRO%20Services/PSmartbulletin.pdf?ext=.pdf. [Accessed: Jan. 10, 2019].

28. *Smart technology for your oven and stove* [Online]. Available: https://www.lifewire.com/smart-oven-range-4159902. [Accessed: Jan. 10, 2019].

29. L. Blain, "World's first fully digital valves open up engine possibilities," New Atlas, August 11, 2018. https://newatlas.com/camcon-digital-iva-valve-system/55827/

30. T. Prestifilippo, "FIELDVUEW DVC6200 Series Digital Valve Controller, A Single Instrument Solution Across Your Facility." http://omeas.com/wp-content/uploads/2018/08/Product-catalog-Fisher-DVC6200.pdf

31. E. Saopraseuth, N. Wienhold, E. Butler, S. Guerra, and H. Khlaaf, "Emphasis Class 1 And Class 2 Assessment of Rosemount Pressure and Temperature Transmitters." https://www.adelard.com/assets/files/docs/pp11v30_npic2019_Rosemount.pdf

32. T. Nobes, "Smart Instruments in Safety Instrumented Systems – Sellafield Experiences," Measurement and Control, Volume 41, Issue 6, July 2008 https://journals.sagepub.com/doi/pdf/10.1177/002029400804100603

33. T. Jacobi, D. Floyd, R. Wood, A. Hashemian, H.M. Hashemian, and B. Shumaker. "Investigation of Instrumentation Containing an Embedded Digital Device," NPIC-HMIT 2017.

34. EPRI TR-1001503, "Identification and Description of Instrumentation, Control, Safety, and Information Systems and Components Implemented in NPPs," Electric Power Research Institute, Palo Alto, CA, June 2001.

35. R. T. Wood, R. A. Joseph III, K. Korsah, M. D. Muhlheim, and J. A. Mullens, LTR/NRC/RES/2012-001, "Classification Approach for Digital I&C Systems at NPPs," February 2012. (ADAMS Accession No. ML120970232)

36. R. T. Wood, et. al., "Emerging Technologies in Instrumentation and Controls," NUREG/CR-6812 (ORNL/TM-2003/22), March 2003. (ADAMS Accession No. ML031900433)37. Greg Kaser, "The World Nuclear Supply Chain – An Overview," World Nuclear Association, NEA International WPNE Workshop, Paris, 11 March 2014.

37. Greg Kaser, "The World Nuclear Supply Chain – An Overview," World Nuclear Association, NEA International WPNE Workshop, Paris, 11 March 2014.

38. H. M. Hashemian, "Nuclear Power Plant Instrumentation and Control, " *Nuclear Power - Control, Reliability and Human Factors*, Pavel Tsvetkov, IntechOpen, DOI: 10.5772/18768, September 26th 2011. Available from: https://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/nuclear-power-plant-instrumentation-and-control

39. Nuclear News, 23rd Annual Vendor/Contractor Profile Issue, August 2017.

40. Nuclear Utility Obsolescence Group (NUOG), vendor links. http://www.nuog.org/NUOG_Vendor_Links.html

41. Nuclear Suppliers Association (NSA). http://www.nuclearsuppliers.org/

42. *Nuclear Plant Journal*, Browse By Product, 2020. http://www.nuclearplantjournal.com/index.php?option=com_content&view=article&id=125&Itemid=149

43. *Nuclear Plant Journal*, Browse by Company, 2020. http://www.nuclearplantjournal.com/index.php?option=com_content&view=article&id=130&Itemid=150

44. *Nuclear Engineering International*, Company A-Z. http://www.neimagazine.com/contractors/indexAtoZ.html

45. Nuclear Procurement Issues Corporation (NUPIC). https://nupic.com/NUPIC/Home/Home.aspx

46. World Nuclear Association. http://www.world-nuclear.org/our-association.aspx

47. Nuclear Engineering Enabling Technologies (NEET) Workshop on Qualification of Embedded Digital Devices, Bethesda North Marriott Hotel, North Bethesda, MD, March 11, 2016.

48. R. Wood, "Addressing Embedded Digital Devices in Diversity and Defense in Depth Analyses," IAEA Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Systems Important to the Safety of Nuclear Power Plants, Vienna, 17-21 February 2020.

49. "Advisory Committee on Reactor Safeguards Plant Operations and Fire Protection Subcommittee Meeting Minutes," Atlanta, GA, July 28, 2016. (ADAMS Accession No. ML16243A457)

50. T. S. Nobes, "Smart Instruments in Safety Instrumented Systems – Sellafield Experiences," Measurement + Control Vol 41/6 July 2008.

51. H. Sozer, B. Tekinerdogan, and M. Aksit, "Extending Failure Modes and Effects Analysis Approach for Reliability Analysis at the Software Architecture Design Level," Department of Computer Science, University of Twente, P.O. Box 217 7500 AE Enschede, The Netherlands, 2007.

52. K. Kavanagh, "NRC's Vendor Inspection & Quality Assurance Update," 3rd Workshop on Vendor Oversight for New Reactor Construction, June 21, 2012. (ADAMS Accession No. ML12171A243)

53. EPRI 3002002982, "Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications, Revision 1 to EPRI NP-5652 and TR-102260," Electric Power Research Institute, Palo Alto, CA, September 2014.

54. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, Palo Alto, CA, October 1996.

55. 10 CFR 21.21 Notification of failure to comply or existence of a defect and its evaluation.

56. Doug VanTassell, "Commercial Grade Dedication Challenges," NRC Workshop, June 14, 2018. (ADAMS Accession No. ML18150A373)

57. EPRI 3002008010, “Guideline on Prevention and Detection of Undeclared Digital Content,” Electric Power Research Institute, Palo Alto, CA, 2016.

58. Curtiss Wright Nuclear Division, “Undeclared Digital Content,” 24, 2020. (ADAMS Accession No. ML21076A003)

59. U.S. NRC Information Notice 2014-11, “Recent Issues Related to the Qualification and Commercial Grade Dedication of Safety-Related Components,” September 19, 2014. (ADAMS Accession No. ML14149A520)

60. Nutherm International, Inc, “Subject: Report of Potential 10CFR Part 21, Allen Bradley Time Relay Model 700RTC,” June 4, 2015. (ADAMS Accession No. ML17311A903)

61. U.S. NRC Information Notice 2016-01: Recent Issues Related to the Commercial Grade Dedication of Allen Bradley 700-RTC Relays, February 17, 2016. (ADAMS Accession No. ML15295A173)

62. Brunswick Steam Electric Plant (BSEP), Unit 1, 5000325, Licensee Event Report 2015-002-1, “Emergency Diesel Generator Loss of Safety Function,” November 16, 2015. (ADAMS Accession No. ML15329A374)

63. Bhavesh Patel, Duke Energy, “Allen Bradley 700-RTC Relay Part 21 Issues,” NRC Regulatory Information Conference, March 2016.

64. Part 21 Report No: P21-04302015, Rev. 3, “Update: Report of potential 10 CFR Part 21, Allen Bradley Timing Relay Model 700RTC,” AZZ/NLI, August 15, 2016. (ADAMS Accession No. ML16238A186)

65. United Controls International, “Subject: Report of Potential Part 21 on Allen Bradley Time Delay Relay 700-RTC-11200U1,” July 20, 2015. (ADAMS Accession No. ML15205A293)

66. U.S. NRC, “Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 273 to Renewed Facility Operating License No. DPR-50 Exelon Generation Company, LLC, Three Mile Island Nuclear Station, Unit 1 Docket No. 50-289,” May 27, 2010. (ADAMS Accession No. ML092740791)

67. J. Servatius, S. Alexander, and T. Gitnick, “Evaluation of Guidance for Tools Used to Develop Safety-Related Digital Instrumentation and Control Software for NPPs, Task 2 Report: Analysis of the State of Practice,” ISL-ESRD-TR-14-03, August 2014. (ADAMS Accession No. ML15043A206)

68. U.S. NRC I&C-ISG-06, Revision 1, “Digital Instrumentation and Controls Licensing Process”, January 19, 2011. (ADAMS Accession No. ML110140103)

69. U.S. NRC I&C-ISG-06, Revision 2, “Digital Instrumentation and Controls Licensing Process”, December 2018. (ADAMS Accession No. ML18269A259)

70. National Aeronautics and Space Administration, “NASA Software Safety Guidebook.” NASA-GB-1740.13.71. Radio Technical Commission for Aeronautics (RTCA), “Software Tool Qualification Considerations,” DO-330, December 2011.

71. RTCA/DO-330, “Software Tool Qualification Considerations,” December 2011.

72. International Organization for Standardization (ISO), "Road vehicles – Functional safety," ISO 26262-1:2018, 2018.73. EPRI NP 5652, “Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07),” June 1988.

73. EPRI NP 5652, “Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07),” June 1988.

74. EPRI TR-102260, “Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items,” Electric Power Research Institute, Palo Alto, CA, March 1994.

75. International Electrotechnical Commission, “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems,” IEC 61508-2, Geneva, Switzerland, 2010-04.

76. International Society of Automation (ISA), “Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements,” ANSI/ISA 84.00.01-2004, Part 1 (IEC 61511-1 Mod), Research Triangle Park, North Carolina, September 2004.77. EPRI TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications,” Electric Power Research Institute, Palo Alto, CA, December 1997.

77. EPRI TR-107339, “Evaluating Commercial Digital Equipment for High Integrity Applications,” December 1997.

78. EPRI TR-1011710, Handbook for Evaluating Critical Digital Equipment and Systems, Electric Power Research Institute, Palo Alto, CA, November 2005.

79. International Electrotechnical Commission, “Nuclear Power Plants—Instrumentation and Control for Systems Important to Safety—General Requirements for Systems,” IEC 61513, Geneva, Switzerland, March 2001.

80. International Electrotechnical Commission, “Computer hardware,” IEC 60987, Geneva, Switzerland, 2013.

81. International Electrotechnical Commission, “Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer based systems performing category A functions,” IEC 60880:2006, Geneva, Switzerland, 2006.

82. International Electrotechnical Commission, “NPPs - Instrumentation and Control Important for Safety - Software Aspects for Computer-Based Systems Performing Category B or C Functions,” IEC 62138, First Edition, Geneva, Switzerland, January 2004.

83. U.S. Department of Defense, “Standard Practice for System Safety,” MIL-STD-882E, 11 May 2012.

84. U.S. Department of Defense, “Joint Software Systems Safety Engineering Handbook,” Version 1.0 Published August 27, 2010.

85. G. Johnson, “Nuclear use of I&C Equipment Certified for Commercial Safety Use,” Presented at Opportunities and Challenges for Water Cooled Reactors in the 21st Century Vienna, 2009 October 27 –29.

86. 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”.

87. Nuclear Energy Institute, “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Rev. 6, April 2010. (ADAMS Accession No. ML101180437)

88. EPRI 3002012753, Technical Report, Revision 2, “Cyber Security in the Supply Chain, Cyber Security Procurement Methodology,” Electric Power Research Institute, Palo Alto, CA, October 2018.

89. Nuclear Energy Institute, “Identifying Systems and Assets Subject to the Cyber Security Rule,” NEI 10-04, Revision 2, July 2012. (ADAMS Accession No. ML12180A081)

90. Nuclear Energy Institute, “Cyber Security Control Assessments,” NEI 13-10, Rev. 5, February 2017. (ADAMS Accession No. ML17046A658)

91. North American Electric Reliability Corporation (NERC), “Order Approving Revised Reliability Standards For Critical Infrastructure Protection And Requiring Compliance Filing,” Cyber Security Standards CIP-002 to CIP-009, September 30, 2009. https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/OrderApproving_V2_CIP-002_CIP-009-09302009.pdf#search=Cyber%20Security%20Standards%20CIP%2D002

92. IEEE Std. 1686-2013, “IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, Approved December 11, 2013.

93. Vendor Expectations from a Cyber Security Perspective, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjppvOrxrTrAhVLhuAKHYTJBSYQFjAAegQIAxAB&url=https%3A%2F%2Fnupic.com%2FNUPIC%2FGetFile.aspx%3FID%3D74%26tbl%3DHOME_HOT_TOPICS_DOCS%26idFN%3Did%26fileFN%3Dfile_name&usg=AOvVaw0Ns2UnavVZinm5fortREzZ [Accessed: September 6th, 2020].

94. CSA Group, “Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants,” CSA N290.14-15, November 2015.

95. D. Alberico et. al., “Software System Safety Handbook,” Joint Software System Safety Committee, Joint Services Computer Resources Management Group, U.S. Navy, U.S. Army, and the U.S. Air Force, December 1999.

96. U.S. NRC, “Frequently Asked Questions About Digital I&C.” (ADAMS Accession No. ML063620169) https://www.nrc.gov/docs/ML0636/ML063620169.pdf

97. Mike Cain, “ACRS Briefing: Brunswick NPP Emergency Diesel Generator Commercial Grade Dedication Finding,” July 28, 2016. (ADAMS Accession No. ML16210A515)

98. Shearon Harris Nuclear Power Plant, Unit 1, “Both Emergency Load Sequencers Subject To Common Mode Failure Due To Improper Application Of Relays Not Accounting For Dc Inductive Load Rating,” LER 90-015, June 25, 1990. (ADAMS Accession No. ML18009A580)

99. U.S. Nuclear Regulatory Commission (NRC), "Common-Cause Failures Due to Inadequate Design and Control Dedication," NRC Information Notice No. 94-20, Washington, D.C., 1994. (ADAMS Accession No. ML031060589)

100. Waterford Steam Electric Station, “LER 382/17-002 – Automatic Reactor Scram due to the Failure of Fast Bus Transfer Relays to Automatically Transfer Station Loads to Off-Site Power on a Main Generator Trip,” September 18, 2017. (NRC ADAMS Accession No. ML17261B215)

101. “Shearon Harris NPP - NRC Integrated Inspection Report 05000400/2013002, “ April 30, 2013. (ADAMS Accession No. ML13120A340)

102. EGM 14-002, “Enforcement Guidance Memorandum 14-002, Dispositioning Westinghouse Pressurized Water Reactor Licensee Noncompliance With 10 CFR 50.59, ‘Changes, Tests, And Experiments,’ for the Installation of Complex Programmable Logic Device (CPLD) Based Solid State Protection System (SSPS) Cards,” October 2, 2014. (ADAMS Accession No. ML14014A125)

103. IR 05000400/2013009; 04/01/2013 – 07/15/2013; “Shearon Harris NPP, Unit 1; Evaluations of Changes, Tests, and Experiments and Permanent Plant Modifications Baseline Follow-up,” August 12, 2013. (ADAMS Accession No. ML13224A290)

104. U.S. Nuclear Regulatory Commission (NRC),"Effects of Ethernet-Based,Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," NRC Information Notice: 2007-15, ADAMS Accession No. ML071010303, Washington, D.C., 2007.

105. EPRI 1016731, “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems,” Electric Power Research Institute, Palo Alto, CA, December 2008.

106. Palo Verde Nuclear Station Unit 3, “Reactor Trip Due to Lightning Induced Electrical Fault,” (50-530) LER 91-008-00, December 13, 1991. (ADAMS Accession No. ML17306A337)

107. Turkey Point Units 3 and 4, 50-250/50-251, LER 94-005-02, “Design Defect in Safeguards Bus Sequencer Logic Timing Places Both Units Outside the Design Basis,” 50-250/50-251, LER 94-005-02, July 17, 1995. (ADAMS Accession No. ML17353A295)

108. Turkey Point Unit 3, 50-250, LER 2014-005-0, “Manual Reactor Trip Due to Loss of Instrument Air,” 50-250, LER 2014-005-0, October 10, 2014. (ADAMS Accession No. ML14303A475)

109. U.S. Department of Energy, Office of Health, Safety and Security, “Software Quality Assurance, Firmware Defect in Programmable Logic Controller,” Safety Advisory 2010-08, October 2010.110. EPRI TR-108331, “Requirements Engineering for Digital Upgrades, Specification, Analysis, and Tracking,” Electric Power Research Institute, Palo Alto, CA, December 1997.

110. EPRI TR-108331, “Requirements Engineering for Digital Upgrades, Specification, Analysis, and Tracking,” December 1997.

111. S. Guerra, P. Bishop, R. Bloomfield, and D. Sheridan, “Assessment And Qualification Of Smart Sensors,” Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2010).

112. U.S. NRC Research Information Letter 1002, “Identification and Analysis of Failure Modes in Digital Instrumentation and Controls (DI&C) Safety Systems—Expert Clinic Findings, Part 2,” August 12, 2013. (ADAMS Accession No. ML14197A201)

113. Erin Engineering, “Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions”, Electric Power Research Institute, Palo Alto, CA,, 2008. (ADAMS Accession No.ML090860465)

114. U.S. NRC SECY-09-0061, “Status of The Nuclear Regulatory Commission Staff Efforts to Improve the Predictability and Effectiveness of Digital Instrumentation and Control Reviews,” April 14, 2009.

115. S. Birla, Russell Sydnor, and N. Carte, “(Availability of) An International Report on Safety Critical Software for Nuclear Reactors by the Regulator Task Force on Safety Critical Software (TF-SCS),” NUREG/IA-0463, December 2015. (ADAMS Accession No. ML15348A206)

116. U.S. NRC Commissioner Briefing on Digital Instrumentation and Control, Rockville, Maryland, May 14, 2019. (Adams Accession No. ML19137A336)

117. U.S. Department of Transportation, Federal Aviation Administration, “Software Service History Report,” DOT/FAA/AR-01/125, Office of Aviation Research, Washington, D.C. 20591, January 2002.

118. R. Wood, et. al., “Development and Demonstration of a Model Based Assessment Process for Qualification of Embedded Digital Devices in Nuclear Power Applications, Second Annual Progress Report,” September 2017.

119. U.S. NRC Research Information Letter 1001: Software-Related Uncertainties in the Assurance of Digital Safety Systems—Expert Clinic Findings, Part 1. (ADAMS Accession No. ML111240017)

120. A. E. Summers, “Kiss Off Safety System Myths, Many Misconceptions Muddle Maneuvers to Manage Risks,” Chemical Processing, Environmental Health & Safety I Safety Instrumented Systems, Nov 07, 2011.

121. M. van der Meulen, “On the Use of Smart Sensors, Common Cause Failure and the Need for Diversity,” Centre for Software Reliability, City University, London http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.3366&rep=rep1&type=pdf

122. Nuclear Plant Reliability Data System (NPRDS). 1982 Annual Report. October 1983. Data inclusive for 7/74 - 12/82.

123. A. E. Summers, “IEC 61508 Product Approvals–Veering off Course,” ControlGlobal.com, July 2008. https://www.controlglobal.com/articles/2008/187/

124. UK Office of Nuclear Regulation, “Safety Assessment Principles for Nuclear Facilities,” 2014 Edition, Revision 1 (January 2020). http://www.onr.org.uk/saps/saps2014.pdf

125. U.S. NRC Final Safety Evaluation by the Office of Nuclear Reactor Regulation, Topical Report WCAP-17867-P, Revision 1, “Westinghouse SSPS Board Replacement Licensing Summary Report,” Pressurized Water Reactor Owners Group, September 19, 2014. (ADAMS Accession No. ML14260A143)

126. UK Office for Nuclear Regulation, “Technical Assessment Guide – Computer Based Safety Systems,” NS-TAST-GD-046, Rev. 5, Liverpool, 2019.

127. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) / Institute of Electrical and Electronic Engineers (IEEE), “Systems and software engineering — Vocabulary,” ISO/IEC/IEEE 24765-2017, 2017-09.

128. EPRI 1019182, “Protecting against Digital Common-Cause Failure: Combining Defensive Measures and Diversity Attributes,” Electric Power Research Institute, Palo Alto, CA,Final Report, November 2010.

129. B. Fitzgerald, T. Prestifilippo, and C. Holden, “Digital field devices make headway and deliver results in NPPs,” Nuclear Exchange, November 2012.

130. U.S. NRC Research Information Letter 1101, “Technical Basis to Review Hazard Analysis of Digital Safety Systems,” February 13, 2015. (ADAMS Accession No. ML14237A359)

131. B. F. Dittman, “Digital I&C Research Relating to Embedded Digital Devices,” Workshop on Safe Use of EDDs, October 9, 2014. (ADAMS Accession No. ML14280A569)

132. K. Korsah, S. M. Cetiner, M. D. Muhlheim, and W. P. Poore III, “An Investigation of Digital Instrumentation and Control System Failure Modes,” ORNL/TM-2010/32, March 2010.

133. S. Khaiyum and Y. S. Kumaraswamy, “Failure Modes in Embedded Systems and its Prevention,” *Journal of Software Engineering Research*, Jun. 2011, Available: http://astronomyjournal.yolasite.com/resources/2.pdf.

134. K. Korsah, M. D. Muhlheim, and D. E. Holcomb, “Industry Survey of Digital I&C Failures,” ORNL/TM-2006/626, May 2007.

135. K. Korsah, S. Cetiner , M. Muhlheim, and W. P. Poore III, ”An Investigation of Digital Instrumentation and Control System Failure Modes,” NPIC-HMIT 2010.

136. Letter from William J. Shack, Chairman, ACRS, to Dale E. Klein, Chairman, U.S. NRC, “Subject: Digital Instrumentation and Control Systems Interim Staff Guidance,” April 29, 2008. (ADAMS Accession No. ML081050636)

137. R. R. Lutz, “Analyzing software requirements errors in safety-critical, embedded systems,” Proceedings *of the IEEE International Symposium on Requirements Engineering*, 126-133, 1993.

138. National Research Council 2007. Software for Dependable Systems: Sufficient Evidence?. Washington, DC: The National Academies Press. https://doi.org/10.17226/11923.

139. P. Gruhn and S. Lucchini, “Safety Instrumented Systems: A Life-Cycle Approach,” International Society of Automation, 2019.

140. International Society of Automation, “Safety Integrity Level (SIL) Verification of Safety Instrumented Functions,” ISA-TR84.00.02-2015, Research Triangle Park, North Carolina, Approved 8 September 2015.

141. S. Abdel-Khalik, “Draft Final Digital Instrumentation & Control Interim Staff Guidance-06: Licensing Process,” Oct. 2010. (ADAMS Accession No. ML102850357)

142. U.S. NRC Inspection Procedure 38703, “Commercial Grade Dedication,” 1996.

143. U.S. NRC Inspection Procedure 43004, “Inspection of Commercial-Grade Dedication Programs,” November 2013. (ADAMS Accession No. ML16344A092)

144. U.S. Nuclear Regulatory Commission Staff, “Safety Evaluation for Topical Report 2016-RPC003-TR-001 RadICS Safety System Digital Platform,” August 2019 (NRC Adams Accession No. ML19134A193).

145. U.S. NRC Information Notice 1997-081, “Deficiencies in Failure Modes and Effects Analyses for Instrumentation and Control Systems” (ADAMS Accession Number: ML031050048)

146. L. Betancourt, S. Birla, J. Gassino, and P. Regnier, *NUREG/IA 0254 Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems*, Nuclear Regulatory Commission, 2011 (ADAMS Accession Number: ML11201A179)

147. EPRI 300200509, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” Electric Power Research Institute, Palo Alto, CA, June 27, 2013.

148. U.S. Department of Transporation, Federal Aviation Administation, *FAA System Safety Handbook*, Chapter 8, “Safety Analysis/Hazard Analysis Tasks,” December 30, 2000.

149. EPRI 3002002990, “Digital Common-Cause Failure Susceptibility: 2014 Project Status” Electric Power Research Institute, Palo Alto, CA, November 2014.

150. IEEE Std. 100-2000, “Authoritative Dictionary of IEEE Standards Terms,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2000.

151. UK Ministry of Defence, “Requirements for safety related electronic hardware in defence equipment,”, Defence Standard 00-54, 1999.

152. IEEE Std. 610.12-1990, “IEEE Standard Glossary of Software Engineering Terminology,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1990.

153. Government of Japan, “Convention on Nuclear Safety National Report of Japan for the Third Review Meeting,” August 2004. https://www.meti.go.jp/english/report/downloadfiles/NISAreport3e.pdf

154. EPRI Technical Report 3002011816, “Digital Engineering Guide, Decision Making Using Systems Engineering,” Electric Power Research Institute, Palo Alto, CA, October 2018.

155. lEEE Std. 1100-2005, “IEEE Recommended Practice for Powering and Grounding Electronic Equipment,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, Approved 9 December 2005.

156. EPRI 1001468, Final Report, “Generic Qualification of the Rosemount 3051N Pressure Transmitter Summary of Activities and Results,” Electric Power Research Institute, Palo Alto, CA, June 2000.

157. A. Nack, “Standardizing Functional Safety Assessments for Off-The-Shelf Instrumentation and Controls,” Masters Theses, The University of Tennessee, May 2016.

158. IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, New Jersey, 2003.

159. R. A. Kisner et. al., “Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants,” ORNL/NRC/LTR-07/05, August 2007.

160. International Atomic Energy Agency, “Specification of requirements for upgrades using digital instrument and control systems,” IAEA-TECDOC-1066, Vienna, 1999.

161. World Nuclear Association, Report No. 2015/008, “Safety Classification for I&C Systems in Nuclear Power Plants – Current Status & Difficulties,” September 2015.

162. International Atomic Energy Agency, “Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants: A Reference Book, Nuclear Energy Series Report,” IAEA NP-T-3.12, Vienna, Austria, December 2011.

163. 10 CFR 21.3, “Definitions.”

164. G. G. Preckshot and J. A. Scott, “A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications,” NUREG/CR-6421, March 1996. (ADAMS Accession No. ML063530384)

165. EPRI TR 1025243, “Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications,” Electric Power Research Institute, Palo Alto, CA, June 2012.

166. U.S. NRC Regulatory Guide 1.231, Revision 0, Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Safety- Related Applications for Nuclear Power Plants, January 2017. (ADAMS Accession No. ML16126A183)

167. EPRI 3002002289, “Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications, Revision 1 of 1025243,” Electric Power Research Institute, Palo Alto, CA, December 2013.

168. EPRI NP-6895, “Guidelines for the Safety Classification of Systems, Components, and Parts Used in Nuclear Power Plant Applications (NCIG-17),” Electric Power Research Institute, Palo Alto, CA, 1991.

169. U.S. Department of Transporation, Federal Aviation Administration, “Software Development for the National Airspace System (NAS),” FAA-STD-026A, June 1, 2001.

170. National Aeronautics and Space Administration, “NASA Software Engineering Requirements”, NASA NPR 7150.2A, November 2009.

171. British Standard Institution (BSI), “Railway applications—Communication, signaling and processing systems—Software for railway control and protection systems,” BS EN 51208:2011+A1:2020.

172. International Atomic Energy Agency, “Instrumentation and Control Systems Important to Safety in Nuclear Power Plants,” IAEA NS-G-1.3, Vienna, Austria, 2002.

173. International Atomic Energy Agency, “Technical Challenges in the Application and Licensing of Digital Instrumentation and Control Systems in Nuclear Power Plants,” Vienna IAEA Nuclear Energy Series No. NP-T-1.13, 2015.]

174. International Atomic Energy Agency, “Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” IAEA Safety Standards Series No. SSG-30, Vienna, 2014.

175. International Electrotechnical Commission, “Nuclear power plants - Instrumentation and control important to safety – Classification of instrumentation and control functions,” IEC 61226, Edition 3, Geneva, Switzerland, 2005·09·23.

176. E. Butler, et. al., “COTS Digital Devices in Safety Critical Industries,” Report 2019:627, ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC, November 2019.

177. International Atomic Energy Agency, “Modern Instrumentation and Control for Nuclear Power Plants, a Guidebook,” IAEA Technical Reports Series No. 387, Vienna, 1999.

178. U.S. NRC SRP BTP 7-17, Rev. 6, “Guidance on Self-Test and Surveillance Test Provisions,” August 2016. (ADAMS Accession No. ML16019A316)

179. S. Birla, R. Sydnor, and N. Carte, “(Availability of) An International Report on Safety Critical Software for Nuclear Reactors by the Regulator Task Force on Safety Critical Software (TF-SCS),” NUREG/IA-0463, December 2015. (ADAMS Accession No. ML15348A206)

180. International Atomic Energy Agency, “Safety of Nuclear Power Plants: Design,” IAEA Safety Standard Series Requirements NS-R-1:2016, Vienna, 2016.

181. K. Korsah, et. al., “Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update,” NUREG/CR-6992, October 2009. (ADAMS Accession No. ML092950511)

182. International Electrotechnical Commission, “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations,” IEC 61508-4, Edition 2, Geneva, Switzerland, 2010-04.

183. S. Brown and J. Rose, “Architecture of FPGAs and CPLDs: A Tutorial,” Department of Electrical and Computer Engineering, University of Toronto.

184. EPRI 3002012755, “HAZCADS: Hazards and Consequences Analysis for Digital Systems,” Electric Power Research Institute, Palo Alto, CA, Dec 17, 2018.

185. ASME/ANS RA-Sa-2009, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” Addendum A to RA-S-2008, ASME, New York, NY, American Nuclear Society, La Grange Park, IL, February 2009.

186. NRC Web: “Glossary” http://www.nrc.gov/reading-rm/basic-ref/glossary.html

187. U.S. Department of Energy, “Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities,” DOE-STD-1195-2011, April 2011.

188. Siemens, “Functional safety in process instrumentation with SIL rating, Questions, examples, background.” https://cache.industry.siemens.com/dl/files/169/109766169/att_980479/v1/SIL-Broschuere_EN.pdf

189. F. Liebusch, “Relays in safety-related control systems,” Electronic Specifier, January 9, 2017. https://www.electronicspecifier.com/products/power/relays-in-safety-related-control-systems

190. MEN Mikro Elektronik, “Embedded Electronics Product and Expertise Overview for Mission-Critical Industrial, Aerospace, Power & Energy, Marine, Automotive and Medical Solutions.”

191. International Atomic Energy Agency, “Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plan,” Vienna IAEA Nuclear Energy Series No. NP-T-3.27,, 2018.

192. J. C. Laprie, “Dependable Computing: Concepts, Limits Challenges,” Proceedings of the 25th IEEE International Symposium on Fault-Tolerant Computing—Special Issue, Institute of Electrical and Electronics Engineers, Pasadena, California, pp. 42–54 (1995).

193. R. T. Wood, et. al., Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems,” NUREG/CR-7007, February 2010.

194. International Electrotechnical Commission, “Functional safety of electrical/electronic/programmable electronic safety-related systems,” IEC 61508:2010, Geneva, Switzerland, 2010.

195. International Society of Automation (ISA), “Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements,” ANSI/ISA-61511-1-2018 / IEC 61511-1:2016, Research Triangle Park, North Carolina, (IEC 61511-1:2016+AMD1:2017 CSV, IDT).

196. A. E. Summers, K. A. Ford, and G. Randy, “Estimation and Evaluation of Common Cause Failures in SIS,” Chemical Engineering Progress, November 1999.

197. International Atomic Energy Agency, “Procedures for conducting common cause failure analysis in probabilistic safety assessment,” IAEA TECDOC-648, Vienna, May 1992.

198. UK Health and Safety Executive (HSE), “Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry,” Dec 14, 2018. https://www.hse.gov.uk/foi/internalops/og/og-00054.htm

199. Letter from K. Deutsch, F. Bamdad, and P. Fox to S. A. Stokes, Technical Director, Defense Nuclear Facilities Safety Board, Staff Issue Report, “Alternative Methodology for Safety Integrity Level Determination of Instrumented Systems at the Low-Activity Waste Pretreatment System,” June 12, 2017.

200. G. Coles, “Technical Specifications Surveillance Interval Extension of Digital Equipment in Nuclear Power Plants: Methods and Implementation Strategy,” INL/EXT-19-55342, Revision 0, September 2019.

201. T. [Edward) Quinn, J. Mauck, R. Bockhorst, and K. Thomas, “Digital Sensor Technology,” INL/EXT-13-29750, July 2013.

202. International Society of Automation (ISA), “Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the application of IEC 61511-1:2016,” ANSI/ISA-61511-2-2018 / IEC 61511-2:2016, Research Triangle Park, North Carolina, (IEC 61511-2:2016, IDT)

203. IEEE Std. C37.231-2006(R2012), “IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, Approved 12 June 2006, Reaffirmed 29 March 2012.

204. R. Wood, J. Mauck, and E. Quinn, “Addressing Embedded Digital Devices in Safety-Related Systems of Nuclear Power Plants,” NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017.

205. International Society of Automation (ISA), “Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod),” ISA-TR84.00.04-2015, Part 1, Research Triangle Park, North Carolina, Approved 6 April 2015.

206. S. Nunns, “Principles for proof testing of safety instrumented systems in the chemical industry,” Prepared by ABB Ltd for the Health and Safety Executive, 2002.

207. UK Office for Nuclear Regulation, “Safety Systems,” NS-TAST-GD-003, Revision 8, March 2018. http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.pdf

208. National Aeronautics and Space Administration, “NASA Software Safety Guidebook,” NASA-GB-8719.13, March 31, 2004.

209. IEEE Std. 1012-2004, “IEEE Standard for Software Verification and Validation,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2004.

210. IEEE Std. 829-2008, “IEEE Standard for Software and System Test Documentation,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2008.

211. T. Chu, M. Yue, G. Martinez-Guridi, and J. Lehner, “Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants,” Draft Report for Comment, NUREG/CR-7044, July 2011.

212. T. Chu, et. al., “Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability,” NUREG/CR-7234, May 2017.

213. R. T. Wood et. al., “Common-Cause Failure Mitigation Practices and Knowledge Gaps,” ORNL/LTR-2012/556 (NEET/ASI/ORNL/TR-2012/01), October 2012.

214. J. Dion, M. K. Howlander, and P. D. Ewing, “Wireless Network Security in Nuclear Facilities,” NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010. (Adams Accession No. ML103210371)

215. B.J. Kaldenbach, et. al., “Assessment of Wireless Technologies and Their Application at Nuclear Facilities,” Oak Ridge National Laboratory, NUREG/CR-6882, July 2006. (Adams Accession No. ML062140045)

216. M. Howlader, C.J. Kiger and P.D. Ewing, “Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Environment,” Oak Ridge National Laboratory, NUREG/CR-6939, July 2007. (Adams Accession No. ML072210179)

217. EPRI 3002017641, “EPRI Research Helps Ontario Power Generation (OPG) Deploy Its First Wireless Sensor Network at One Plant,” Electric Power Research Institute, Palo Alto, CA, Dec 23, 2019.

218. Y. Zhang, B. Jaques, and V. Agarwal, “Final Technical Report on Nanostructured Bulk Thermoelectric Generator for Efficient Power Harvesting for Self-powered Sensor Networks,” Boise State University, March 2018.

219. V. Agarwal and Z. Ren, “Sensors and Instrumentation Award Summaries,” Nuclear Energy Enabling Technologies – Advanced Sensors and Instrumentation, May 2016.

220. E. Eagle, B. Venkataraman, and D. Hardesty, “Embedded Digital Device Regulatory Issue Summary Update Embedded Digital Device Workshop,” Workshop on Safe Use of EDDs, October 08, 2014. (ADAMS Accession No. ML14281A535)

221. G. Clefton, “Overview - Embedded Digital Devices,” Workshop on Safe Use of EDDs, October 9, 2014. (ADAMS Accession No. ML14280A548)

222. E. Lee, “Cyber Security,” Workshop on Safe Use of EDDs, October 9, 2014. (ADAMS Accession No. ML14280A537)

223. U.S. NRC RIS 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” May 31, 2018. (ADAMS Accession No. ML18143B633)

224. Nuclear Energy Institute, “Guidelines for 10 CFR 50.59 Evaluations,” Appendix D [Draft], “Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications,” NEI 96-07, Appendix D, December 20, 2016. (ADAMS Accession No. ML17075A371)

225. United States Government Accountability Office, Report to Congressional Committees, “Internet of Things, Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD,” GAO-17-668, July 2017.

226. B. D. Shumaker, A. H. Hashemian, H. M. Hashemian, and R. T. Wood, “Summary Report of Technical Findings from Workshop on Qualification of Embedded Digital Devices,” DOE Report M3CA-15-TN-UTK-0703-032, AMS Corp., Knoxville, TN, July 2016.

227. U.S. NRC BTP 7-19, Rev. 7, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems Review Responsibilities,” August 2016. (ADAMS Accession No. ML16019A344)

228. R. T. Wood, et. al., “Development of a Model Based Assessment Process for Qualification of Embedded Digital Devices in NPP Applications: Research Approach and Current Status,” 2017. https://www.semanticscholar.org/paper/DEVELOPMENT-OF-A-MODEL-BASED-ASSESSMENT-PROCESS-FOR-Wood-Hashemian/c01e2e66782aa8dde9bb75aabe568b49e3677fd7

229. B. D. Shumaker et. al., “Development and Demonstration of a Model Based Assessment Process for Qualification of Embedded Digital Devices in Nuclear Power Applications Technical Report, Summary Report of Technical Findings from Workshop on Qualification of Embedded Digital Devices,” July 25, 2016.

230. A. Melin, R. Kisner, and R. Vidrio, “Embedded Instrumentation & Control for Extreme Environments,” Advanced Sensors and Instrumentation, Issue 5, September 2016.

231. B. Shumaker, R. Wood, C. Elks, and C. Smidts, “Qualification of Embedded Digital Devices in Instrumentation,” Advanced Sensors and Instrumentation, Issue 6, March 2017.

232. C. Elks, T. Bakker, and M. Gibson, “Verifiable Digital I&C and Embedded Digital Devices for Nuclear Power,” Advanced Sensors and Instrumentation, Issue 6, March 2017.

233. S. Schuppner, “DOE-NE Digital I&C Research,” IAEA Technical Meeting on Critical Challenges with Digital Instrumentation and Control Systems at Nuclear Power Plants, October 8-11, 2019.

234. DOE Office of Nuclear Energy, Advanced Sensors and Instrumentation Award Summaries, “Development of Model Based Assessment Process for Qualification of Embedded Digital Devices in NPP Applications,” June 2018.

235. P. Picca, “Relationship between the IAEA NE series report on digital COTS and the new IAEA safety report on smart devices IAEA technical meeting 19th February 2020,” Vienna, Austria, February 19, 2020.

236. R. Whitley, “Non Power Reactor: “MOX Project Commercial Grade Dedication Challenges,” June 21, 2012. (ADAMS Accession No. ML12171A541)

237. SAE International, “Guidelines for Development of Civil Aircraft and Systems,” SAE ARP 4754A, December 21, 2010.

238. U.S. Food and Drug Administration (FDA), “General Principles of Software Validation; Final Guidance for Industry and FDA Staff,” January 11, 2002. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation

239. U.S. Department of Health and Human Services Food and Drug Administration, “Guidance for Industry Q9 Quality Risk Management, Annex I: Risk Management Methods and Tools,” June 2006. https://www.fda.gov/media/71543/download

240. International Electrotechnical Commission, “Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA),” IEC 60812 Edition 3.0, Geneva, Switzerland, 2018-08.

241. Federal Energy Regulatory Commission, Major Orders and Regulations. https://www.ferc.gov/enforcement-legal/legal/major-orders-regulations

242. National Aeronautics and Space Administration, “Standard for Models and Simulations,” NASA-STD-7009A W/CHANGE 1, Approved: 2016-07-13.

243. R. Katz, R. Barto, and K. Erickson, “Logic Design Pathology and Space Flight Electronics,” NASA Goddard Space Flight Center, 1997.

244. 29 CFR § 1910.119, “Process safety management of highly hazardous chemicals,” January 1, 2019.

245. Letter from R. E. Fairfax, to L. M. Ferson, Manager of Standards Services, ISA, “Compliance with PSM and ANSI/ISA-S84.01 for safety instrumented systems,” March 28, 2000. https://www.osha.gov/laws-regs/standardinterpretations/2000-03-23

246. Occupational Health and Safety Administration, U.S. Department of Labor, “What is a Nationally Recognized Testing Laboratory (NRTL).” https://www.osha.gov/dts/otpca/nrtl/nrtl_faq.html#employers_regulators

247. Occupational Health and Safety Administration, U.S. Department of Labor, “Type of Products Requiring NRTL Approval.” https://www.osha.gov/dts/otpca/nrtl/prodcatg.html

248. Organisation for Economic Co-operation and Development, Nuclear Energy Agency, CNRA Working Group on the Regulation of New Reactors, “Report of the Survey on the Design Review of New Reactor Applications, Volume 1, Instrumentation and Control,” NEA/CNRA/R(2014)7, 28-Jul-2014.

249. Swedish Radiation Safety Authority, “Licensing of safety critical software for nuclear reactors, Common position of international nuclear regulators and authorised technical support organisations,” 2010 BEL V, BfS, Consejo de Seguridad Nuclear, ISTec, NII, SSM, STUK, 2007. https://inis.iaea.org/collection/NCLCollectionStore/_Public/41/028/41028258.pdf

250. CSA Group, “Qualification of pre-developed software for use in safety-related instrumentation and control applications in nuclear power plants,” CSA N290.14-07 (R2012).

251. Atomic Energy of Canada Limited, “Standard for Software Engineering of Safety Critical Software,” AECL CE-1001-STD, Revision 2, 12/01/1999.

252. French Nuclear Safety Authority, “Seventh French Report under the Convention on Nuclear Safety,” August 2016. https://www-ns.iaea.org/downloads/ni/safety_convention/7th-review-meeting/france-7th-report-national-csn.pdf

253. AFCEN Subcommittee RCC-E, “Design and construction rules for electrical and I&C systems and equipment,” 2016. https://afcen.com/en/publications/rcc-e/42/rcc-m-2012

254. Federal Ministry for the Environment, nature conservation and nuclear safety, “Safety Requirements for Nuclear Power Plants,” SiAnf, BMU, Berlin, 2015.

255. Kerntechnische Ausschuss (KTA), “Reactor protection system and surveillance devices of the safety system,” Safety Standard KTA 3501, November 2015. http://www.kta-gs.de/e/standards/3500/3501_engl_2015_11.pdf

256. The Association of German Engineers/Association of German Electricians, “Requirements of commercial grade products and criteria for their use in the instrumentation and control systems important to safety in nuclear power plants - General part, Guideline,” 3528 Blatt 1, VDI/VDE, Düsseldorf/Frankfurt am Main, 2017.

257. G. Karmakar and Y. Nirgude, “AERB SG D-25 and IEC 60880 for certification of software in safety systems of Indian NPP,” *Proceedings of International Conference on VLSI, Communication, Advanced Devices, Signals & Systems and Networking (VCASAN-2013)*, Volume: Lecture Notes in Electrical Engineering Vol. 258 Bangalore, July 2013. https://www.researchgate.net/publication/267116185_AERB_SG_D-25_and_IEC_60880_for_certification_of_software_in_safety_systems_of_Indian_NPP

258. Atomic Energy Regulatory Board, “Computer Based Systems of Pressurised Heavy Water Reactors,” AERB Safety Guide AERB/NPP-PHWR/SG/D-25, Mumbai-400 094, India, January 2010. https://www.aerb.gov.in/storage/images/PDF/CodesGuides/NuclearFacility/NPPDesign/3.pdf

259. H. Singh, “Regulatory Requirements and Review Process for Qualification of Smart Devices for Use in NPPs,” IAEA Technical Meeting, Vienna, February 17-21, 2020.

260. N. Agrawal, “Issues & Challenges in Qualification of Smart Transmitters in Indian Nuclear Power Plants,” IAEA Technical meeting on the Safety Aspects of Using Smart Digital Devices in Nuclear Systems Important to the Safety of Nuclear Power Plants, Vienna, Austria, 17 to 21 February 2020.

261. Nuclear Regulatory Authority, “Outline of New Regulatory Requirements (Design Basis),” April 3, 2013. https://www.nsr.go.jp/data/000067117.pdf

262. Korea Institute of Nuclear Safety, “KINS Safety Review Guidelines (SRG) for Light Water Reactor,” KINS/GE-001, 2015.

263. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Station,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, 19 December 2003.

264. U.S. NRC SRP Appendix 7.0-A, Rev. 6, “Review Process for Digital Instrumentation and Control Systems,” August 2016.

265. Yun Goo Kim, “Smart Device and CCF analysis in APR1400,” IAEA Technical Meeting on Smart Devices, Vienna, 17-21 February 2020.

266. F. Ullah, “Safety Aspects of Using Smart Digital Devices in Nuclear Systems,” Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Systems, IAEA Headquarters Vienna, Austria, 17 to 21 February 2020.

267. B. Mircea, “Smart Devices In Cernavoda NPP,” IAEA Technical Meeting on the Safety Aspects of Using Smart Digital Devices in Nuclear Systems Important to the Safety of Nuclear Power Plants, IAEA Headquarters Vienna, Austria, 17 to 21 February 2020.

268. Personnal communication Mircea Barbu to M. D. Muhlheim, June 4, 2020.

269. M. Anton Iacobet, “Current status of the regulatory activities related to computer security,” IAEA Technical meeting on the Safety Aspects of Using Smart Digital Devices in Nuclear systems Important to the Safety of Nuclear Power Plants, Vienna, Austria, 17 to 21 February 2020.

270. International Society of Automation, “Method for evaluating the performance of positioners with analog input signals and pneumatic output,” ANSI/ISA S75.13.01, Research Triangle Park, North Carolina, 2013.

271. Federal Nuclear and Radiation Safety Authority of Russia (Gosatomnadzor of Russia), “General Regulations on Ensuring Safety of Nuclear Power Plants,” OPB-88/97, NP-001-97 (PNAE G- 01 011-97), 1997.

272. V. Sivokon and D. Chichikin, “Challenges of NPP I&C System Digitization, International Considerations,” IAEA Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Important to the Safety of NPPs, 17-21 February 2020.

273. E. Andropov, “Third Approach: Between ‘Analogue’ and ‘Smart’,” Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Systems, IAEA Headquarters Vienna, Austria, 17 to 21 February 2020.

274. S. Guerra, “Smart Device Justification in the UK, The Cogs Approach,” IAEA Technical Meeting on Safety Aspects of Using Smart Digital Devices in Nuclear Important to the Safety of NPPs, 17-21 February 2020.

275. Staff Requirements Memorandum (SRM) to SECY-98-144, “White Paper on Risk-Informed and Performance-Based Regulation,” March 1, 1999. (NRC ADAMS Accession No. ML003753601)

276. EPRI 3002011817, “Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power,” Final Report, Electric Power Research Institute, Palo Alto, CA, July 2019.

277. G. Johnson, “Comparison of IEC and IEEE standards for computer-based control systems important to safety,” in 2001 IEEE Nuclear Science Symposium Conference Record, 2001, no. HCSS++, pp. 2474–2481.

278. J. S. Lee and K. Kwon, “Comparison of the Software Safety Criteria between IEC and IEEE Standards for the Digital Instrumentation and Control System,” in Transactions of the Korean Nuclear Society Autumn Meeting, 2006, pp. 1–2.

279. T. S. Lockhart, “Vetting Smart Instruments for the Nuclear Industry,” Moore Industries-International, Inc., September 2015. https://www.miinet.com/images/pdf/whitepapers/Vetting_Smart_Instruments_for_the_Nuclear_Industry_White_Paper_Moore_Industries.pdf

280. Reference Manual 00809-0100-4808, Rev CA, “Rosemount 3051N Smart Pressure Transmitter for Nuclear Service,” June 2008. https://www.emerson.com/documents/automation/manual-rosemount-3051n-smart-pressure-transmitter-for-nuclear-service-en-89488.pdf

281. Personal communication from Mark Bowell, Principal Inspector – Nuclear Safety, Sellafield DFW Division, to D. S. Halverson, NRC, February 5, 2020.

282. R. T. Wood, et al., “First Annual Progress Report,” DOE Report M3CA-15-TN-UTK_-0703-033, The University of Tennessee, Knoxville, TN, September 2016.

283. American Petroleum Institute , “Process Control Systems—Process Control Systems Functions and Functional Specification Development,” API Recommended Practice 554, Part 1, Second Edition, July 2007, Reaffirmed, November 2016.

284. American Petroleum Institute , “Process Control Systems—Process Control System Design, Downstream Segment,” API Recommended Practice 554, Part 2, First Edition, October 2008, Reaffirmed, November 2016.

285. American Petroleum Institute , “Risk-Based Inspection Methodology April 2016, API Recommended Practice 581, Third Edition, Addendum 1, April 2019.

286. MicroComputer Data Processing Company, “Glossary of functional safety standards," https://mcdpinc.com/glossary

287. U.S. NRC Generic Letter 89-02, “Actions to Improve the Detection of Counterfeit and Fraudulently marketed Products,” March 21, 1989.

288. U.S. NRC Generic Letter 91-05, “Licensee Commercial-Grade Procurement and Dedication Programs,” April 9, 1991.

289. U.S. NRC, “The Vendor Times,” December 2018. (ADAMS Accession No. ML18312A422)

290. U.S. NRC BTP 7-18, Revision 6, “Guidance on The Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems,” August 2016. (ADAMS Accession No. ML16019A327)

291. EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in NPPs,” Electric Power Research Institute, Palo Alto, CA, December 1996.

292. U.S. NRC Safety Evaluation Report, “Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-107330, "Generic

Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," July 30, 1998. (ADAMS Accession No. ML12205A265)

293. EPRI 1008256, Rev. 1, "Plant Support Engineering: Guidelines for the Technical Evaluation of Replacement Items in NPPs—Revision 1," Electric Power Research Institute, Palo Alto, CA, 2006.

294. EPRI 3002005326, "Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems," Electric Power Research Institute, Palo Alto, CA, June 30, 2016.

295. EUROCAE (European Organisation for Civil Aviation equipment) ED-79/ARP-4754, Certification considerations for highly-integrated or complex aircraft, EUROCAE, 17 Rue Hamelin, 75783 Paris, Cedex 16, France, 1996.

296. Y. Papadopoulos and J. A. McDermid, "The potential for a generic approach to certification of safety critical systems in the transportation sector," Reliab. Eng. Syst. Saf., vol. 63, no. 1, pp. 47–66, Jan. 1999.

297. International Atomic Energy Agency, "Safety of Nuclear Power Plants: Design," IAEA Specific Safety Requirements No. SSR-2/1, Vienna STI/PUB/1534, January 2012.

298. International Atomic Energy Agency, "Safety of Nuclear Power Plants: Commissioning and Operation," IAEA Specific Safety Requirements No. SSR-2/2 (Rev. 1), Vienna, 2016.

299. International Atomic Energy Agency, "Terminology Used in Nuclear Safety and Radiation Protection," Vienna, IAEA Safety Glossary, 2018 Edition.

300. P. Picca, "Relationship between the IAEA NE series report on digital COTS and the new IAEA safety report on smart devices," IAEA technical meeting Vienna, Austria, 19 th February 2020.

301. D. Fournier, "Safety Report NSNI-18-23, Safety Aspects of Using Smart Devices in Nuclear Systems Important to Safety," IAEA technical meeting Vienna, Austria, February 17–23, 2020.

302. International Electrotechnical Commission, "Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)," IEC 62340, Edition 1.0, Geneva, Switzerland, 2007-12.

303. International Electrotechnical Commission, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 7: Overview of Techniques and Measures", Second Edition, IEC 61508-7 Ed. 2.0, Geneva, Switzerland, April 2010.

304. International Electrotechnical Commission, "Examples of methods for the determination of safety integrity levels," IEC 61508-5, Edition 2.0, Geneva, Switzerland, 2010-04.

305. International Accreditation Forum, "About US." https://www.iaf.nu//articles/About/2

306. International Electrotechnical Commission, “Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies,” ISO/IEC 17011, Geneva, Switzerland, 2017-11.

307. International Electrotechnical Commission, “Conformity assessment—Requirements for bodies certifying products, processes and services,” BS EN ISO/IEC 17065:2012, Geneva, Switzerland, 2012.

308. Nuclear Energy Institute, “ “Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications” NEI 17-06, Revision B, September 2019.

309. International Electrotechnical Commission, , “Evaluation methods for microprocessor-based instruments,” NPR-IEC/TS62098,2001.

310. International Electrotechnical Commission, , “Transmitters for use in industrial process control systems; Part 3: Methods for evaluation of intelligent transmitters” IEC 60770-3, Ed. 2, .0, b:2-014.

311. International Organization for Standardization (ISO), “Quality Management Systems—Requirements,” ISO 9001:2015, October 21, 2015.

312. Exida, “Results of the IEC 61508 Functional Safety Assessment Project: DVC6200 SIS Digital Valve Controler and Position Monitor,” October 18, 2019.

313. International Society of Automation, “Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidelines for the determination of the required safety integrity levels,” ANSI/ISA-61511-3-2018 / IEC 61511-3:2016, Research Triangle Park, North Carolina, Approved 11 July 2018.

314. British Standard Institution (BSI), “Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)—Part 1: Basic Requirements and Generic Process,” BS EN 50128:1999, 1999.

315. International Electrotechnical Commission, “Medical Device Software - Software Life Cycle Processes,” ISO/IEC 62304, Geneva, Switzerland, 2006.

316. Radio Technical Commission for Aeronautics (RTCA), “Software Considerations in Airborne Systems and Equipment Certification,” Radio Technical Commission for Aeronautics, DO-178C, 2011.

317. M. D. Muhlheim, et. al., “Assessment of Applicability of Standards Endorsed by Regulatory Guides to Sodium Fast Reactors,” ORNL/SR-2017/520, September 2017.

318. IEEE 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, September 11, 2009.

319. U.S. NRC Regulatory Guide 1.168, Revision 2, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” July 2013. (ADAMS Accession No. ML13073A210)

320. IEEE P1891, “Standard Criteria for Application of Intelligent Digital Devices to Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NRC ADAMS Accession No. ML14280A578

321. International Society of Automation, “Guidelines for the Application of ANSI/ ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative,” ISA-84.00.01-2004 Part 2 (IEC 61511-2 Mod), Research Triangle Park, North Carolina, 2 September 2004.

322. Organisation for Economic Co-operation and Development Nuclear Energy Agency, “Vendor Inspection Co-operation Working Group (VICWG).” http://www.oecd-nea.org/mdep/working-groups/vicwg.html

323. G. Galletti, “NRC Vendor Inspection Update,” NUPIC General Membership and Vendor Meetings, June 2014. (ADAMS Accession No. ML14150A118)

324. D. R. Wallace, L. M. Ippolito, and B. B. Cuthill, “Reference Information for the Software Verification and Validation Process,” NIST Special Publication 500-234, April 1996.

325. U.S. Department of Commerce, National Institute of Standards and Technology, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations,” NIST SP 800-161, April 2015.

326. Office of Nuclear Regulation, “A guide to Nuclear Regulation in the UK, 2016 Update,” 2016. http://www.onr.org.uk/documents/a-guide-to-nuclear-regulation-in-the-uk.pdf

327. J. Masters and J. Britton, “How To Achieve EN 50128 Compliance,” PR QA Programming Research. https://www.perforce.com/resources/qac/how-achieve-en-50128-compliance ₽

328. UK Office for Nuclear Regulation, “Categorisation of Safety Functions and Classification of Structures, Systems and Components,” NS-TAST-GD-094, Revision 1, July 2019. http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-094.pdf

329. Occupational Safety and Health Administration, Process Safety Management. https://www.osha.gov/SLTC/processsafetymanagement/

330. Occupational Safety and Health Administration, Standard Interpretations, “Use of ANSI/ISA S84.00.01-2004 Parts 1-3 (IEC 61511 MOD) to comply with OSHA's Process Safety Management standard.” https://www.osha.gov/laws-regs/standardinterpretations/2005-11-29

331. Avanceon, “Standards and Tools – MES & Automation.” https://avanceon.com/standards-and-tools/

332. IEEE 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, Approved June 27,1991.

APPENDIX A DEFINITIONS

Augmented quality

Augmented quality is an optional subset of the classification category non-safety-related [A.5]. It may be applied to any item that is subject to non-safety-related regulatory requirements or special requirements imposed by the customer.

Automation

Any technique, method, or system of operating or controlling a process which reduces human intervention to a minimum and does not require continuous input from an operator [A.14].

Basic component (10 CFR 21.3)

(1)(i) When applied to NPPs licensed under 10 CFR part 50 or part 52 of this chapter, basic component means a structure, system, or component, or part thereof that affects its safety function necessary to assure:

(A) The integrity of the reactor coolant pressure boundary;

(B) The capability to shut down the reactor and maintain it in a safe shutdown condition; or

(C) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in § 50.34(a)(1), § 50.67(b)(2), or § 100.11 of this chapter, as applicable.

(ii) Basic components are items designed and manufactured under a quality assurance program complying with appendix B to part 50 of this chapter, or commercial grade items which have successfully completed the dedication process.

(2) When applied to standard design certifications under subpart C of part 52 of this chapter and standard design approvals under part 52 of this chapter, basic component means the design or procurement information approved or to be approved within the scope of the design certification or approval for a structure, system, or component, or part thereof, that affects its safety function necessary to assure:

(i) The integrity of the reactor coolant pressure boundary;

(ii) The capability to shut down the reactor and maintain it in a safe-shutdown condition; or

(iii) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in §§ 50.34(a)(1), 50.67(b)(2), or 100.11 of this chapter, as applicable.

(3) When applied to other facilities and other activities licensed under 10 CFR parts 30, 40, 50 (other than nuclear power plants), 60, 61, 63, 70, 71, or 72 of this chapter, basic component means a structure, system, or component, or
part thereof, that affects their safety function, that is directly procured by the licensee of a facility or activity subject

to the regulations in this part and in which a defect or failure to comply with any applicable regulation in this chapter, order, or license issued by the Commission could create a substantial safety hazard.

(4) In all cases, basic component includes safety-related design, analysis, inspection, testing, fabrication, replacement of parts, or consulting services that are associated with the component hardware, design certification, design approval, or information in support of an early site permit application under part 52 of this chapter, whether these services are performed by the component supplier or others.

Closed-loop (feedback) control

A control system in which the controlled quantity is measured and compared with a standard representing the desired performance. Note: Any deviation from the standard is fed back into the control system in such a sense that it will reduce the deviation of the controlled quantity from the standard [A.2].

Commercial grade item (10 CFR 21.3)

(1) When applied to NPPs licensed pursuant to 10 CFR Part 50, *commercial grade item* means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified).

(2) When applied to facilities and activities licensed pursuant to 10 CFR Parts 30, 40, 50 (other than NPPs), 60, 61, 63, 70, 71, or 72, *commercial grade item* means an item that is:

(i) Not subject to design or specification requirements that are unique to those facilities or activities;

(ii) Used in applications other than those facilities or activities; and

(iii) To be ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalog).

Configurable software

Software that is commercially available that allows the user to modify the functioning of the software in a limited way to suit user needs within clearly defined limits. Configurable software is an out-of-the-box solution that allows the owner to personalize certain aspects of the software themselves, without the help of experienced software developers. Configurable software is flexible, scalable and can be continually shaped through a human-machine interface to meet and organization’s industry-specific and organization-specific needs.

Control action (automatic control)

Of a control element or a controlling system, the nature of change of the output effected by the input. Note: The output may be a signal or the value of a manipulated variable. The

input may be the control loop feedback signal when the command is constant, an actuating signal, or the output of another control element [A.2]

Dedicating entity (10 CFR 21.3)

When applied to NPPs licensed pursuant to 10 CFR Part 50, *dedicating entity* means the organization that performs the dedication process. Dedication may be performed by the manufacturer of the item, a third-party dedicating entity, or the licensee itself. The dedicating entity, pursuant to § 21.21(c) of this part, is responsible for identifying and evaluating deviations, reporting defects and failures to comply for the dedicated item, and maintaining auditable records of the dedication process.

Dedication (10 CFR 21.3)

1. When applied to NPPs licensed pursuant to 10 CFR Part 30, 40, 50, 60, *dedication* is an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed ***equivalent to an item designed and manufactured under a 10 CFR Part 50, appendix B, quality assurance program***. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at holdpoints at the manufacturer's facility, and analysis of historical records for acceptable performance. In all cases, the dedication process must be conducted in accordance with the applicable provisions of 10 CFR Part 50, appendix B. The process is considered complete when the item is designated for use as a basic component.
2. When applied to facilities and activities licensed pursuant to 10 CFR Parts 30, 40, 50 (other than NPPs), 60, 61, 63, 70, 71, or 72, dedication occurs after receipt when that item is designated for use as a basic component.

Dedication provides reasonable assurance that the commercially manufactured item conforms to its design and will perform its intended safety function. As noted in the introduction to 10 CFR 50, Appendix B, control under a 10 CFR 50, Appendix B–compliant QA program provides adequate confidence that a structure, system, or component will perform satisfactorily in service.

Table A-1 Control Under 10 CFR 50, Appendix B Program Vs. Dedication Under CGD [A.1]

Control under Appendix B–compliant QA program	Commercial grade dedication
Original equipment manufacturer	Third party / licensee
Access to original design requirements	Does not necessarily have access to original design requirements
Knows what design requirements are important to ensure design functions can be performed	A failure modes and effects or other analysis is needed to postulate critical characteristics
Is verifying important design requirements using Appendix B QA program controls	Might need to use reverse engineering techniques to determine acceptance criteria/tolerances
Uses Appendix B controls to ensure materials and parts used meet the original design requirements (drawings, specifications, etc.)	Does not use Appendix B controls to ensure materials and parts used meet the original design requirements (drawings, specifications, etc.)

Dedication is not a central tenet of QA—it is an alternative acceptance method that is performed under the auspices of an Appendix B–compliant QA program.

- Dedication is an acceptance process that finds its basis in 10 CFR 50, Appendix B, Criterion VII (Table A-2)

Table A-2 Dedication is Based on Criterion VII in 10 CFR 50, Appendix B [A.1]

10 CFR 50, Appendix B, Criterion VII, Control of Purchased Material, Equipment, and Services	EPRI 3002002982
Measures shall be established to assure that purchased material, equipment, and services, whether purchased directly or through contractors and subcontractors, conform to the procurement documents. These measures shall include provisions, as appropriate, for source evaluation and selection, objective evidence of quality furnished by the contractor or subcontractor, inspection at the contractor or subcontractor source, and examination of products upon delivery. . .	Method 2 – Commercial Grade Survey Method 4 – Item/Supplier performance Method 3 – Source Surveillance Method 1 – Special Tests and Inspection

Digital component (RIS 2016-05)

Digital components include executable code or software-developed programmable logic that is permanently or semi-permanently installed within the device (commonly referred to as firmware). [A.15]

Dumb instruments

Dumb instruments do not feature a microprocessor, firmware or similarly contrived performance. They include simple mechanical pressure switches and older design transmitters based on op-amps, etc. [A.19].

Embedded digital device

A component consisting of one or more digital electronic parts that use software, software-developed firmware, or software-developed logic that is integrated into plant equipment [A.16].

Firmware

The combination of a hardware device and computer instructions and data that reside as **READ-ONLY** software on that device. The software cannot be readily modified under program control [A.17].

Firmware refers to a small piece of code that can reside in non-volatile memory. [A.18]

Non-modifiable non-configurable firmware is deliverable as an integral part of the items, where the computer instructions and data can only be modified by replacement of the hardware device. Firmware that can change features based on changes to a configuration baseline is considered configurable software.

Non-modifiable configurable firmware is delivered as an integral part of the items, with a limited ability to adjust functionality by modifying configuration parameters, via a set-up process.

Modifiable-configurable firmware is delivered as an integral part of the items, where the computer instructions and data can be modified, including at run time.

RIS 2016-05 [A.15] states that “Firmware includes, but may not be limited to, devices such as programmable logic devices, field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), erasable programmable read only memory (EPROM), electrically erasable programmable read only memory (EEPROM), and complex programmable logic devices (CPLDs).”

Function

A *function* is a defined objective or characteristic action of a system or component. For example, an I&C system may have inventory control as its primary function [A.2]. A *plant function* is an I&C function to control, operate, and/or monitor a defined part of a process. An I&C function may be subdivided into a number of subfunctions (for example, measuring function, control function, actuation function) for the purpose of allocation to I&C systems [A.3].

Functionality

Functionality attributes identify significant functional activities and actions that are performed by the EDDs. This attribute addresses the functionality provided by an EDD that enables the implementation of its functions.

To understand functionality, the uses of the terms *functionality*, *function*, *safety*, and *safety-related* must be understood. From this, the functionality of the EDD can be understood in its proper perspective.

Functionality includes the capabilities of the various computational, user interface, input, output, data management, and other features provided by a digital product (i.e., platform) [A.2].

Functionality represents the operations that must be carried out [A.4]. Functions generally transform input information into output information. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.

HAL (hardware abstraction layer)

HAL is a layer of programming that allows a computer operating system to interact with a hardware device at a general or abstract level rather than at a detailed hardware level [A.22]. Thus, HAL allows desktop applications to discover and use the hardware of the host system.

The application programming interface (**API**), enables software modules to communicate with each other by using common objects and data exchange mechanisms [A.23], regardless of the type of the underlying hardware.

Important to safety

The term *important to safety* is not defined in 10 CFR 50.2 or in the NRC glossary; however, for electric equipment the term “important to safety” is defined in 10 CFR 50.49(b) as comprising equipment that (b)(1) is safety-related, (b)(2) is not safety-related, but the failure of which could impact safety, and (b)(3) certain post-accident monitoring equipment as described in Regulatory Guide 1.97.

Limited functionality

A device of limited functionality has the following characteristics [A.8]:

- It contains predeveloped software or programmed logic;
- It is autonomous and performs only one conceptually simple principal function, which is defined by the manufacturer and which is not modifiable by the user;
- It is not designed to be reprogrammable;
- If it is reconfigurable, the configurability is limited to parameters relating to compatibility with the process being monitored or controlled, or interfaces with connected equipment.

Middleware

The use of middleware isolates the applications software and the operating system. The middleware is a layer of software that is between and interfaces with both the operating system (OS) and the applications software [A.24]. Thus, all interactions between the applications software and the OS take place through the middleware. Middleware is an effective technique for isolating safety-critical functionality.*Not safety related*

Not safety related is commonly referred to as *nonsafety* or *nonsafety related*.

Open-loop control system (general)

A system in which the controlled quantity is permitted to vary in accordance with the inherent characteristics of the controlsystem and the controlled power apparatus for any given adjustment of the con troller. Note: No function of the controlled variable is used for automatic controlof the system. It is not a feedback control system [A.2].

Plant function

A *plant function* is an I&C function to control, operate, and/or monitor a defined part of a process. An I&C function may be subdivided into a number of subfunctions (for example, measuring function, control function, actuation function) for the purpose of allocation to I&C systems [A.3].

Process variable

Safety limits, which are chosen to maintain the integrity of physical barriers, can be defined in terms of directly measured process variables [A.25]. Those parameters or quantities that are controlled at the correct limit are called Process Variables [A.26]. Because process variables change, instrumentation systems measure the variable then control the variable to keep the variable within the given limits. Process variables are part of a process/system that is being monitored and/or controlled. Pressure, temperature, flow and level are examples of process variables.

Qualification

ISL defined qualification as used in industry practice as follows [A.5]:

Qualification: (1) As used in the aerospace industry, qualification is a systematic process through which software tools are verified to be suitable for their intended use(s) and to the extent possible, to be free of deficiencies that could adversely affect critical DI&C system software or result in failure to detect deficiencies in that software.

Quality Assurance

10 CFR 50, Appendix B establishes quality assurance (QA) requirements for the design, manufacture, construction, and operation of those structures, systems, and components. The pertinent requirements of this appendix apply to all activities affecting the safety-related functions of those structures, systems, and components; these activities include designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

As used in this appendix, the term *quality assurance* comprises all those planned and systematic actions necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service. QA includes quality control (QC), which comprises those QA actions related to the physical characteristics of a material, structure, component, or system which provide a means to control the quality of the material, structure, component, or system to predetermined requirements.

Risk-significant

Risk-significant licensing basis events are those with frequencies within 1% of the Frequency-Consequence Target with site boundary doses exceeding 2.5 mrem. The use of the 1% metric is consistent with the approach to defining risk-significant event sequences in the PRA standards.

Safety function

A *safety function* is one of the processes or conditions (e.g., negative reactivity insertion, emergency core cooling system [ECCS], containment isolation) essential to maintaining plant parameters within acceptable limits established for a design basis event [A.6, A.7, A.8].

Safety-related

10 CFR 50.2 defines *safety related* SSCs in terms of reliance on those SSCs to remain functional during and after design basis events.

The term *safety-related* is used to describe systems that are required to perform a specific function or functions to ensure risks are kept at an accepted level. Such functions are, by definition, *safety functions*. Any system, implemented in any technology, which carries out safety functions is a safety-related system. Two types of requirements are necessary to achieve functional safety [A.9]:

- safety function requirements (what the function does), and
- safety integrity requirements (the likelihood of a safety function being performed satisfactorily).

Safety-related SSC

Safety-related SSCs describes those SSCs that are relied upon to remain functional during and following design basis events to assure [A.10]:

1. The integrity of the reactor coolant pressure boundary
2. The capability to shut down the reactor and maintain it in a safe shutdown condition; or
3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

Safety significant function

10 CFR 50.69 defines a *safety significant function* as "A function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk. Thus, systems that are highly safety significant are those whose failure can result in high consequences [A.11]."

The safety-significant function in 10 CFR 50.69 does not replace the existing safety-related and non-safety–related categorizations. Rather, 10 CFR 50.69 divides these categorizations into two subcategories based on high or low safety significance that blends risk insights into the categorization process.

Software failure

IEC 61513 for NPP I&C systems [A.3] defines a software failure as a "system failure due to activation of a design fault in a software component." It is noted in the standard that "[a]ll software failures are due to design faults, since software consists solely of design and does not wear out or suffer from physical ffailure. Since the triggers which activate software faults are encountered at random during system operation, software failures also occur randomly." See also "failure", "fault", "software fault" in IEC 61513 [A.3].

Solid-state device

Solid-state gets its name from the path that electrical signals take through solid pieces of semi-conductor material [A.27]. Solid-state devices, such as a transistor, use conductors to control the flow of signals through a circuit. An integrated circuit (IC) chip is a collection of transistors and wires that hook them together.

A.1 REFERENCES

A.1 M. H. Tannenbaum and J. Simmons, "Control of Items Under 10 CFR 50, Appendix B With, and without, commercial grade item dedication," NRC Workshop on Vendor Oversight, June 14, 2018. (ADAMS Accession No. ML18150A371)

A.2 IEEE Std. 100-2000, "Authoritative Dictionary of IEEE Standards Terms," Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2000.

A.3 International Electrotechnical Commission, "Nuclear Power Plants—Instrumentation and Control for Systems Important to Safety—General Requirements for Systems," IEC 61513, Geneva, Switzerland, August 2011.

A.4 U.S. NRC SRP BTP 7-14,Rev. 6,"Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." (ADAMS Accession No. ML16019A308)

A.5 J. Servatius, S. Alexander, and T. Gitnick, "Evaluation of Guidance for Tools Used to Develop Safety-Related Digital Instrumentation and Control Software for NPPs, Task 2 Report: Analysis of the State of Practice," ISL-ESRD-TR-14-03, August 2014. (ADAMS Accession No. ML15043A206)

A.6 EPRI TR-103669-V1, "Programmable Logic Controller Qualification Guidelines for Nuclear Applications, Volume 1: Technical Information and Guidelines," Electric Power Research Institute, Palo Alto, CA, October 1994.

A.7 International Atomic Energy Agency, “Safety of Nuclear Power Plants: Design,” IAEA Safety Standard Series Requirements NS-R-1 :2016, Vienna, 2016.

A.8 International Atomic Energy Agency, “Design of Instrumentation and Control Systems for Nuclear Power Plants,” IAEA Specific Safety Guide No. SSG-39, Vienna, 2016.

A.9 International Electrotechnical Commission, “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508,” IEC/TR 61508-0:2005, Geneva, Switzerland, September 2005.

A.10 10 CFR 50.2, “Definitions.”

A.11 10 CFR 50.69, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors.”

A.12 International Electrotechnical Commission, “Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations,” IEC 61508-4, Geneva, Switzerland, 2010.

A.13 ISO/IEC/IEEE 24765, “Systems and software engineering — Vocabulary,”, International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) / Institute of Electrical and Electronic Engineers (IEEE), Geneva, Switzerland, 2010.

A.14 Dictionary.com, “Automation.” https://www.dictionary.com/browse/automation

A.15 U.S. NRC RIS 2016-05, “Embedded Digital Devices in Safety-Related Systems,” April 29, 2016. (ADAMS Accession No. ML15118A015)

A.16 E. O. Eagle Jr., U.S. NRC Office of New Reactors, “Embedded Digital Device Issue in Plant Safety and Design Certification,” November 2013. (ADAMS Accession No.ML13317A004)

A.17 U.S. Department of Defense, “Standard Practice for System Safety,” MIL-STD-882E, 11 May 2012.

A.18 M. Rouse, DEFINITION embedded system. https://internetofthingsagenda.techtarget.com/definition/embedded-system

A.19 T. S. Nobes, “Smart Instruments in Safety Instrumented systems—Sellafield Experiences,” Measurement + Control, Vol 41/6, July 2008. https://journals.sagepub.com/doi/pdf/10.1177/002029400804100603

A.20 IEEE/EIA 12207.1-1997, “Information technology—Software life cycle processes—Life cycle data,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, April 1998.

A.21 Radio Technical Commission for Aeronautics, “Software Considerations in Airborne Systems and Equipment Certification,” RTCA DO-178C, December 2011.

A.22 M. Rouse, Hardware Abstraction Layer (HAL). https://whatis.techtarget.com/definition/hardware-abstraction-layer-HAL

A.23 IEEE Std C37.1-2007, “IEEE Standard for SCADA and Automation Systems,” Institute of Electrical and Electronics Engineers, Piscataway, NJ, May 8, 2008.

A.24 U.S. Department of Defense, “Joint Software Systems Safety Engineering Handbook,” Version 1.0, Published August 27, 2010.

A.25 T. [Edward) Quinn, J. Mauck, R. Bockhorst, and K. Thomas, “Digital Sensor Technology,” INL/EXT-13-29750, July 2013.

A.26 Sivaranjith, “What is process variable and types of process variables?,” Automation Forum, December 2017. https://automationforum.in/u/sivaranjith

A.27 “What does solid-state mean in relation to electronics?,” How stuff works. https://electronics.howstuffworks.com/questions558.htm

APPENDIX B COMPONENT TYPES

Eighteen types of components were identified as likely to have connected or internal EDDs and be used in NPPs in safety related applications (Table B-1). This list is not a complete list of components that may include EDDs, but a down-selection process was necessary to determine the widespread use of EDDs and how they are used.

This process focused on vendors and devices positioned to be included in nuclear power plants in the near term. Vendors operating outside of the nuclear industry in less safety critical applications are known to use more complex functionality in their EDDs than described in the sections below.

In the down-selection process, services (non-components), passive components (e.g., piping), and structural components (including cable trays) were removed from further review.

Table B-1 Types of Components in Safety Related Applications in NPPs Likely to have EDDs

Chart (data) recorders	Priority logic modules
Circuit breakers	Pumps
Diesel generators	Radiation monitors
Flowmeters	Relays, time-delay relays
Gas analyzers	Temperature transmitters
Level meters	Uninterruptible power supplies (UPSs)
Motor control centers (MCCs)	Valve actuators
Power supplies	Valves
Pressure transmitters	Voltage regulators

B.1 Chart Recorder

The vendor search identified four vendors of chart recorders and data readout devices that have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in chart recorders and to determine the types of functional roles allocated to the devices.

Digital chart recorders are examples of a component that can have multiple functions. Chart recorders use video display units (VDUs) to display information to operators and touch screens to provide parameter, display, and alarm control. The data from the recorders can be made available using various communications protocols to other users.

The digital chart recorders identified through this search emulated their analog replacements. For example, the trend graphs on the VDUs look like the output from analog trend or strip-chart recorders. Not surprisingly, the human systems integration (HSI) provided by most man-machine interface system (MMIS) vendors today simply makes the analog HSI equipment into similar looking images on digital VDUs [B.1]. Few vendors seem to re-think the problem of process data display and control when moving to digital technologies. In fact, the digital upgrade of Mission Control Center (MCC) at the Johnson Spaceflight Center can provide insights for the nuclear

industry with respect to displaying information and the use of chart recorders. Insights from the conversion of the MCC from analog to digital include the following [B.2]:

- The older, more experienced flight controllers preferred the mainframe/monochrome system, while the new controllers preferred the real-time data system color workstations.

- Having color graphics workstations that emulated the old displays wasted much of the color graphics capability.

- The original displays in the prototype system presented a large and potentially bewildering amount of information to the flight controller.

- High reliability is achievable—the new MCCs operate around the clock and ideally have no more than 20 minutes of downtime a year.

The advantages of digital chart recorders are that they can provide multiple displays that can be sequential or channel-selected digital indication of the channel readings and provide the operator interface for configuration. Alarms indicate an alarm condition on any display. With digital technology, microprocessors can be used to make ongoing controller adjustments based on the actual, real time process dynamics. Thus, the functionality of chart recorders can be greatly increased over the alanog counterparts.

The chart recorders may be used in safety related applications. For example, Yokogawa Corporation of America's chart recorders [B.3] have been qualified under a 10 CFR 50, Appendix B program and can monitor and record up to 4, 12, 48 or 500 channels of data. These recorders, because they are recording data to be stored and analyzed, can have greater connectivity through a flash card slot, USB port, and ethernet connection.

B.2 Circuit Breakers

The vendor search identified 23 vendors of circuit breakers; of these, 5 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in circuit breakers and to determine the types of functional roles allocated to the devices.

Engineers from a major industry supplier provided an overview on the availability and use of embedded digital components or piece parts of low voltage circuit breakers—identified as smart or intelligent devices. If desired, their low voltage circuit breakers may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

For medium voltage circuit breakers, digital monitoring or control may be implemented via smart protective relays.

Low voltage circuit breakers equipped with embedded digital control features are capable of full control based on values of desired parameters, such as voltage, current, frequency, power factors, diagnostic results, etc. Circuit breakers equipped with embedded digital monitoring features may display similar parameters of interest, such as current, voltage, frequency, power factors, diagnostic results, etc. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Medium voltage circuit breakers equipped with embedded digital control features implemented via smart or intelligent protective relays located either at or distant to the circuit breaker are capable of full control based on values of selected parameters, such as current, voltage, frequency, power factors, diagnostic results, etc. Circuit breaker protective relays equipped with embedded digital monitoring features may display similar parameters of interest, such as current voltage, frequency, power factors, diagnostic results, etc. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Communications capabilities with the embedded digital equipment are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

One supplier that was contacted writes its own firmware in-house for circuit breakers, which is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, or function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

Vendors indicated they perform an extensive range of factory acceptance testing that would be made available depending on customer requirements, and they could include job-specific failure modes and effects analyses if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment to be used in NPPs.

B.3 Diesel Generators

The vendor search identified 16 vendors of diesel generators; of these, 3 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in diesel generators and to determine the types of functional roles allocated to the devices.

Diesel generators are complex devices requiring numerous control and monitoring systems, such as engine starting, fuel, speed control, cooling, and lubrication systems, plus electrical load sequencing and voltage regulation.

B.3.1 DG Transfer Switches

Engineers from a major industry supplier provided an overview on the availability and use of embedded digital components or piece parts of DG transfer switches: smart or intelligent devices. If desired, transfer switches may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

Transfer switches equipped with embedded digital control features are capable of full control based on values of desired parameters, such as current, voltage, frequency, power factors, diagnostic results, etc. Transfer switches equipped with embedded digital monitoring features may display similar parameters of interest such as current, voltage, frequency, power factors, diagnostic results, etc. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Communications capabilities with the embedded digital equipment are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

One supplier contacted writes its own firmware in-house for DG transfer switches, which is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, or function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

An extensive range of factory acceptance testing is available depending on customer requirements and could include job-specific failure modes and effects analyses, if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment to be used in NPPs.

B.4 Flowmeter

The vendor search identified seven vendors of flowmeters that have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in flowmeters and to determine the types of functional roles allocated to the devices.

Flow meters can be magnetic, coriolis, or vortex flow meters.

Magnetic flow meters are also known as *electromagnetic flow meters* or *mag meters*, and they are comprised of a transmitter and sensor that together measure flow. The magnetic flow meter's sensor is placed inline and measures an induced voltage generated by the fluid as it flows through a pipe. The transmitter takes the voltage generated by the sensor, converts the voltage into a flow measurement, and transmits that flow measurement to a control system.

Vortex flow meters do not use impulse lines, and there are no moving parts to maintain or repair, less leak potential, and a wide flow turndown range. Vortex meters can be used in remote areas. Additionally, vortex meters are unique in that they can accommodate liquids, gasses, steam and corrosive applications. Vortex flow meters are also able to withstand high process pressures and temperatures. An integral temperature sensor enables temperature compensated mass flow for

saturated steam. Mass flow, volumetric flow, or temperature are available as configurable outputs.

Coriolis flow meters are composed of a sensor, which contains the measurement tubes, and a transmitter, which displays the outputs and allows the meter to be configured to the process. Coriolis flow measurement can provide simultaneous measurement of mass flow, density, temperature and viscosity. A coriolis flowmeter has one or more measuring tubes which an exciter causes to oscillate artificially. As soon as the fluid starts to flow in the measuring tube, additional twisting is imposed on this oscillation due to the fluid's inertia. Two sensors detect this change of the tube oscillation in time and space as the "phase difference." This difference is a direct measure of the mass flow. In addition, the fluid density can also be determined from the oscillation frequency of the measuring tubes. The temperature of the measuring tube is also registered to compensate thermal influences. The process temperature derived from this is available as an additional output signal.

The flow meters provide diagnostics to monitor component health and an operator display. Flow meters for use in process industries can provide smart wireless adapters with communication capabilities.

B.5 Gas Analyzers

The vendor search identified 26 vendors of gas analyzers; of these, 3 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in gas analyzers and to determine the types of functional roles allocated to the devices.

An engineer with a major industrial vendor of H_2/O_2 gas analyzers for 1E Containment Atmosphere Monitoring System (CAMS) provided an overview of their design and production processes. The gas analyzers measure gas concentrations in containment from 500 ppm to 100%.

The design of the gas analyzers uses ANSI/ASME NQA-1-2000 to meet the 10 CFR 50 Appendix B criteria. Seismic, environmental, and EMI testing of the gas analyzers follow NRC endorsed standards.

The system is arranged into two assemblies, a remote control center and a sample station assembly. The remote control center includes a PLC-based control and conditioning assembly, a touch screen display, and a system switch panel. The remote control center is designed for mild environment locations, and the sample station is designed for operation in the harsh post-accident conditions.

During normal operating conditions, the gas analyzers are in direct contact with the sample. During post-accident conditions, the containment atmosphere includes super-heated steam. By terminating the heat trace on the inlet sample line upstream of the analyzer ~8 feet, the temperature in the sample line cools down to the dew point.

The CAMS takes analog input from sensors within containment and then uses the PLC to determine H_2 partial pressure and total pressure. An analog signal is then sent to the control room for an alarm on high hydrogen partial pressure or if high total pressure occurs. The alarm values are plant specific per technical specifications. Plant response is also plant specific (operator actions for turning fans on, venting, hydrogen recombiners, etc.).

The PLC assembly provides all on-off control logic for the sample loop assembly and data processing for the sensors. The conditioner performs the necessary calculations and outputs the results in three forms: analog signals, a visual indication, and alarms.

The PLC is provided to the vendor by a supplier and is programmed with proprietary software. The PLC includes a set of modules selected to process data accumulated from the local analyzer sample station, provide logic output for operation of all sample station ON-OFF functions, and provide information to the field in the forms of analog output signals, alarm contact closures, and as a visual display.

B.6 Level Meter

The vendor search identified seven vendors of level meters that have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in level meters and to determine the types of functional roles allocated to the devices.

Water level measurements in nuclear applications include level measurements in fuel pools, vessels, and sumps. Wireless transmission of its output signal can allow the transmitters to be installed in accessible indicator location(s) using either wired or wireless technology.

Intelligent buoyancy/displacement transmitters are designed to measure liquid level, interface, or density of liquids based on the Archimedes buoyancy principle. Buoyancy level sensors and switches include horizontal floats, vertical floats, and displacer switches of all kinds. Displacement instruments determine liquid level by sensing the buoyant force exerted on a displacer by the liquid it displaces, unlike float-type level instruments, in which the displacer moves very little relative to the rising or falling liquid.

Water (or liquid) levels can also be measured by ultrasonic technology. Unlike typical sight-glass or differential pressure indications using long runs of tubing, the ultrasonic technology is not susceptible to erroneous readings caused by air accumulation or constrictions in the tubing. Ultrasonic technology is not sensitive to differing pressures, such as would be experienced during RCS vacuum refill evolutions.

Guided wave radar (GWR) sensors, both permanently installed is another level measurement technology for a wide variety of process media and conditions, including water at saturation (boiling) conditions.

Many level measurement instruments are microprocessor-based that communicate liquid level, specific gravity (density), and liquid level interface. HART or FOUNDATION™ Fieldbus communications protocols are standard protocols. An HMI interface provides access to information, easy remote configuration and supervision with a PC or HART terminal or by using the local keys.

B.7 Motor Control Centers (MCCs)

The vendor search identified 18 vendors of MCCs; of these, 5 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in MCCs and to determine the types of functional roles allocated to the devices.

Engineers from a major industry supplier provided an overview on the availability and use of embedded digital components or piece parts of MCCs: smart or intelligent MCCs. If desired, their MCCs may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

MCCs equipped with embedded digital control features are capable of full control—start, stop, control based on values of desired parameters, such as voltage, current, frequency, power factors, diagnostic results, etc. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Communications capabilities with the embedded digital equipment in the MCCs are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

One supplier contacted writes its own firmware in-house, which is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, or function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

An extensive range of factory acceptance testing is available depending on customer requirements and could include job-specific failure modes and effects analyses, if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment to be used in NPPs.

As an example of the functionality of the MCCs, the display system for the Siemens tiastar (not capitalized by Siemens) Smart Motor Control Center with SmartStart displays the data for the following [B.4]:

- SIMOCODE pro for full-voltage non-reversing and reversing starters
- Siemens variable frequency drives
- SIRIUS 3RW44 soft starters
- Siemens WL circuit breaker
- The display panel emulates the front view of the MCC.

The tiastar Smart MCC also provides control for each starter device via:

- SmartStart control station mounted in the MCC
- Field-mounted 120 VAC pilot devices
- Ethernet-connected PLC/DCS system

B.8 Pressure Transmitters

The vendor search identified 43 vendors of pressure transmitters; of these, 8 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in pressure transmitters and to determine the types of functional roles allocated to the devices.

An engineer with a major industrial vendor of nuclear and commercial grade instrumentation and valves provided an overview of their design and production processes. As an illustration of the size of the vendor, product literature notes over 10 million of a particular model pressure transmitter have been installed worldwide. For nuclear applications, 10 CFR 50 Appendix B criteria govern all processes. For non-nuclear applications, processes are ISO 9001 compliant. For both nuclear and non-nuclear use, significant product testing takes place, including intensive audits of a fraction of the production run to ensure all performance specifications are met.

Digital components make up a large share of the non-nuclear commercial market, with increasing penetration since the 1990s. Wireless communications are widely available in commercial products and provide productivity and diagnostics elements. ASICs to meet design specifications are used in some applications. The vendor assembles its own boards or procures pre-populated boards for which individual parts are specified. The vendor does its own programming of its digital devices and systems. Process controls of comparable levels are used for both software and circuit board products. Design and bill of material revisions are conducted under traceability requirements that include model numbers, serial numbers, and date codes.

B.9 Priority Logic Modules

The vendor search identified 5 vendors of priority logic modules (PLMs); of these, 3 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in PLMs and to determine the types of functional roles allocated to the devices.

PLMs are an interface between actuators and multiple commanding systems (e.g., safety, control, manual). Section 2 of DI&C-ISG-04 refers to these devices as *priority modules* [B.5].

A PLM receives device actuation commands from multiple safety and non-safety sources and sends the command having highest priority on to the actuated device (Figure B-1). Priority logic is implemented with software, firmware, or a combination. Logic is required to determine which incoming command has priority to control safety equipment in order to meet NRC requirements. The actuated device can be a safety-related component such as a motor actuated valve, a pump motor, a solenoid-operated valve, etc. The priority module must also be safety related.

Areva's AV-42 Priority Logic Module was to be the central interface in the protection system and was also referred to as a *priority control module* (Figure B-1). The Taiwan 1&2 plants have numerous AV-42 modules actuating 627 outputs [B.6].

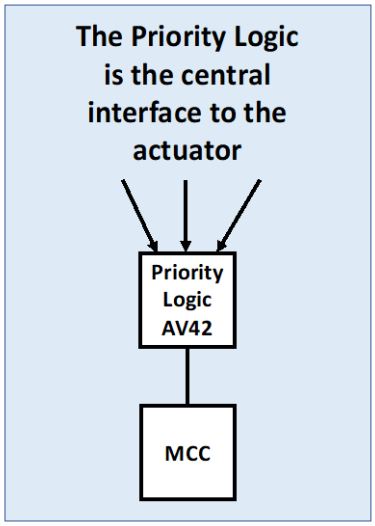


Figure B-1 AV-42 Priority Logic Module

Invensys's Triconex PLM receives diverse actuation commands from 1E-qualified safety and nonsafety sources such as safety systems, diverse systems, emergency control panels, and the operator's normal HMI. Once received, the PLM sends the highest priority command to an actuation device such as a solenoid valve or a pump motor.

A PLM is also known as a component interface module (CIM) used in the APR1400. A CIM at the APR1400 is used, among other things, to interface the output signals from the engineering safety features-component control system (ESF-CCS) digital controllers to the plant's safety components (e.g., pumps, valves, dampers) to allow control of each component based on automatic safety actuation signals and manual safety actuation signals from plant operators. For most applications, a single CIM controls a single engineered safety feature (ESF) plant component. Each CIM is used to control one plant component.

A PLM may be considered different than an EDD. Both can be hardware or software (firmware) and can provide diagnostics, communication, and monitoring. However, the PLM has multiple inputs and the output is based on the priority of the inputs.

The key component in the CIM design is a FPGA. Its first use is within the Westinghouse AP1000 nuclear reactor protection and safety monitoring system. The CIM incorporates advanced features to allow for diagnostics, testability, and modularity. The main features of the CIM include:

- Command prioritization and component control for discrete plant components
- I/O for control of plant component, indication of component status and connection to plant systems
- Serial communication protocols for a reduction in hard-wired interfaces
- Online testing capabilities for rapid indication of component faults and assistance in troubleshooting and plant maintenance

- Local control and indications provide additional test and troubleshooting capabilities

B.10 Power Supplies

The vendor search identified six vendors of power supplies that have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in power supplies and to determine the types of functional roles allocated to the devices.

Smart panels enable users to pinpoint overloads and inefficiencies proactively. Ethernet connections allow the smart panels to communicate to users directly and to manage electrical distribution assets in different locations. Data provided include energy information, as well as physical properties, including trip status, cycle count, and contact wear indicators.

Power conditioners (also known as a *line conditioners* or *power line conditioners*) are devices that can be used to improve the quality of the power that is delivered to electrical load equipment. When combined with voltage regulation, it provides noise filtering capabilities and surge protection to safeguard connected equipment against damage, degradation, or malfunction. Power conditioners filter the high frequency noise on the AC line. Circuit breakers, input filters, etc., can be interfaced in a power conditioning unit, depending on the application conditions and ripple current. None of the power conditioners reviewed had ethernet or communications capabilities.

The power supplies reviewed had internal diagnostics with visual diagnostic LEDs for input, and some had output status LEDs rather than an HMI, while others had a display that indicated voltages and currents simultaneously. The HMI screens can log data over time on one or more outputs to provide energy consumption over time. Some power supplies can be connected to a PC via an ethernet cable, allowing the test sequences to be automated and users to access data results. Data can then be exported to popular tools such as MATLAB and Microsoft Excel or Word for further analysis.

A power inverter, or *inverter*, is a power electronic device or circuitry that changes direct current (DC) to alternating current (AC). The input voltage, output voltage and frequency, and overall power handling depend on the design of the specific device or circuitry.

Surge protection devices / filters, power supplies, and UPSs can use a network protocol to interconnect control devices for data exchange.

B.11 Pumps (Pump Controllers)

The vendor search identified 59 vendors of pumps/pump controllers; of these, one has also designed, built, and installed an I&C system at an NPP. A focused survey of this vendor found their expertise to be in safety-related pumps that do not make use of EDDs. The survey was expanded to include vendors of pumps used in nuclear facilities other than those that installed an I&C system at an NPP.

Pump controllers can be used for managing pump flow and/or pressure, from full off to full on, and may incorporate flow or pressure control via varying pump speed or use of flow or pressure control valves, utilization bypass lines, etc., to help ensure the pump operates in the most efficient manner. When installed as part of an integrated control system, significant pump and system performance and reliability improvements may be achieved. Self-diagnostic capability provides pump performance and health evaluation in real time, plus historical trends and conditions.

Integrated controllers may provide responsiveness to large changes in flow or pressure and and/or precise control for small setpoint changes. Communication devices compatible with a number of standards can provide information that can be accessed anywhere along the loop. Digital communication provides easy access to the performance and condition of the pump as well as other integrated components. Controllers may be located remotely from processes. This flexibility can reduce exposure to hazardous environments and make it easier to evaluate the condition of pumps in hard-to-reach locations. Electronics may be fully encapsulated so that they resist the effects of vibration, temperature, and corrosive atmospheres. Modular design allows critical working components to be replaced without removing field wiring or pneumatic or hydraulic tubing, if used.

One vendor responded to contacts via its website and discussed the usage of EDDs in their pumps/pump controllers, describing the types of functional roles allocated to the devices. Like the other vendor contacted, this vendor does not use EDDs on pumps used in NPPs. The vendor noted that utility customers were adamant about equipment specification and process control in order to prevent changes to their presently approved control or operability licensing basis. For non-nuclear use, the vendor noted digital monitoring for pump performance with various network connection options, with parameters such as flow, vibration, temperature, and pressure.

B.12 Radiation Monitors

The vendor search identified 55 vendors of radiation monitors; of these, 4 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in radiation monitors and to determine the types of functional roles allocated to the devices.

The four vendors were contacted, and discussions were held with two. Both noted that their components widely use EDDs. One noted that it would not be practical to identify the specific components because there are too many.

Both noted applications in safety systems and non-safety systems. Components in safety systems were built to 1E and under 10 CFR 50 Appendix B or NQA-1 programs.

For general applications, one vendor mentioned several commercial power plant and research reactor implementations in the United States and noted long-term European use of digital reactor control systems. The vendor commented that the increasing performance of FPGAs was benefiting their implementation and did not carry the burden of OS software. However, they use ASICs, CPLDs, and microprocessors, as well, depending on the product. This vendor noted optical and hardwired network connections, with fiber backbones replacing prior generation master/slave configurations. In-house programming is used, as well as commercial software development tools. In-house programming was done in FORTRAN, C, or machine language. DevTrack was one software tool noted. Product version control is maintained, as is visible through display via a menu button. Factory acceptance testing is used to confirm performance. Customers may customize the testing program and witness the testing.

The vendor commented on difficulties in performing digital upgrades, noting a long wait for NRC approval of a research reactor digital upgrade and another research reactor operator choosing an analog upgrade because of anticipated delays for approving a digital system. The vendor also noted vendor component approval lists maintained for reactor sites and the benefit to industry in extending the vendor approvals across the industry.

The other vendor discussed layers of redundancy in components used in safety systems. The vendor noted that new chips were implemented as they became available in non-safety systems, primarily for performance benefits. The vendor employed project version control measures. For safety systems, updates were seldom required. For safety systems, devices have very limited connectivity and require validation activities. The vendor noted audits by customers, EPRI, etc., to ensure that requirements were met and processes were followed. Products are tested, documented, and certified as needed and required.

B.13 Relays, Time-Delay Relays

The vendor search identified 14 vendors of relays and time-delay relays; of these, 4 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in relays and time-delay relays and to determine the types of functional roles allocated to the devices.

Engineers from a major industry supplier provided an overview on the availability and use of embedded digital components or piece parts of relays: smart or intelligent devices for the many types of relays they make. If desired, relays may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

Relays equipped with embedded digital control features are capable of full control based on values of desired parameters, such as current, voltage, pressure, temperature, level, flow, frequency, power factors, diagnostic results, etc. Relays equipped with embedded digital monitoring features may display similar parameters of interest. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Communications capabilities with the embedded digital equipment are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

One supplier contacted writes its own firmware in-house. It is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, or function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

An extensive range of factory acceptance testing is available depending on customer requirements and could include job-specific failure modes and effects analyses if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment for use in NPPs.

B.14 Temperature Transmitters

The vendor search identified 28 vendors of temperature transmitters; of these, 6 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in temperature transmitters and to determine the types of functional roles allocated to the devices.

An engineer with a major industrial vendor of nuclear and commercial grade instrumentation and valves provided an overview of their design and production processes. For nuclear applications, 10 CFR 50 Appendix B criteria govern all processes. For non-nuclear applications, processes are ISO 9001 compliant. For both nuclear and non-nuclear use, significant product testing takes place, including intensive audits of a fraction of the production run to ensure all performance specifications are met.

Digital components make up a large share of the non-nuclear commercial market, with increasing penetration since the 1990s. Wireless communications are widely available in commercial products and provide productivity and diagnostics elements. ASICs to meet design specifications are used in some applications. The vendor assembles its own boards or procures pre-populated boards for which individual parts are specified. The vendor does its own programming of its digital devices and systems. Process controls of comparable levels are used for both software and circuit board products. Design and bill of material revisions are conducted under traceability requirements that include model numbers, serial numbers, and date codes.

B.15 Uninterrupted Power Supplies (UPSs)

The vendor search identified 28 vendors of UPSs; of these, 5 have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in UPSs and to determine the types of functional roles allocated to the devices.

Engineers from a major industry supplier provided an overview on the availability and use of embedded digital components or piece parts of UPSs: smart or intelligent devices. If desired, UPSs may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

UPSs equipped with embedded digital control features are capable of full control based on values of desired parameters such as voltage, frequency, battery charge, load, etc. The UPS automatically transfers to battery mode if a utility power outage occurs or if the utility power does not conform to specified parameters. UPSs equipped with embedded digital monitoring features may display similar parameters of interest. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements. The UPS monitors the battery charge condition and reports the status on the control panel. The battery is always connected to the UPS and is ready to support the inverter should the utility input become unavailable.

Communications capabilities with the embedded digital equipment are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

The UPS monitors its health and will automatically switch to bypass mode if it detects an overload, load fault, or internal failure. Bypass mode is an operating mode, not an alarm condition.

One supplier contacted writes its own firmware in-house. It is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, and function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

An extensive range of factory acceptance testing is available depending on customer requirements and could include job-specific failure modes and effects analyses, if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment for use in NPPs.

B.16 Valve Actuators

The vendor search identified 57 vendors of valve actuators; of these, two have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors was performed to identify the usage of EDDs in valve actuators and to determine the types of functional roles allocated to the devices.

It is possible in many cases to automate an existing manual valve, thereby replacing an existing manual process valve into an automated on/off or control valve [B.7]. Most modern ball valves have pre-drilled mounting holes that can be used to mount the actuator without compromising the integrity of the valve.

A valve actuator may be an intermediate device between a valve controller or positioner and the valve itself that implements the command for a valve to change position or it could include its own integral processor/controller. Digital signal processing would take place in the controller or the actuator processor and could incorporate measured parameters from the valve and valve actuator, such as position, pneumatic or hydraulic pressure, motor current or voltage, etc., that relate to component condition monitoring or many system process parameters when used for control purposes. Additional discussion is provided in the next section on valves (valve controllers) due to the significant overlap of signal processing functions of valve actuators and controllers in the two sections.

B.17 Valves (Valve Controllers)

The vendor search identified 84 vendors of valves/valve controllers; of these, two have also designed, built, and installed an I&C system at an NPP. A focused survey of these vendors and several others was performed to identify the usage of EDDs in valves/valve controllers and to determine the types of functional roles allocated to the devices. Valve controllers are attached to the valve and can also be installed on existing valves.

Valve controllers can be used for throttling control and on/off control. Fully encapsulated electronics resist the effects of vibration, temperature, and corrosive atmospheres. The controllers provide quick responsiveness to large step changes and precise control for small setpoint changes. They may incorporate logic solvers to further improve performance. A communication device can provide information that can be accessed anywhere along the loop. Digital communication provides easy access to the condition of the valve. This flexibility can reduce exposure to hazardous environments and make it easier to evaluate valves in hard to reach locations. The modular design allows critical working components to be replaced without removing field wiring or pneumatic tubing. When installed in an integrated control system, significant hardware and installation cost savings can be achieved. The self-diagnostic capability provides valve performance and health evaluation.

Diagnostics capabilities include real-time monitoring process and component parameters of the valve using on-board sensors built into or onto the valve and controller such as position, travel, supply and outlet pressure, air consumption, and internal component integrity. Alerts may be set to identify problems. Data may also be stored to support trend assessment and performance history. The collected data provide insights to the overall health of the valve and controller. Diagnostics may run continuously or on set intervals and may be integrated over many components.

Operational performance is enhanced through improved accuracy of the digital positioner. The improved accuracy is achieved by enabling consideration of a number of factors digitally to adjust the positioner output pressure. Self-tuning features improve the dynamic response of the associated control valve resulting in better process control. The digital nature of the positioners permits remote diagnostics to be performed routinely or whenever deemed appropriate.

Implementing digital positioners on critical control valves also enables online partial stroke testing of the control valve without upsetting the normal process control. This testing provides assurance that the control valve actually moves upon demand.

For installation in high radiation areas, high temperature, etc., the controllers can be installed hundreds of feet away from the valve.

These results are similar to the NEET program results that primarily identified residential and business uses of valve controllers, with the exception that valve controllers in an NPP can be qualified for harsh environments and used in safety-related applications.

A major industrial vendor of nuclear and commercial grade instrumentation and valves was contacted and provided an overview of their design and production processes. As an illustration of the size of the vendor, product literature notes over 10 million of one model of a pressure transmitter have been installed. For nuclear applications, 10 CFR 50 Appendix B criteria govern all processes. For non-nuclear applications, processes are ISO 9001 compliant. For both nuclear and non-nuclear use, significant product testing takes place, including intensive audits of a fraction of the production run to ensure all performance specifications are met.

Digital components make up a large share of their non-nuclear commercial market, with increasing penetration since the 1990s. Wireless communications are widely available in commercial products and provide productivity and diagnostics elements. ASICs to meet design specifications are used in some applications. The vendor assembles its own boards or procures pre-populated boards for which individual parts are specified. The vendor does its own programming of its digital devices and systems. Process controls are of comparable levels for

both software and circuit board products. Design and bill of material revisions are conducted under traceability requirements that include model numbers, serial numbers, and date codes.

A review of the retrofit of Fisher (Emerson) FieldVue™ digital valve controllers at the Pickering nuclear station in Ontario, Canada [B.8], illustrated the benefits and the regulatory process for implementing digital valve controllers in safety significant systems of a commercial nuclear power station. The digital valve controllers, with an estimated population of two million in use worldwide per this article, replaced obsolescent equipment that was becoming more difficult and more costly to support and maintain, and it offered potential performance improvements, as well. The use of the digital controllers on safety significant valves meant that concerns with their reliability and different failure modes than analog-based controllers be examined to demonstrate that the design basis of the plant would not be affected.

B.18 Voltage Regulators

The vendor search identified 8 vendors of voltage regulators; of these, 1 has also designed, built, and installed an I&C system at an NPP. A focused survey of this vendor was performed to identify the usage of EDDs in voltage regulators and to determine the types of functional roles allocated to the devices.

Engineers from one supplier contacted provided an overview on the availability and use of embedded digital components or piece parts of voltage regulators: smart or intelligent devices. If desired, voltage regulators may incorporate embedded digital equipment such as ASICs or microprocessors to provide (1) monitoring functions or (2) monitoring and control functions. Equipment diagnostics to ascertain component health and reliability are available using manufacturer-specific software.

Voltage regulators equipped with embedded digital control features are capable of full control based on values of desired parameters, such as current, voltage, frequency, power factors, diagnostic results, etc. Voltage regulators equipped with embedded digital monitoring features may display similar parameters of interest. Control logic and monitoring features may be modified via local access at the device or from remote network access based on the customers' requirements.

Communications capabilities with the embedded digital equipment are available for common network types and topologies. Broadcast messages to groups of devices are not permitted; each device must be individually specified. By default, no configuration changes are allowed on operating devices; however, this may be overridden by the customer.

The embedded digital equipment may perform the logic operations or an external device (e.g., PLC) may perform the logic operations. Degrees of embedded equipment or external devices performing the logic operations are supported. For example, a PLC may be the primary controller, but the embedded equipment could pick up control functions in the event of a PLC or communications failure.

One supplier contacted writes its own firmware in-house. It is typically implemented on dedicated IC chips. A style label is used with the component model number for configuration control purposes. Any change in form, fit, and function prompts a repeat of their system testing. It is not clear how field modifications would affect the style number and configuration control.

An extensive range of factory acceptance testing is available depending on customer requirements and could include job-specific failure modes and effects analyses, if needed.

Many of the suppliers contacted typically use third-party commercial grade dedicating entitys for equipment for use in NPPs.

B.19 References

B.1 R. T. Wood, et. al., “Emerging Technologies in Instrumentation and Controls,” NUREG/CR-6812 (ORNL/TM-2003/22), March 2003 (ADAMS Accession No. ML031900433).

B.2 M. D. Muhlheim, et. al., “Insights Gained for Updating an Analog I&C System to a Digital System,” NPIC&HMIT 2012, San Diego, CA, July 22–26, 2012.

B.3 Yokogawa Electric Corporation, “Daqstation DXAdvanced DX1000/DX2000,” Bulletin 04L41B01-01E. https://web-material3.yokogawa.com/BU04L41B01-01E.pdf

B.4 Siemens Industry, Inc (2016), “tiastar TM Motor Control Center Catalog and Application Guide.” Order No: CCPC-CATAG-0916 www.usa.siemens.com/mcc

B.5 Digital Instrumentation and Controls, DI&C-ISG-04, Revision 1, “Highly-Integrated Control Rooms—Communications Issues (HICRc)”, March 06, 2009 (ADAMS Accession No. ML083310185).

B.6 Memorandum to P. L. Hiland, from S. A. Arndt, “Subject: Report of Foreign Travel to the International Atomic Energy Agency Technical Meeting on the Impact of Digital Instrumentation and Control Technologies on the Operation and Licensing of Nuclear Power Plants in Beijing, China from November 2–8, 2008,” December 17, 2008.

B.7 R. Moore, Cross Co. “How to Automate an Existing Manual Valve,” Control Engineering, December 2018.

B.8 B. Fitzgerald, M. Cheng-Newsom, F. Mercaldi, “Pickering Exploits Digital Valve Technology,” Nuclear Engineering International, July 2015.

APPENDIX C SOFTWARE TOOLS

This Appendix is provided for informational purposes and is not an evaluation of software tools, as that was not selected as an area of focus for this project. However, it is expected that the use of software tools will become more significant in the future. This will require both being able to determine that use of those tools is acceptable, but also being able to credit them as appropriate for the evidence they can produce.

C.1 Introduction

Early software development methods relied on human inspection and testing for validation and verification; however, with increased automation (i.e., tool use) there is a comparable reduction in human involvement. That is, there is a tendency to rely on the software tools more. Although the use of software tools has always been a part of software development, there is a generally tendency to increase their use. When asked by ORNL, vendors indicated that they write software code by manual methods or use software tools to develop the code or for V&V depending on the customer and the application of the component.

The software in EDDs may be developed by software coders and through the use of software tools. The Information Systems Laboratories, Inc. (ISL) review of software development tools concluded that while it is unlikely that any tool can be certified as completely correct and error free, the use of a software development tool is generally considered to produce a better product than manual methods [C.1]. Many of the software tools in use have a large user base that provides feedback, are well supported, and have been in use long enough to be well tested. ISL's conclusion is that the risk of failures caused by using such a tool is less than the risk of failure from not using any tool. However, undetected faults in the automated tools or tool-assisted engineering activities may pose serious risks to nuclear safety. In either case, having a good process and consistent method to assess the safety of the software development is important to all stakeholders in the nuclear industry from equipment vendors, utility licensees, and government regulatory organizations.

C.2 Guidance

Although the NRC and Industry guidance is focused on safety systems, it is applicable to the software in EDDs and throughout the software lifecycle.

C.2.1 NRC Related Guidance

NRC's guidance in NUREG-0800 on the use of software tools [C.2] states that "The software tool should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If, however, it cannot be proven that defects not detected by software tools or introduced by software tools will be detected by V&V activities, the software tools should be designed as Appendix B quality software itself, with all the attendant regulatory requirements for software developed under an Appendix B program."

The prospect of using commercial off the shelf (COTS) software in NPPs and the development of software design software tools is not new. NUREG/CR-6421 [C.3], published in 1996, recommends that software tools[17] be rated for safety impact, initially evaluated using assurance

17 The original text of NUREG/CR-6421 references IEC 1226 and IEC 880. The new numbering system for IEC standards takes the old number + 60000 to create a new number, e.g. IEC 880 → IEC 60880, and IEC 1226 → IEC 61226.

methods for similar tools, and continuously evaluated during tool use. The NUREG/CR recommends that software tools could be placed in any one of the four categories depending on the tool function and the associated software classification (A, B, C, and unclassified). If a software tool can embed an error in other software important to safety, then the software tool is assigned the same category as the software in which the error can occur. If the software tool can only challenge software important to safety (e.g., exposing existing errors), then the software tool is assigned the next lower safety category. The NUREG/CR also presents prelimary COTS acceptance criteria (Table C-1).

Table C-1 Preliminary COTS Acceptance Criteria in NUREG/CR-6421

Description
Risk and hazards analyses shall be used to identify system-level safety functions required.
The safety functions (if any) that the COTS product will perform shall be identified.
The COTS product shall be under configuration and change control.
The safety category of the COTS product shall be determined depending upon category A, B, or C, respectively.

SRP BTP 7-14 states that “The SDP [software development plan] should require that tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools.” However, BTP 7-14 does not provide any specific guidance for qualifying the software tools. In short, the degree to which a tool is solely relied upon to ensure critical features are achieved, determines the degree to which it must be qualified. For example, a word processor that is used to prepare a printed paper document which is reviewed and approved, does not need to be qualified in any way because its output is independently (and completely) reviewed and approved.

BTP 7-14 does reference the software tool requirements from IEEE Std. 7-4.3.2-2003 (endorsed by Regulatory Guide 1.152, Rev. 3). IEEE Std. 7-4.3.2-2003 does not address justification for the selection of software tools and acceptance criteria for compilers, operating systems, and libraries but rather requires users to confirm the software tools are suitable for use. However, a major change implemented in the 2016 revision of IEEE 7-4.3.2 provides more specific criteria on the use of software tools used for digital devices and development of hardware, software, firmware, and programmable logic. IEEE 7-4.3.2-2016 [C.4] requires that software be developed, modified, or accepted in accordance with a software QA plan and that the software QA plan shall address the software tools used for system development and maintenance. This standard defines software tools as “A sequence of instructions and commands used in the design, development, testing, review, analysis, or maintenance of a programmable digital device or its documentation.” The software tools are further specified to be either developed to a similar standard as the safety-related software or the tools be used in a manner such that defects not detected by the tools should be detected by validation and verification (V&V) activities. That is, the associated development tools should not introduce problems.

Regulatory Guides (RGs) 1.152 and 1.168 through 1.173 provide some guidance on software used in safety systems, primarily through the endorsement of various IEEE standards. RG 1.152 focuses on establishing and maintaining a secure operational environment and a secure

development environment for system software. Because this guidance does not specifically address software tools, it is not clear if the software tools used to develop the software and the development environment of the software tool need to be secure for its use in developing safety-related software. That is, is the development of the software tools excluded from requiring a secure development environment. Obviously the software tools would need to be within the secure development and operating environment while in use on developing the safety related software. If the tools were dedicated through the verification option described in this section, then they would need to follow the same regulations as other safety software. IEEE 7-4.3.2 2016 includes a clause that such software tools shall be incorporated into the secure development and operational environment and controlled under configuration management.

Other ISL conclusions related to software tools and NRC include:

> *"The NRC should consider regulatory guidance that clarifies the distinction between COTS software that becomes part of the final software product and COTS tools that are used in the software development process.*
>
> *The NRC should consider regulatory guidance that requires automatically generated code to be scrutinized with the same rigor as hand-generated code."*

This could be addressed in updating guidance for software development and the tools used to develop software in RG 1.152 or BTP 7-14.

ISL noted that based on its analysis of software tool qualification practices and guidance used in industry that the qualification of software tools would not fit well into the NRC regulatory framework [C.1]. If a software tool were subject to the CGD process, appropriate critical characteristic would need to be identified. Critical characteristics of software tools that could be reviewed and tested could include a review of the development process, security, and quality, and testing for determinism, simplicity, and reliability.

ISL defined qualification as used in industry practice as follows:

> **Qualification**: (1) As used in the aerospace industry, qualification is a systematic process through which software tools are verified to be suitable for their intended use(s) and to the extent possible, to be free of deficiencies that could adversely affect critical DI&C system software or result in failure to detect deficiencies in that software.

C.2.2 Industry Practices

Software tools are becoming a more major part of development forcing their consideration, and beyond that could have regulatory utility in their ability to support V&V activities. Guidance and practices show that although there is a framework for their use there are issues.

ISL noted that the overwhelming consensus of industry practice with respect to verification, validation, and qualification of software tools is that such activities are only required if (1) the software tool output is not systematically verified (i.e., the output is verified every time the tool is used), (2) the software tool automates, eliminates, or reduces activities and tasks required by software development life cycle processes, and (3) the software tool is being used to develop safety-related software [C.1].

Most industries use a graded software classification scheme to determine the rigor applied to the software development process. Some of those industries use the software classification scheme

along with the type of software tool to determine the rigor necessary to verify, validate, or qualify of software tools used in the software development processes. The civil aviation industry has published a document (i.e., RTCA DO-330 [C.5]) that specifically covers software tool development and qualification including qualification of COTS software tools. The automotive industry (i.e., ISO 26262) and the European nuclear power industry (i.e., IEC 60880) recommend methods of qualifying software tools and provides guidance for those methods but lacks specific procedures for implementing the methods.

IAEA SSG-39 requires software tools to be verified and assessed consistent with tool reliability requirements, the type of tool, the potential of the tool to introduce fault or fail to make the user aware of existing faults, and the extent to which the tool may affect redundant elements of a system or diverse systems. Tools that can introduce faults or fail to detect faults need to be verified to a greater extent than other tools; however, verification is not necessary if the tool output is systematically and independently verified.

According to the former Multinational Design Evaluation Program (MDEP) Digital Instrumentation and Control Working Group (DICWG) Generic Common Position DICWG No 2 [C.6], the use of appropriate software tools can increase the integrity of the I&C development process and the software reliability by reducing the risk of introducing faults during the process. Tools can be used to capture system and software requirements; transform requirements into final system code and data; perform verification, validation, and testing; prepare and control application data; and manage and control processes. Tools can also reduce the effort required for testing and maintaining logs.

IEC 60880 [C.7] specifically addresses the use of software tools. The requirements in IEC 62138 are consistent with but less rigorous than the IEC 60880 requirements. IEC 62138 focuses efforts on tool certification and the certification of the tool development process rather than a rigorous tool qualification process. IEC 62138 [C.8] considers software tools to be support system software that is part of the system software in a typical I&C system and is either off-line or on-line (i.e., embedded in nonsafety support systems).

IEC 61226 [C.9] designates COTS software, including software tools, as safety class A, B, or C depending on the level of software produced and whether there exists a diverse alternative or another software tool that verifies the output. This places the same requirements for the software tools as those for the safety system requirements.

IEC 61508-7 [C.10] states that the certification of a tool will typically be certified against national or international standards. Ideally, the tools used in all development phases (specification, design, coding, testing and validation) and those used in configuration management, should be subject to certification. To date, only compilers (translators) are regularly subject to certification procedures. IEC 61508 further notes that certified tools and certified translators are usually certified only against their respective language or process standards. And are usually not certified in any way with respect to safety.

CSA N-290.14-15 [C.11], in use by The Canadian Nuclear Safety Commission (CNSC), extends the software tool requirements of IEC 61508 and requires that the failure modes for each use of the software engineering tool should be considered and the relevant failure effects on the target software should be identified. The three-step process in Appendix D of this standard first determines the impact severity of the tool failure, the presence of any mitigating circumstances, and the assessment approach based on the first two steps.

1. The potential impact severity of the tool failure classifies the effects of failure into one of the following five categories based on its potential impact on the safety, functionality, reliability, performance, or security requirements of the related candidate product [C.11]:

    a) Direct — the tool has been incorporated within the candidate product, and as a result, tool failure effect can directly prevent the candidate product from meeting its requirements. Accordingly, the tool should be treated as a pre-developed digital item and shall be qualified to the same degree of rigor as the target digital item (e.g., a software library included in a custom software digital item).

    b) Indirect-causal — a tool failure effect can introduce errors in the candidate product which, if undetected, could result in the tool failing to meet its requirements (e.g., a compiler).

    c) Indirect-preventive — a tool failure effect can result in the non-detection of errors (e.g., during verification) in the candidate product which could result in the failure to meet its requirements.

    d) Minimal — a tool failure effect can have an impact on the candidate product, but no mechanism has been identified that could result in the candidate product failing to meet its requirements.

    e) No impact — a tool failure effect can have no impact on the candidate product in meeting its requirements.

2. Mitigating circumstances of the failure that eliminate or reduce the impact of the failure effect are divided into three groups:

    a) None — there are no circumstances which mitigate the impact of the failure.

    b) Single — there is a single, reliable mitigating activity or procedure which defends against the impact (e.g., testing, review, checksum comparison, etc.).

    c) Multiple — there are multiple (more than one) reliable mitigating activities or procedures which defend against the impact (e.g., different tests with overlapping coverage, a combination of verification processes and procedural factors, etc.).

3. The assessment approach (Category1, Category 2, Category 3, or “0”) is identified based on the candidate product’s categorization, the impact severity of the tool failure, and the mitigating circumstances. For Category1, 2, or 3, the software engineering tool is treated as if it were a digital item of the identified category.

The FAA requires that all software tools be identified, validated, and addressed within the software development activities and documentation [C.12]. This software may include computer-aided software engineering (CASE) tools, data in these tools, compilers, test tools, test data, simulations, emulations, utilities, configuration management tools, databases and data files, and other software. For the FAA, software is classified based on how an error affects the software and the system that contains the software. The software classification defines the rigor necessary to demonstrate compliance with software development requirements.

The FDA guidance for medical device software [C.13] recognizes that developers are beginning to use component-based development tools and techniques. Object-oriented methodologies and the use of off-the-shelf software components hold promise for faster and less expensive software development. However, component-based approaches require very careful attention during integration. Prior to integration, time is needed to fully define and develop reusable software code and to fully understand the behavior of off-the-shelf components. Similar to other industries, FDAs guidance states that "[software] tools should have a degree of quality no less than the software product they are used to develop."

DoD, in its guide for achieving reliability, availability, and maintainability [C.14], states that RAM Design Tools can be used to conduct formal design reviews and can use the specific tools for addressing RAM such as FMEA, FTA, RBD, WCCA, LCC, and Testability Analysis (TA), reliability tests, embedded diagnostic and prognostic instrumentation in the design, and a logistic support analysis.

The aerospace industry assigns software tools in a classification separate from the embedded system software, whereas the civil aviation industry classifies software tools to the same level as the software developed with the tool [C.1]. The aerospace industry classifications are based on effects of anomalous behavior of the software rather than software functionality.

In 1980, a special committee (SC-145) of the Radio Technical Commission for Aeronautics (RTCA) was created to develop guidelines for evaluating software used on aircraft. Avionics systems are not certified directly but are evaluated as part of the aircraft as a whole [C.15]. The primary method for qualifying software tools is in accordance with RTCA DO-330 [C.5]. RTCA DO-330 relies on the development, verification, and validation of software tools in accordance with a high-quality and well-organized life cycle process. Alternative tool qualification methods include using service history, exhaustive input testing, formal methods, and use of dissimilar tools. Unlike most other industries that superficially address COTS software tools, RTCA DO-330 provides a comprehensive qualification process for COTS tools that divides qualification responsibilities between the COTS developer and tool user [C.1].

The alternative tool qualification methods in RTCA DO-330 are analogous to CGI dedication when there is not much information available from the vendor beyond the published product description and a user's manual, and commercial-grade surveys (EPRI Method 2) or source verifications (EPRI Method 3) are impractical leaving only special tests and inspections (EPRI Method 1) and use of supplier and product performance history (EPRI Method 4). ISL noted that RTCA DO-330 contains a tool qualification liaison process that contains similar activities and tasks as DI&C-ISG-06 to facilitate the review and approval of software tools.

Similar to other industries, NASA documents [C16, C17, C18, C19, C20, C21] state that software tools used in developing software that is used in safety-critical systems should be identified and the level of rigor associated with the verification, validation, and accreditation of software tools should be determined by the tool functions and the safety classification of the systems in which the software will be used [C.1].

BS EN 50128 [C.22] contains requirements and guidance for software tool selection, use, documentation, and qualification for the railway industry. BS EN 50128 also provides a comprehensive process for determining the confidence level in software tools used in the software development process similar to the tool qualification level used in the civil aviation industry. The BS EN 50128 safety-related software development life cycle process only depends on the tool

functionality. Tools are assigned to one of three classes and all tools must be assigned to one of these classes depending on their potential to affect the executable code (Table D-2).

Table C-2 Classes of Software Tools

Class	Description	Example
T1	Tool output does not contribute to executable code	Text editor Version control software (VCS)
T2	Tool tests / verifies design or executable code; cannot introduce defects into the executable code, but may fail to detect existing defects	Static analysis tool Code coverage test tool
T3	Tool output contributes to executable code	Compiler Linker

The T1 class applies to tools that affect neither the verification nor the final executable. T2 applies to tools where a fault could lead to an error in the results of verification or validation. An example of a T2 tool is a coding standard checker. T3 applies to tools which, if faulty, could introduce errors into the final executable (for example a compiler).

ISL noted that based on its analysis of industry practice, all industries should expand coverage of software tool requirements to cover software tool use in all phases of software development and all types of software tools to minimize the potential hazards of using tools [C.1]. Clause 5.3.2 of IEEE Std. 7-4.3.2-2016, revised after ISLs review, addresses the quality of software tools throughout the software lifecycle.

In Japan, a symbolic language (Problem Oriented Language—POL) is used to provide an intuitive structured representation of the software specifications (interlock block diagrams) that is implemented through graphically driven coding tools [C.23]. Additionally, simplicity of software structure is promoted through simple logic, cyclical execution, static resource usage, and avoidance of external interrupts. Thus, the Japanese nuclear power industry emphasizes consensus software development practices that are intended to facilitate software verification and validation as a primary means for minimizing the potential for systematic software faults.

C.3 Approved Platforms

Software tools are used not only at the component level but at the system level. Examples of specific tools are provided below.

Framatome Technologies Control STAR system is a modular, digitally programmable system that is designed for safety-related applications in nuclear power plants. The Software Application Management System (SAMS) is a program generation software tool that allows the user to construct control algorithms for Control STAR using a personal computer [C.24]. SAMS is Windows-based and menu-driven, so Control STAR can be programmed by control personnel, without any special computer programming skills. Programming Control STAR simply requires selecting functional building block icons from the SAMS library and connecting them on the screen. The software converts the functional diagram to a BASIC code used by the module.

Schneider Electric used an automated software development tool called SAGA for its SPINLINE 3 system. This tool was used to develop most of the SPIN N4 software, which contains ~200,000 lines of 1E "C" code. The CLARISSE System and Software Development Environment of SPINLINE 3 includes SCADE, which is the evolution of SAGA, and all the tools to produce automatically generated executable code. The SPINLINE 3 has already been widely used on several NPPs for Safety and Safety-related applications at KOZLODUY, QINSHAN, DUKOVANY (in 2000). The previous version of the SPINLINE 3 system – the SPIN N4 – has been implemented at the N4 nuclear power plants in France (Chooz and Civaux) for RPS and RCLS. The NRC approved the SPINLINE 3 in 2014 [C.25].

Software tools were used extensively in the development of the RadICS, which was reviewed by the NRC in its review of the RadICS Safety System Digital Platform. The RadICS Topical Report (TR) lists eight different software tool types and eleven specific software tools that are used during RadICS logic development activities. The functions of each tool are described in the TR and a tool classification is assigned based upon specific tool characteristics and usage. The TR also identifies configuration items generated for each software tool. Software tools used for RadICS function block logic (FBL) and Electronic Design (ED) development were not themselves developed in accordance with the RadICS Appendix B QA. These software tools are used in a manner such that defects not detected by the software tools will be detected by V&V activities described in the RadICS V&V Plan and corrected through the RadICS corrective action programs. The NRC approved the RadICS in 2019 [C.26].

C.4 Conclusions

Different industries, agencies, and organizations have different criteria for qualifying software tools and their use. For example, the NRC states that software tools should be used in such a manner that defects not detected by the software tool will be detected by V&V activities, but if this cannot be proven the software tool should be designated as Appendix B quality software itself. An ISL observation, based on an analysis of tool qualification practices in other industries, is that tool qualification would not fit well into the NRC regulatory framework.

IEEE Std. 7-4.3.2-2003, endorsed by RG 1.152, Rev. 3, does not address justification for the selection of software tools and acceptance criteria for compilers, operating systems, and libraries; rather, it requires users to confirm the software tools are suitable for use. A major change implemented in the 2016 revision of IEEE 7-4.3.2 provides criteria on the use of software tools used for digital devices and development of hardware, software, firmware, and programmable logic. Endorsing IEEE Std. 7-4.3.2-2016 or just Clause 5.3.2 would address the use of software tools throughout the software lifecycle and the quality issues associated with them.

Similar to some NRC guidance, NASA and IEC 61226 specify the same requirements for the software tools as those for the safety systemsthat the tools were used on. FDA's guidance states that "[software] tools should have a degree of quality no less than the software product they are used to develop." The FAA requires that all software tools be identified, validated, and addressed within the software development activities and documentation. The aerospace industry assigns software tools in a classification separate from the embedded system software, whereas the civil aviation industry classifies software tools to the same level as the software developed with the tool. BS EN 50128 for the railroad industry contains several requirements for software tools used in the safety-related software development life cycle process that only depend on the tool functionality. Tools are assigned to one of three classes, and all tools must be assigned to one of these classes, depending on their potential to affect the executable code

The coverage of software tool requirements and guidance throughout the nuclear and nonnuclear industries varies considerably. Only a few industries impose requirements and provide guidance for software tools use in all phases of the software development process. Most industries do not impose requirements or provide specific guidance for the qualification of software tools. Most industries focus their efforts on the coding and testing processes and modeling, construction, and implementation tools. Only a few industries specify software tool requirements and provide guidance for other software development processes like the requirements specification phase, the conceptual design phase, and the detailed design phase. Somewhat related but outside the scope of this review, a few industries specify requirements or provide guidance for management support tools, maintenance tools, documentation tools, configuration management tools, and quality assurance tools other than requiring that such tools be identified, and their use documented.

C.5 References

C.1 J. Servatius, S. Alexander, and T. Gitnick, "Evaluation of Guidance for Tools Used to Develop Safety-Related Digital Instrumentation and Control Software for NPPs, Task 2 Report: Analysis of the State of Practice," ISL-ESRD-TR-14-03, August 2014 (ML15043A206).

C.2 U.S. NRC NUREG-0800 Appendix 7.1-D,Rev. 1,"Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," August 2016 (NRC ADAMS Accession No. ML16019A114).

C.3 G. G. Preckshot and J. A. Scott, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," NUREG/CR-6421, March 1996 (NRC Adams Accession No. ML063530384).

C.4 IEEE 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Piscataway, NJ, January 29, 2016.

C.5 Radio Technical Commission for Aeronautics (RTCA), "Software Tool Qualification Considerations," DO-330, December 2011.

C.6 Multinational Design Evaluation Program (MDEP) Digital Instrumentation and Control Working Group (DICWG) "Common Position on Software Tools for the Development of Software for Safety Systems," Generic Common Position DICWG No 2, Version C, March 13, 2013.

C.7 International Electrotechnical Commission, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer Based Systems Performing Category A Functions," IEC 60880:2006, Geneva, Switzerland, 2006.

C.8 International Electrotechnical Commission, "NPPs - Instrumentation and Control Important for Safety - Software Aspects for Computer-Based Systems Performing Category B or C Functions," IEC 62138, First Edition, Geneva, Switzerland, January 2004.

C.9 International Electrotechnical Commission, "Nuclear Power Plants—Instrumentation and Control Systems Important for Safety—Classification," IEC 61226, ed. 2.0, Geneva, Switzerland, February 2005.

C.10 International Electrotechnical Commission, “Functional safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Part 7: Overview of Techniques and Measures,” IEC 61508-7, Edition 2.0, Geneva, Switzerland, 2010-04.

C.11 CSA Group, “Qualification of Digital Hardware and Software for Use in Instrumentation and Control Applications for Nuclear Power Plants,” CSA N290.14-15.

C.12 U.S. Department of Transportation,Federal Aviation Administration,“Software Development for the National Airspace System (NAS),” FAA-STD-026A, June 2001.

C.13 U.S. Food and Drug Administration (FDA), “General Principles of Software Validation; Final Guidance for Industry and FDA Staff,” January 11, 2002. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation

C.14 U.S. Department of Defense, “DOD Guide for Achieving Reliability, Availability, and Maintainability,” August 3, 2005.

C.15 National Research Council 2007. Software for Dependable Systems: Sufficient Evidence?. Washington, DC: The National Academies Press. https://doi.org/10.17226/11923.

C.16 National Aeronautics and Space Administration, “NASA Software Engineering Requirements,” NPR 7150.2A, September 27, 2004.

C.17 National Aeronautics and Space Administration, “Software Assurance Standard,” NASA-STD-8739.8, 2004-07-28.

C.18 National Aeronautics and Space Administration, “Standard for Models and Simulations,” NASA-STD-7009A with Change 1, 2016-07-13.

C.19 National Aeronautics and Space Administration, “Software Safety Standard,” NASA-STD-8719.13C, 05-07-2013.

C.20 National Aeronautics and Space Administration, “NASA Software Safety Guidebook,” NASA-GB-8719.13, March 31, 2004.

C.21 National Aeronautics and Space Administration, “NASA Complex Electronics Handbook for Assurance Professionals,” NASA-HDBK-8739.23, 02-02-2016.

C.22 British Standards Instutition (BSI), “Railway applications—The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)—Part 1: Basic Requirements and Generic Process,” BS EN 50128:1999, 1999.

C.23 R. T. Wood et al., “Common-Cause Failure Mitigation Practices and Knowledge Gaps,” ORNL/LTR-2012/556 (NEET/ASI/ORNL/TR-2012/01), October 2012.

C.24 EPRI 1001503, “Identification and Description of Instrumentation, Control, Safety, and Information Systems and Components Implemented in Nuclear Power Plants,” Electric Power Research Institute, Palo Alto, CA, June 2001.

C.25 U.S. NRC, “Final Safety Evaluation by the Office of Nuclear Reactor Regulation for SPINLINE 3 Platform Licensing Topical Report Rolls Royce Civil Nuclear,” September 8, 2014 (NRC Adams Accession No. ML14143A27).

C.26 U.S. NRC, “Safety Evaluation for Topical Report 2016-RPC003-TR-001 RadICS Safety System Digital Platform,” August 2019 (NRC Adams Accession No. ML19134A193).

APPENDIX D EMERGING TECHNOLOGY (ET)

In this work, emerging technologies refers to devices related to EDDs, practices, design development and assessment methods and tools, and issues associated with evolving technology and new initiatives by the industry that could be included in license amendment applications or impact digital systems of nuclear plants, but which are not yet widespread in the nuclear industry.

Investigating emerging technologies was not conducted as an independent effort to consider all types of emerging technologies, but served to capture those that were identified during the evaluation of EDDs and that are related to EDDs. In addition, existing literature reviewing emerging technologies in the U.S. nuclear industry was reviewed for relationships with EDDs. In many cases these emerging technologies could also apply to digital instrumentation and control systems generally.

It is undeniable that advances in the capabilities of electronically enhanced components are occurring at a high rate. These advances include technical areas that extend to applications in the nuclear industry, from upgrades to existing plant systems to enhanced monitoring and control to supporting autonomous operation for advanced reactor designs. It seems that increased penetration of digital components into current and future nuclear power plants is inevitable as vendors are incorporating EDDs into more and more of their components.

The field of I&C technologies is broad and varied. It can be visualized in two slices as described in NUREG/CR-6812 (ORNL/TM-2003/22) [D.1]:

- The vertical slice, which is functionally focused, addresses the technologies that embody the sensing, communications, monitoring, control, and presentation and command systems between the process (i.e., the reactor, heat transport, and energy conversion systems) and the plant personnel (i.e., operations and maintenance staff).

- The horizontal slice at the lowest level is equipment focused and consists of the instrumentation string from the sensors and signal processing elements to the diagnostic modules and controllers (e.g., computational platforms) to the actuation devices. The variety of technologies that constitute the I&C systems of an NPP can be difficult to address as a whole. Therefore, the tack taken in this survey is to identify technology focus areas.

Based on the vertical or function-focused slice, the I&C technology breakdown is as follows:

- measurement systems,
- communications or networking,
- diagnostics and prognostics,
- control and decision,
- human-system interaction, and
- high-integrity software.

Based on the horizontal or equipment-focused slice, the I&C technology breakdown is as follows:

- sensors,
- communications media,
- microprocessors and other integrated circuits, and

- computational platforms (computers, programmable logic controllers, application-specific integrated circuits, etc.).

The chosen list of technology focus areas for section D.1 is derived from the technology breakdown offered by each of the vertical and horizontal slices.

- sensors and measurement systems,
- communications media and networking,
- microprocessors and other integrated circuits,
- computational platforms,
- self-diagnostics and prognostics,

- human-system interactions,
- high-integrity software, and

- I&C architectures in new plants.

Many of the emerging technology focus areas listed above may not have had any sort of digital controller when originally installed and may have had little or no logic, but now may contain a digital system that adds functionality. For example, a pump may now contain an array of sensors to support diagnostics or support cavitation detection through high frequency vibration sensors [D.2]. These sensors' digital subcomponents may be external and placed up to hundreds of feet away from the component to avoid a high radiation environment similar to the FIELDVUE DVC6200 controller [D.3].

Sections D.2, D.3, D.4, and D.5 come from areas of emerging technologies identified during the project, or that were otherwise known to the authors.

D.1 ET in I&C Applicable to EDDs

ORNL reviewed the advances of I&C in several technology areas in the following reports:

- NUREG/CR-6812 (ORNL/TM-2003/22) [D.1]
- NUREG/CR-6888 (ORNL/TM-2005/75) [D.4]
- NUREG/CR-6992 (ORNL/TM-2008/184) [D.5]
- ORNL/TM-2006/626 [D.6]

The eight focus areas reviewed in NUREG/CR-6992—the last update report on ET—are summarized below, with an assessment of the advances in technology and its potential impact on EDDs.

It is expected that the use of EDDs will significantly increase at NPPs. The ability to add an EDD to existing components will lead to an increased use of such devices. Microprocessors allow EDDs to be designed to allow them to be configured for more than one application. This in turn means that many vendors not previously supplying components or digital field devices to NPPs will most likely begin to supply components or digital field devices to NPPs. Because the use of EDDs at NPPs will likely increase, and more vendors of EDDs will not be from inside the nuclear industry, cyber security vulnerabilities and concerns will be greater. In addition, concerns with respect to software development and the use of software tools will also increase.

D.1.1 Sensors and Measurement Systems

The use of sensors with inherent drift-free characteristics can eliminate some of the need for calibration. Incorporating calibration capabilities in EDDs could potentially reduce the need for manual calibration. Methods such as cross calibration are not be available to EDDs because of their local use and isolation. It appears that, in general, the sensing technologies in the nuclear power industry represent adaptations of well-established measurement concepts, and new sensors are typically evolutionary rather than revolutionary in nature. Thus, new sensor technologies, primarily arising out of the needs for advanced reactors or 3-D printing sensors into components may be incorporated into EDDs at some point.

D.1.2 Communications Media and Networking

Advances in digital communication systems in general have focused on boosting data transmission speeds, developing more robust protocols, error correction and encryption techniques, and (for wireless systems) spread spectrum techniques. Advances in communication techniques would be very slow to be incorporated into EDDs, simply because of their function. EDDs do make extensive use of digital communication, but this use is to convey information on the component and not the system. The independence issue is not so easily resolved with regard to wireless communications systems in EDDs. The applications of wireless communication between EDDs are likely to be limited in the foreseeable future to non-safety–related diagnostics and maintenance systems, inventory management systems, and voice and data communications to employees and field crews.

D.1.3 Microprocessors and Other Integrated Circuits

The growing system complexity of semiconductor devices and the cost of ASICs could lead to higher use of processors. This could make it more difficult to guarantee delivering future EDDs free of errors. In addition, the successful development of high-k transistor integrated circuits and the potential for multi-gate transistor ICs could revolutionize the integrated circuit industry, but it could also introduce new aging phenomena, higher sensitivity to environmental conditions (e.g., temperature and radiation), and other issues related to qualification methodologies if incorporated into EDDs.

Failure modes and mechanisms for both current and emerging digital I&C technologies in EDDs need to be characterized to assess whether any new failure modes can cause unforeseen or unknown component and system responses.

D.1.4 Computational Platforms

The computational platforms for EDDs can cover an extraordinarily broad range of devices. At the simplest end, an EDD might consist of a few logic devices in a PLC or a few elements on an ASIC. The program being executed is almost as simple as getting an analog device to run when turned on. The regulatory question then becomes, when does an EDD become so simple that it no longer comes under the heading of *digital computer*? Regulatory guidance for such systems and devices (e.g., FPGAs, CPLDs) that are halfway between simple and complex is currently not as well defined. For example, DI&C-ISG-04 [D.7] requires a priority module design to be fully (i.e., 100%) tested if it combines the diverse actuation signals with the actuation signals generated by the digital system or if software tools used in its development are not to be validated. If the priority module is designed using a CPLD or a device of similar complexity, it may be very difficult, if not impossible, to prove that such a device has been fully tested.

Complex computing platforms (e.g., those using multicore processors) and OSs are more likely to be used in control and information display applications in I&C systems rather than in EDDs because of the much more rigorous demand for V&V in a safety system application. Microprocessors allow EDDs to be designed to allow them to be configured for more than one application. EDDs, if they use a processor, would have an OS that can to be used to run the application software. Operating systems provide the fundamental interface between software and hardware in most digital applications. Thus, their performance and reliability characteristics should be well understood.

D.1.5 Self-diagnostics, and Prognostics

Self-diagnostic techniques can be used in EDDs for monitoring the condition of rotating machinery condition, instrument response time measurements, predictive analysis of failures in sensors and sensor lines, and motor current signature analysis. The advantage of EDDs is that diagnostics can move from periodic human-based inspection (e.g., surveillance testing) to online monitoring for condition-based maintenance and eventually prognostics. These areas include sensors, better understanding of measurement in the plant environment (e.g., what and how to measure), enhanced data interrogation, communication and integration, new predictive models for damage/aging evolution, system integration for real-world deployments, and integration of enhanced condition-based maintenance/prognostics philosophies.

In some cases the EDD may not be integral to the device, but may be a separate device attached to the system of interest. For example, a pump may now contain an array of sensors to support diagnostics or support cavitation detection through high frequency vibration sensors [D.8]. These sensors may be external and designed for a nuclear power plant with its high radiation environment [D.8].

Self-diagnostics offers tremendous new opportunities for plants to operate more reliably, manually test less frequently, reduce risk of latent failures, reduce maintenance costs, and reduce worker exposure. The issues from a regulatory standpoint are mainly concerned when self-testing is applied to a safety system and the self-testing performs a required function under regulatory control. A number of fundamental questions emerge, as follows:

1. Are there any subjective monitoring criteria that an expert adds to surveillances that are lost in the self-diagnostic system?

2. Are the systems being monitored and their failure modes easy to recognize?

3. Are the failures in the self-diagnostics easy to recognize?

4. Can the operator accurately tell the difference between the failure of the self-diagnostics and the failure of the device it is monitoring?

5. Does the presence of the self-diagnostics affect the reliability of the safety function?

6. How can the self-diagnostic function be protected against a software fault that leads to a CCF to detect a failed protection system?

The modular nature of some EDDs can simplify resolving some of these questions. The EDD performing the diagnostics may not be tightly integrated with the portions of the EDD performing

the safety function. For a diagnostic device bolted onto the component, this separation may be very clear and physical. However even within a device there may be internal separation, for example some EDDs have different SIL certifications for internally separated functions such as the DVC6200 SIS Digital Valve Controller and Position Monitor where portions are assessed at SIL 3 and others at SIL 2.

D.1.6 Human-system Interactions (HSIs)

There are many evolving design and evaluation tools that can optimize the design of human interfaces and speed up their evaluation, and all are based on computer software technologies. Many of these tools are being developed outside of the nuclear power industry. It is widely accepted that poor human factors engineering contributes to poor human performance, increased errors, and reduced human reliability.

D.1.7 High-integrity Software

Software cannot typically be proven to be error-free and therefore could be considered susceptible to CCFs if identical copies of the software are present in redundant EDDs. The use of diversity to protect against CCFs in software design is not likely to change. However, a great deal of effort can go toward advanced software development techniques to reduce the likelihood of software faults in an EDD, to make the software less costly, and to make the software easier to review and license for use. The software development cycle in safety system use models such as the waterfall lifecycle model for nuclear software development, although modern lifecycle models are more iterative, and can benefit from tools better able to track requirements in such a process. Of the vendors contacted, software in EDDs can be developed by writing individual lines of code or using software tools to write the code. It is believed by many that the use of software tools helps automate design steps and report generation, organize the work in new ways that tend to make errors less likely, or automate testing and V&V. It is no longer just the computer program that runs on the EDD that affects quality, but the much larger system of software used to develop the software.

D.1.8 I&C Architectures in New Plants

A review of the I&C features of new I&C system designs indicated that these designs use fully digital and networked architectures. Some safety-related modules and subsystems in the plants reviewed include ASICs, FPGAs, or CPLDs. The same issues for ensuring reliable safety system designs—issues whose resolution can enhance the regulatory process for digital systems—are applicable to EDDs. These include (1) the need for a complete characterization of failure modes, (2) determining how much V&V should be required for EDDs that are halfway between simple (e.g., binary ON, OFF, and/or a small number of combinatorial logic) and complex, (3) determining how the self-testing function can be protected against a software fault that leads to a CCF, and (4) determining how much credit should be given to an online diagnostic system, which in itself could be more complex than a simple processing function.

D.2 ET in EDDs

ET in EDDs can be from advances in industry migrating into the nuclear arena or unique needs for new nuclear plant designs.

Embedded digital capabilities will enable new types of components that are not feasible without the high-speed data acquisition and processing capabilities supplied by the on-board electronics.

For nuclear applications, there are some emerging applications of autonomous control for creating reactor components that operate in extreme environments. For example, replacing mechanical bearings with magnetic bearings can allow a pump to be made from materials that can operate above 650 °C.

Current generation NPPs use a centralized control architecture that requires exceptional operator knowledge of the power plant, and the cost and difficulty of designing the operational and safety systems are significant because of the system complexity. Localized control through the use of EDDs will allow for simplifying the design and operation of complex systems while improving modularity similar to object-oriented control architectures.

Future advanced reactors may employ EDDs more extensively than the existing fleet due to the opportunity to integrate instrumentation into the SSCs during fabrication and/or construction. Embedding digital devices into components is also more likely at advanced reactors due to the advancement in the capabilities of digital technologies and consequent potential for improving component performance and reliability.

D.2.1 Future Uses of EDDs

The combination of on-device processing and digital communication for optimizing process performance for both technical performance and enterprise-level business goals will likely be more ubiquitous in the future. Embedded digital capabilities will also enable new types of components that are not feasible without the high-speed data acquisition and processing capabilities supplied by the on-board electronics. It is likely that components with EDDs will

- Become more aware of their health
- Be aware of the health of other devices in the process
- Be able to autonomously take actions to operate resiliently
- Be aware of their place in the overall process
- Understand how changes they make to process variables under their control will impact the overall process
- Store data and analyze past behavior
- Coordinate with other EDD components
- Understand how the process changes over time
- Abstract the operational functions that are exposed to the operator
- Autonomously develop system models
- Solve optimization problems

The search for EDDs in components was focused on those components that are supplied by vendors to the nuclear power industry. The review for EDDs also assumed a broader view to identify their use in industry. This review shows that EDDs are prevalent in industry. It is likely

that their use will migrate into the NPP industry, and their use will become more prevalent. For example, 663 UPSs were identified with EDDs; only 8 of these were from vendors that supply UPSs to NPPs.

The primary functions of EDDs used in components are to perform diagnostics and to communicate via modem host interfaces. The expansive use of EDDs in industry, in which EDDs perform fine control of a system, will likely migrate into the nuclear sectors.

EDDs are used to monitor and communicate the health of the components and to identify problems or failures. EDDs will migrate into the NPP arena first through the nonsafety systems and eventually to safety systems. By employing EDDs in components in non-safety and secondary side control, NPPs will be able to add fine control to their system, thereby reducing uncertainties. Reducing uncertainties and increasing reliability via surveillance, testing (diagnostics), and auto-calibration on the secondary side means that more heat can be generated on the primary side. This in turn has resulted in some licensees requesting power uprates.

Installing EDDs on existing components is becoming easier. Because of this, its use will increase, and EDD vendors from outside the nuclear industry will most likely begin to market EDDs to nuclear vendors and nuclear plants.

Remote-mount digital controllers like Emerson's Fisher FIELDVUE DVC6205 have only the valve position feedback mounted on the control valve, while the remainder of the digital valve controller can be mounted over 300 feet away in a less severe or more accessible environment. This option now allows digital control where accessibility, extreme temperatures, extreme vibration, or confined space is an issue and where integral mounting is difficult or impractical. Because of this, the use of EDDs and controllers on components in harsh environments or severe conditions will most likely begin to increase.

Future uses could also come about from new software and hardware technologies:

- Communication (fountain code, time-sensitive networking, blockchain)
- Emerging hardware (peel-and-stick sensors)

D.2.2 ET in functionality

Although of limited functionality, it is likely that new HMIs will have added features that will likely create new malfunctions. New physical interactions with the HMI will require an examination of how the actual physical interface could impact performance of SAR-described design functions. For example, if a malfunction with a different result is created as a result of the physical interaction, then the HMI portion of the digital modification would be deemed adverse and would be evaluated per 10 CFR 50.59. Examples of new physical interactions include:

- Use of touch screens in place of pushbuttons, switches, or knobs
- A new interface requiring the human user to choose which component is to be controlled
- Changes to operating procedures
- Information overload
- Changes in how a parameter is displayed
- Changes in the data acquisition process

Ideally, EDDs with limited functionality would operate like IIoT systems and would not require high IEC SILs. This would apply to EDDs in safety or nonsafety systems.

In principle, the added functionality of smart sensors could be the same as for conventional sensors. In reality, this is not the case [D.9]:

1. *The signal processing in smart sensors can involve more elaborate calculations than are possible in conventional sensors. These calculations might for example correct for nonlinearity.*

2. *Smart sensors may have more modes of operation and more parameters than their conventional versions.*

3. *Smart sensors may measure multiple process variables at the same time.*

4. *Smart sensors may provide more information than conventional sensors do. Flow sensors for example often contain temperature sensors for improving the accuracy of the measurement. Conventional sensors do not transmit this temperature, some smart sensors however do.*

5. *Smart sensors contain fault diagnostics; this inevitably leads to complicated algorithms in software and provisions in the hardware of the sensor.*

At the plant and system levels, data communications are important. However, at the EDD component level, data communications between different EDDs is currently not allowed for safety related functions and is therefore not considered. Similarly, wireless communication is currently not allowed for safety related functions. If these capabilities are added or if EDDs are bundled into a system, then the reviews on the functionality of the EDDs would be like those reviews for systems.

D.2.3 Hardened EDDs

Hardened may refer to cyber security hardening or radiation hardening. Each of these is discussed below.

D.2.3.1 Cyber Security

Many companies, such as Lockheed Martin, Raytheon, BEA Systems, and others, are working towards developing hardened networks and devices. Some of the challenges faced are in hardening of existing technology for cases in which the original platform did not require such measures. The PTR Group, Inc., is approaching hardened EDDs by assessing the security risks in the software (Linux). To make software more robust, any data stored or any software implemented must require encryption keys, passwords, etc., and all non-essential software must be removed.

Implementing e-fuses to protect internal registers or storage is one way to address the physical security of EDDs. Removing all external penetrations (USBs, serial ports, ethernet ports, etc.) and using tamper proof screws is also considered to physically harden EDDs.

The development, transport, and use of EDDs used in a safety-related application would follow NRC guidance for safety-related systems.

D.2.3.2 High Temperature and Radiation Environments

Current technology allows the same digital hardware that could be embedded within a device to instead be installed hundreds of feet away from the component. For example, in high radiation

areas, high temperature areas, etc., the digital hardware for valve controllers can be installed hundreds of feet away from the valve.

The development of wireless sensor nodes allows increased sensing, processing, and wireless communication capabilities of small, portable devices [D.10]. Self-powered wireless sensor nodes potentially offer significant expansion in remote monitoring at nuclear facilities and provide important data on plant equipment and component status during normal operation, as well as during abnormal operation or station blackouts and for post-accident evaluation.

Sporian Microsystems, Inc. is working on advancements in sensors and instrumentation to develop and improve the reliability of advanced sensors (and associated instrumentation) that can withstand harsh environments [D.11]. For example, for an internal control rod drive mechanism, it is not possible to verify full insertion externally. The technical challenges of developing a sensor that can reliably verify the control rod position and that can ultimately verify full control rod insertion include its sensitivity to particulates, small size, high reliability, and harsh environment operation, including very high temperatures (600°C), high pressures (2200 psig), borated Grade A water environment, and high irradiation. Ideally, such a sensor system would consist entirely of solid-state sensing (no moving parts) hardware and minimal electrical connections/vessel penetrations. Typical silicon-based electronic components and materials used in equivalent semiconductor devices are not suitable for use at the proposed temperatures. Important to this technology development, Sporian has identified novel materials, manufacturing, and signal conditioning methods, resulting in sensors and instrumentation with greater magnetic field sensitivity in high-temperature environments while minimizing system size and weight.

D.2.4 Wireless Technologies

There is growing level of interest in wireless systems. Use of wireless technology at nuclear plants could include adding wireless sensors to improve the amount of information available to operators. Wireless technology also affords the ability to remotely gather information about equipment or systems in hard-to-reach areas of the plant. In the near future, wireless technology will not be limited to through air transmission of the signal. A self-powered wireless through-wall data communication of an audio signal has been successfully designed and tested and work is progressing on transmitting a video image [D.12].

In existing NPPs, it is often impractical, or cost prohibitive, to add new sensors if they must be hardwired to a monitoring location. This discourages the installation of additional condition monitoring. Wireless sensors may help to resolve this issue. Use of wireless technology to extend plant communication networks has shown promise in the U.S. nuclear industry, resulting in improved dissemination of information and overall personnel efficiency. Worldwide, NPPs have taken advantage of wireless technologies. As experience and confidence is gained, wireless technology applications may be extended from ancillary functions to monitoring of plant conditions for operator information and control. IAEA recommends the active pursuit of the deployment of wireless technology in monitoring and diagnostics applications in NPPs in order to gain experience and develop knowledge that will allow future use of wireless in more demanding plant applications [D.13].

Expected near term wireless applications will include remotely monitoring devices on/near safety related/important to safety, collection of equipment performance data collection, dose rate monitoring, tracking and automated survey map updates. In Canada, the Pickering Nuclear Generating Station (PNGS) already uses wireless sensors as part of its online monitoring to enable condition based monitoring [D.14]. Milestones at PNGS include the first deployment of

wireless sensor networks to collect health data for various plant equipment, the use of Bluetooth 5.0 low energy and 900 MHz wireless sensors, in-house performance of EMI qualification testing, and collection of wireless sensor data at PNGS's historian database.

Concerns with the use of wireless technologies include the susceptibility and adequacy of protecting the devices from cyber-attacks, and the potential for interference between wireless equipment and equipment producing electro-magnetic waves or other wireless equipment. Previous research by NRC and ORNL staff indicates that cybersecurity and issues with electromagnetic propagation (electromagnetic and radio frequency interference, fading, interference abatement) as the major concerns with implementation of wireless technologies [D.15, D.16, D.17]. On February 20, 2020, NRC held a public meeting with industry representatives to have industry provide the NRC with details of their initiative on the use of wireless at NPPs and to discuss cyber security performance oversight [D.18].

PTR Group states that a window of vulnerability for any system using wireless technology is during the initial start-up sequence [D.19]. Also, firmware updates can present similar security problems and require a digital signature or physical token. When addressing wireless communication for EDDs, encryption technology will be critical for security of the system. Encrypted data messages that are sent/received are classified as data-in-flight. For wireless, this is the point at which most attacks happen through spoofing or interception. Knowing the devices connected to the wireless network and regularly taking inventory can help to quickly identify intruders. Use of smart cards or trusted platform modules is one option to increase security. Implementing cryptographic hash into a piece of firmware is another option.

Cameras using wireless technology can provide remote monitoring of equipment. Portable carts containing sensors and cameras can perform some of the work of fire watches, providing continuous monitoring of certain parts of the plant, serving as a replacement for hourly visits for a few minutes by personnel. Such carts are already in use in several U.S. NPPs.

Radiation protection technicians could use wireless technology to monitor radiation levels without visiting higher-dose areas of the plant in person. The Department of Energy has been funding research into advances in wireless technology such as thermoelectric generators for self-powered wireless sensor nodes. While the safety significance of the application of such technology isn't indicated, the research included evaluating the effects of gamma radiation on the materials, indicating uses in harsh environments [D.20].

D.2.5 Micro-Electrical Mechanical Systems (MEMS)

MEMS is a process technology used to create tiny integrated devices or systems that combine mechanical and electrical components [D.21]. These devices or systems have the ability to sense, control, and actuate on the micro scale, and generate effects on the macro scale.

MEMS usually consist of a central unit that processes data (the microprocessor) and several components that interact with the surroundings such as microsensors [D.22]. Because of the large surface area–to–volume ratio of MEMS, forces produced by ambient electromagnetism (e.g., electrostatic charges and magnetic moments), and fluid dynamics (e.g., surface tension and viscosity) are more important design considerations than with larger scale mechanical devices.

MEMS can be found in systems ranging across automotive, medical, electronic, communication and defense applications. Current MEMS devices include accelerometers for airbag sensors, inkjet printer heads, computer disk drive read/write heads, projection display chips, blood pressure

sensors, optical switches, microvalves, biosensors, and many other products that are all manufactured and shipped in high commercial volumes.

A specific research effort for the use of MEMS in NPPs was the DOE NEET project “Development of in-plane Single Crystal Silicon Microrelays for Nuclear Power Applications” which planned to use MEMS to make physical micro-relays on a chip, allowing them to use purely analog logic [D.23].

D.2.6 Autonomous Control

Autonomous control means that the data acquisition, control, actuation, and computation all occur in, on, or physically near the physical object being controlled. This is the classic example of an EDD. Similarly, EDDs may allow external commands from an operator either locally or remote. For example, a switched reluctance motor controller, satellite antenna attitude controller, or autonomous vehicle path planning controller are examples of localized control. While localized control could be as simple as a limit switch–controlled actuator, the greater concern is with the application of more complex advanced local feedback controllers.

For many decades autonomous control has been common in aerospace applications. The high-speed and high-performance of most aerospace applications required developing advanced techniques for designing, analyzing, synthesizing, and implementing controls [D.24, D.25]. Difficult measurement processing and integration applications such as inertial attitude and heading estimation also required high-speed data acquisition and processing platforms to execute the algorithms [D.26, D27].

Increasingly, many automotive applications are implementing more complex autonomous control. Automotive manufacturers are moving away from mechanically coupled systems because of their complexity, weight, and performance restrictions. For example, the Ferrari 2018 GTC4lusso has active all-wheel steering instead of the traditional mechanical solution using track and tie rods to connect the left and right steering arms. The purely mechanical solution fixes the steering geometry and relative steering angle of the left and right wheels. Active all-wheel steering, on the other hand, allows the steering angles of all four wheels to be controlled independently. The GTC4lusso then uses its vehicle dynamics EDD and various sensors to implement advanced autonomous controllers that provide advanced functionality like controlled side slip [D.28], increased grip and handling, optimized steering geometry for all driving conditions and increased overall stability [D.29]. The GTC4lusso also uses an adaptive suspension system and EDD local controller which can adjust suspension stiffness in real time, as well as an engine control unit EDD that currently makes it the most powerful naturally aspirated engine in a road vehicle [D.29]. Another emerging use of EDDs for autonomous, local control is seen in self-driving vehicles [D.30]. These vehicles require complex algorithms for control, sensor fusion, simultaneous localization and mapping [D.31], optimization with dynamically changing constraints [D.32], and safety [D.33].

For nuclear applications, there are some emerging applications of autonomous control for creating reactor components that operate in extreme environments. For exampleechanical bearings begin to fail at around 400 °C and for molten salt reactor applications that operate above 650 °C. This complicates the design, fabrication, and integration of rotating components that are in contact with the high-temperature salt. One possible solution is to replace mechanical bearings with magnetic bearings which can be made from materials that can operate above 650 °C [D.34, D.35] but require a high-speed high-performance local feedback controller to function [D.40].

Autonomous control has the advantages of

- Increased autonomy
- Simplified operator interactions
- Abstracting the operational functions
- Decoupling the control and operation
- New functionality
- Enables the decoupling of physical systems
- Optimized performance
- Reactive to real-time changes in local operating conditions

In contrast to autonomous control, NPPs are for the most part centrally controlled from a single control center, with some localized control employing simple open-loop (e.g., variable frequency drive) or proportional integral derivative controllers (e.g., control rod position controller). This centralized control architecture requires exceptional operator knowledge of the power plant, and the cost and difficulty of designing the operational and safety systems are significant because of the system complexity. Autonomus, localized control is one method for simplifying the design and operation of complex systems while improving modularity similar to object-oriented control architectures.

Previously, the cost to develop high-speed high-performance autonomous controllers was too great for many OEM components. Autonomous control required expensive specialized equipment for experimental design, testing, and validation of the controller and a laborious process of transferring that design into special hardware and software for the production implementation, followed by exhaustive safety and performance testing of the system. The advent of low-cost single board computers, simplified software modeling languages, automatic controller code generation, coupled multiphysics finite element and finite difference modeling, software control synthesis tools, open-source controller libraries, and open-source real-time operating systems have reduced the costs of developing, testing, and deploying complex autonomous controllers. The only aspect of autonomous control that remains costly is the testing of the system performance and safety because of the mostly manual experimental design and execution.

The typical design process for a high-performance high-speed controller consists of the some or all of the following activities

- System dynamics model development
- System identification testing
- Uncertainty quantification
- Controller architecture design
- Controller synthesis
- Mathematical stability analysis
- Data acquisition design
- Signal processing
- Sensor fusion
- Startup/shutdown procedures
- Safety system design
- Software testing
- Hardware testing
- Human machine interface design

Developing an accurate model is the first step in the design of a autonomous controller. Models are divided into two major categories—frequency domain and time domain. Standard linear frequency domain models typically use techniques such as transfer functions. Time domain models such as the state-space representation use techniques such as linear quadratic regulators.

Once an accurate low-order model is developed, it is used to synthesize a controller by various analytical techniques developed for different types of models. A brief (but by no means exhaustive) description of the most commonly used controller synthesis techniques is provided below:

- Loop-shaping
- Pole placement
- Optimal control
- Robust control
- Adaptive control
- Model predictive control
- Sliding-mode control
- Neural network control
- Lyapunov control

This list is by no means complete: a major area of research is the development of new controller synthesis tools. However, this list includes the commonly used techniques in application.

D.2.7 Combined control

Sensor information will be more commonly processed locally in future NPPs where possible because of to the expense and difficulty of long-distance cabling. Sensor signals tend to be small and may include high frequency content because of the characteristics of the process or component being monitored. Cable signal transmission line properties distort the higher frequency signal components. Nuclear plant environments are electromagnetically noisy because of the presence of electrical and electronic components necessitating careful cable grounding, shielding, and routing. Organic cable electrical insulation is combustible and has a lifetime shorter than that of a nuclear plant. Routing cables across plant boundaries can therefore create a fire vulnerability and increases the complexity of plant construction.

There are thousands of miles of cables in each reactor [D.38]. Cable pulling now costs $3,000–$6,000 / meter for safety-related cable; such costs dominate instrumentation, controls, and human-machine interface capital costs [D.39]. Consequently, future reactor SSCs will tend to process sensor signals locally and will pass actionable information to the plant control and/or safety systems when necessary. Transmitted information will be digital, and it may be wireless, to an access point for the plant's high-speed communication network. Other methods include piggybacking information and control onto single cables or using various schemes to put a multitude of devices on a single cable.

Localized information from EDDs could be collected at a control bank of EDDs and have its own I&C control system.

D.2.8 Additive Manufacturing

Additive manufacturing processes allow for direct embedding of sensors in critical locations within nuclear components during the manufacturing process. Proper selection of the sensor to be embedded and placement of the sensor within a component could greatly enhance plant monitoring capabilities, identify early signs of component failure, and reduce the staffing required to operate nuclear plants. The ultimate goal of additive manufacturing processes is to allow for direct embedding of sensors in critical locations within nuclear components during the manufacturing process which, at least as is being considered for ORNL's Transformational Challenge Reactor, would enable fully autonomous control [D.39].

One application of embedded sensors in nuclear plants relates to placement of sensors in locations that are otherwise inaccessible using traditional manufacturing techniques.

D.3 Digital Twins

DOE is performing research on digital twins, which can be applied at both the system and component level.

A *digital twin* refers to a digital replica of the system or component. Two aspects of a digital twin are important: (1) it recognizes the connection between the physical model and the corresponding virtual model or virtual counterpart, and (2) this connection is established by generating real-time data using sensors.

Digital twins integrate IoT, artificial intelligence, machine learning, and software analytics to create living digital simulation models that update and change as their physical counterparts change. A digital twin continuously learns and updates itself from multiple sources to represent its near real-time status, working condition, or position.

In the DOE world, one research project is using a digital twin to recognize cyber-attacks on the control system. Another DOE project is performing research to optimize the operation and maintenance of components.

Another DOE project will develop digital twin technology for advanced nuclear reactors, using artificial intelligence and advanced modeling controls to create tools that introduce greater flexibility in nuclear reactor systems, increased autonomy in operations, and faster design iteration. The development of these digital twins will work towards a 10x reduction of operating and management (O&M) costs at advanced reactor power plants [D.40].

EDDs, in addition to being in the components a digital twin may be analyzing to optimize its operation and maintenance, could support collecting the additional real-time data used by a digital twin.

D.4 Methods and Tools

During the exploration for existing solutions to implement EDDs, several promising methods and tools were discovered. Properly reviewing all of these tools was determined to be beyond the time and budget allocated to this research effort; however, these should be noted as ETs that are already in use outside of the U.S. nuclear industry. Furthermore, while methods and tools are used for EDDs, they could be applied more broadly to RPSs and ESFASs, for example.

A research related report from Idaho National Laboratory is entitled “Preliminary Results of a Bounded Exhaustive Testing Study for Software in Embedded Digital Devices in Nuclear Power Applications [D.41].” In the text describing the applicability of the document, the authors characterize an EDD as a reactive system, meaning it “is characterized by its ongoing interaction with its environment, continuously accepting requests from the environment and continuously producing results.” Their examples of such systems include process control systems and reactor protection systems; therefore, their scope is broader than this report. The report describes the use of combinatorial testing methods and boundary value analysis, along with studies supporting decisions as to how many values and combinations for the variables are sufficient. As with many methods, they then use a set of tools to realize the analysis and testing.

There are many specific software tools in use that fit the categories described in IEEE 7-4.3.2 (2016) and NQA-1. Their treatment is covered in Appendix C of this report. One thing that future evaluations may consider is that for particular tools and methods, claims may be made, such as in INL/EXT-19-55606 titled “Preliminary Results of a Bounded Exhaustive Testing Study for Software in Embedded Digital Devices in Nuclear Power Applications,” [D.41] which claims congruence with 100% testing for its proposed methods and tools. In many cases these advancements have been evolutionary in nature.

However, certain tools and methods represent a more substantial change, in particular model-based engineering. Model-based engineering can differ substantially from existing processes in that certain documents that are currently expected in regulatory guidance, such as a system requirement specification, are not produced, instead the digital engineering environment and the model itself could be used throughout the development lifecycle to capture, implement, and test the requirements. Model-based engineering also opens up the possibility of more substantial analysis and testing being performed during earlier lifecycle phases, which could be used to support NRC staff reviews, particularly when those reviews are focused on earlier lifecycle phases such as the alternate review process in ISG-06.

Such tools have different degrees of implementation across the lifecycle, but well-known examples include SysML, AADL, AnSys SCADE, and Mathworks Simulink (and associated toolboxes) [D.42, D.43, D.44, D.45, D.46].

There has been some work in this area specifically focused on use in NPPs.

EDF, in the framework of a collaborative project CONNEXION, has investigated model-based engineering methods based on simulations to formalize and evaluate DI&C requests in early design phases [D.47].

KAERI and Konkuk University have developed a model-based software development environment for safety-critical digital systems in NPPs to support formal verification and safety analysis called NuDE 2.0 [D.48].

Pakonen et al. [D.49] state that model checking has been used as a practical verification method in every major activity related to digital I&C in Finnish NPPs and that the experience at the VTT Technical Research Centre of Finland Ltd has shown that model checking can reveal design issues in DI&C application logic that are otherwise difficult to detect. However, they note that model checking did not seem commonplace in the nuclear domain outside of Finland as of 2017.

In addition to and somewhat associated with model-based engineering are improvements in the development of requirements. A more mathematically verifiable approach to requirements for

computer controlled shutdown systems at the Nuclear Power Generating Station at Darlington, Canada, is described in Wassyng et al. [D.50].

Recent development in hazard analysis methods, such as Systems Theoretic Process Analysis have been evaluated by EPRI [D.51] and are being adopted by EPRI as part of their methodology for risk informing digital system in NPPs [D.52] and as an advanced method of hazard analysis in support of performing digital engineering modifications in [D.53]. In a study by the method's creators, systems theoretic process analysis was applied to a safety system in a U.S. NPP [D.54]. Such methods for identifying hazards could serve to ensure the correctness of requirements and critical characteristics for EDDs.

Various methods and tools are often used in concert to support a claim. For example, the SymPLe Architecture and Methodology described in Gibson et al. [D.44], as part of the DOE Nuclear Energy Enabling Technologies project, "Realizing Verifiable I&C and Embedded Digital Devices for Nuclear Power," uses the MathWorks Simulink toolchain and Mentor Questasim tools to support model-based design and formal verification, with an original purpose of resolving CCF concerns for EDDs.

D.5 ET in Advanced Reactors

The designs of advanced reactors will probably push the boundaries on technology, including increased use of sensors, autonomous control through EDDs, and advanced technology. Some new uses of EDDs not necessarily applicable to current plants include:

- EDDs in passive SSCs
- EDDs in new types of I&C devices
- Seismic isolators with expand reliance on EDDs
- Different fuel forms
- High temperatures

Future advanced reactors may employ EDDs more extensively than the existing fleet because of the opportunity to integrate instrumentation into the SSCs during fabrication and/or construction. For example, efforts to extend the life of existing LWRs have shown the value of monitoring the condition of the rebar within reinforced concrete and the difficulty of non-destructively externally measuring internal degradation. Consequently, future plants are likely to embed corrosion monitoring instrumentation into reinforced concrete during construction. Digital signal processing electronics would be anticipated to be deployed locally along with the sensors due to the comparative ease of digital networking.

The safety case of advanced reactors is anticipated to depend on the performance of passive SSCs, and EDDs can provide evidence of their continued functionality. Current plants rely instead on labor-intensive periodic inspections to demonstrate the functionality of safety-related SSCs. For example, existing plants perform periodic containment pressure integrity tests as part of maintenance outages. The economic imperative to minimize staffing costs at future plants makes them much more likely to employ EDDs instead for continuous health monitoring. Directly measuring changes in component characteristics and performance can obviate schedule-based maintenance. For example, future passive decay heat rejection systems may include automatic health monitoring components that electrically impress heat pulses onto the heat transfer loop and subsequently monitor changes in loop flow and temperatures as evidence of system functionality. While the logical elements of the health monitoring could be performed with non-embedded digital systems, having remote hardware would require employing additional safety-grade signal cabling

to the system. Embedded health monitoring, in contrast, would only require providing system degradation notification to the plant control system.

Embedding digital devices into components is also more likely at advanced reactors due to the advancement in the capabilities of digital technologies and the consequent potential for improving component performance and reliability. The primary components at existing NPPs were designed and approved decades ago before the advent of high-speed digital systems. Modern control electronics now have sufficient speed and reliability to provide dynamic control of high-speed mechanical components such as pump and turbine shafts. Health and performance monitoring generally rely on small signals with high frequency content providing strong incentive to embed the signal processing rather than employing extensive cabling. Other industries have observed dramatic component reliability and performance improvements with the introduction of EDDs. Modern jet engines have had dramatic reliability gains [D.55]. Locomotive traction drives gain up to 50% improvement in wheel thrust by monitoring the onset of slippage and controlling the drive force such that the wheel traction remains within the static friction regime. EDDs have already begun to be deployed internationally at advanced reactors. The HTR-10 helium circulator employs high-temperature magnetic bearings controlled using a multi-axis high-speed feedback scheme [D.56], avoiding the potential for water ingress across the seals experienced at Fort Saint Vrain helium gas circulator [D.57].

In-situ non-destructive evaluation and material property testing have widespread value for providing evidence of remaining material or component useful life. Properties as diverse as the elastic response of seismic isolators and changes in reactor vessel fracture toughness can be monitored using non-linear acoustics. Non-linear acoustic technologies are not yet commonly deployed in harsh environments. As health monitoring technologies mature, they would be anticipated to be deployed in embedded form (due to their dependence on integrated signal processing) in future reactors.

Most legacy mechanical systems and electronic components such as sensors, actuators, and control systems will not survive in a high-radiation, high-temperature corrosive environment expected in new reactor designs. A magnetic bearing suspension system for the rotor shaft in place of the mechanical bearings would decrease pump maintenance while increasing reliability and efficiency (Figure D-1). Embedded I&C techniques provide the functional and operational improvements [D.58].

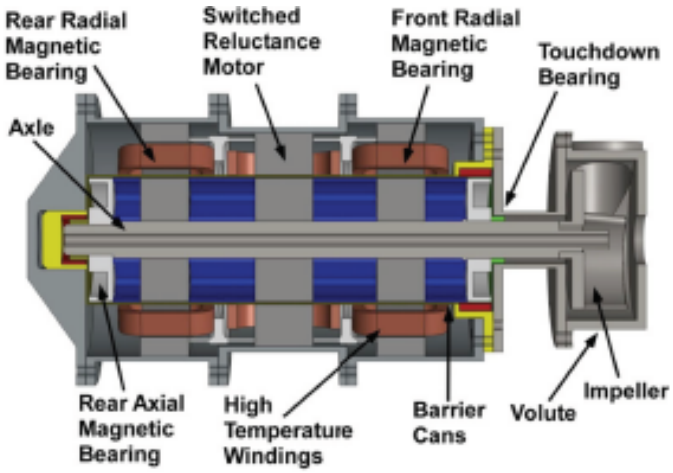


Figure D-1 Concept Drawing of a Canned-Rotor, Magnetically Suspended, Reluctance Drive Motor-pump [D.58]

D.6 References

D.1 R. T. Wood, et. al., “Emerging Technologies in Instrumentation and Controls,” NUREG/CR-6812 (ORNL/TM-2003/22), March 2003 (ADAMS Accession No. ML031900433).

D.2 T. Bass, “Remote Monitoring of Pumps with wireless HART Transmitters,” July 2017. https://www.automation.com/en-US/Articles/2017/remote-monitoring-of-pumps-with-wirelesshart-trans

D.3 Emerson Process Management (2014), “FIELDVUEW DVC6200 Series Digital Valve Controller,” https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=16&ved=2ahUKEwihgvSohpTgAhVEOK0KHdSSDn4QFjAPegQIAxAC&url=http%3A%2F%2Fomeas.com%2Fwp-content%2Fuploads%2F2018%2F08%2FProduct-catalog-Fisher-DVC6200.pdf&usg=AOvVaw3YHl4TXp34SfJKLCwK_VdV

D.4 K. Korsah, R. Wetherington, and R. Wood, “Emerging Technologies in Instrumentation and Controls: An Update,” NUREG/CR-6888, January 2006 (ADAMS Accession No. ML060870216).

D.5 K. Korsah, et. al., “Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update,” NUREG/CR-6992, October 2009 (ADAMS Accession No. ML092950511).

D.6 K. Korsah, M. D. Muhlheim, and D. E. Holcomb, “Industry Survey of Digital I&C Failures,” ORNL/TM-2006/626, May 2007.

D.7 U.S. NRC Interim Staff Guidance DI&C-ISG-04, “Highly-Integrated Control Rooms—Communications Issues (HICRc),” September 28, 2007 (ADAMS Accession No. ML072540138).

D.8 Wilcoxon Pump monitoring guide. https://wilcoxon.com/wp-content/uploads/2019/01/Pump-monitoring-guide.pdf

D.9 M. van der Meulen, “On the Use of Smart Sensors, Common Cause Failure and the Need for Diversity,” Centre for Software Reliability, City University, London.

D.10 Yanliang Zhang and Vivek Agarwal, “Thermoelectric Generator for Efficient Power Harvesting for Self-powered Sensor Nodes,” Advanced Sensors and Instrumentation, Issue 5, September 2016.

D.11 K. Harsh and L. Frediani, Sporian Microsystems, Inc., “A High Temperature High Reliability Control Rod Position Sensor for Improved Nuclear Power System Instrumentation,” Advanced Sensors and Instrumentation, Issue 5, September 2016.

D.12 L. Zuo, “Self-powered Wireless Through-wall Data Communication for Nuclear Environments,” U.S. DOE, Advanced Sensors and Instrumentation Annual Webinar, October 31 – November 1, 2018.

D.13 International Atomic Energy Agency, “Technical Challenges In The Application And Licensing Of Digital Instrumentation And Control Systems In Nuclear Power Plants,” IAEA Nuclear Energy Series No. NP-T-1.13, Vienna, 2015.

D.14 EPRI 3002017641, “EPRI Research Helps Ontario Power Generation (OPG) Deploy Its First Wireless Sensor Network at One Plant,” Electric Power Research Institute, Palo Alto, CA, Dec 23, 2019.

D.15 J. Dion, M. K. Howlander, and P. D. Ewing, “Wireless Network Security in Nuclear Facilities,” NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010. (Adams Accession No. ML103210371)

D.16 B.J. Kaldenbach, et. al., “Assessment of Wireless Technologies and Their Application at Nuclear Facilities,” NUREG/CR-6882, Oak Ridge National Laboratory, July 2006.

D.17 M. Howlader, C.J. Kiger and P.D. Ewing, “Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Environment,” NUREG/CR-6939, Oak Ridge National Laboratory, July 2007.

D.18 U.S. NRC, “NRC Notice of Meeting with the Nuclear Energy Institute February 20, 2020.” (NRC ADAMS Accession No. ML20063L416)

D.19 M. Anderson, “Securing Embedded LINUX,” [PowerPoint Presentation] Embedded Linux Conference, San Diego, CA April 4-6 2016 https://elinux.org/images/5/54/Manderson4.pdf

D.20 Yanliang Zhang and Darryl P. Butt, Vivek Agarwal, Zhifeng Ren, Nanostructured Bulk Thermoelectric Generator for Efficient Power Harvesting for Self-powered Sensor Networks, Advanced Sensors and Instrumentation Award Summaries, Nuclear Energy Enabling Technologies – Advanced Sensors and Instrumentation, May 2016.

D.21 “An Introduction to MEMS (Micro-electromechanical Systems),” PRIME Faraday Partnership, Wolfson School of Mechanical and Manufacturing Engineering Loughborough University, Loughborough, Leics, 2002. https://anastasiadiskonstantinos.appspot.com/pdf/mems.pdf

D.22 Addison Engineering, Inc. “About MEMS.” https://www.addisonengineering.com/about-mems.html

D.23 C. Elks, T. Bakker, and M. Gibson, “Verifiable Digital I&C and Embedded Digital Devices for Nuclear Power,” Advanced Sensors and Instrumentation, United States Department of Energy, Issue 6, March 2017, pp. 1-4. https://www.energy.gov/sites/prod/files/2017/03/f34/NEET-%20Advanced%20Sensors%20and%20Instrumentation%20Newsletter%20-%20Issue%206%20March%202017_4.pdf

D.24 Vernon R. Schmitt, Gavin D. Jenney, and James W. Morris, “Fly-by-Wire,” SAE International, 1998.

D.25 Kenzo Nonnami, Farid Kendoul, and Satoshi Suzuki, “Autonomous Flying Robots,” Springer, 2010.

D.26 Rudolph E. Kalman, “A New Approach to Linear Filtering and Prediction Problems,” *Trans. of the ASME - Journal of Basic Engineering*, Vol. 82, Series D, pp. 35–45, 1960.

D.27 Paul D. Groves, “GNSS, Inertial, and Multisensor Integrated Navigation Systems,” Artech House, 2013.

D.28 Osvaldo Barbarisi, Giovanni Palmieri, Stefanos Scala, Luigi Glielmo , “LTV-MPC for Yaw Rate Control and side Slip Control with Dynamically Constrained Differential Braking,” European Control Conference, 2009.

D.29 Chris Chin, “5 Crazy Technologies That Make the 2018 GTC4lusso the Ultimate Year-Round Ferrari,” 2018. [Online]. Available: https://www.digitaltrends.com/cars/five-crazy-technologies-in-the-2018-ferrari-gtc4lusso/. [Accessed: 2-Jan-2019].

D.30 Alex Davies, “Inside the Races that Jump-Started the Self-Driving Car,” 2017. [Online]. Available: https://www.wired.com/story/darpa-grand-urban-challenge-self-driving-car/. [Accessed: 2-Jan-2019].

D.31 Juan-Antonio Fernandez-Madrigal and Jose B. Claraco, “Simultaneous Localization and Mapping for Mobile Robots: Introduction and Methods,” IGI Global, 2012.

D.32 Dale Shu and Constantino M. Lagoa, “A Linear Temporal Logic Based Approach for Vehicle Motion Planning,” IEEE Int. Conf. on Mechatronics, Churchill, VIC, Australia, 2017.

D.33 Andrzej Wardzinski, “Dynamic Risk Assessment in Autonomous Vehicles Motion Planning,” Int. Conf. on Information Technology, Gdansk, Poland, 2008.

D.34 Roger A. Kisner, et al., “Embedded Sensors and Controls to Improve Component Performance and Reliability: Conceptual Design Report,” ORNL Report, ORNL/TM-2012/433, 2012.

D.35 Roger A. Kisner et al., “Evaluation of Manufacturability of Embedded Sensors and Controls with Canned Rotor Pump System,” ORNL Report, ORNL-TM-2013/269, July 2013.

D.36 Alexander M. Melin, Roger A. Kisner, and David L. Fugate, “Embedded Sensors and Controls to Improve Component Performance and Reliability: System Dynamics Modeling and Control System Design,” *ORNL Report*, ORNL/TM-2013/415, September 2013.

D.37 L. S. Fifield, “State of Electrical Cable Aging in U.S. Nuclear Power Plants,” Transactions of the American Nuclear Society, Vol. 118, Philadelphia, Pennsylvania, June 17–21, 2018.

D.38 D. D. Dudenhoeffer et. al., “Technology Roadmap on Instrumentation, Control, and Human-Machine Interface to Support DOE Advanced Nuclear Energy Programs,” INL/EXT-06-11862, March 2007.

D.39 C. M. Petrie, “Embedding Sensors in Metal and Ceramic Structures,” ANS Annual Meeting, Phoenix, Arizona, June 7-11, 2020.

D.40 Department Of Energy Announces $35 Million To Develop Tools To Transform Operations And Maintenance Of Advanced Nuclear Reactors. https://arpa-e.energy.gov/news-and-media/press-releases/department-energy-announces-35-million-develop-tools-transform

D.41 Elks C., Jayakumar A., Collins A., Hite R., Karles T., Deloglos C., Simmons B., Tantawy A., Gautham S. (2019). Preliminary Results of a Bounded Exhaustive Testing Study for Software in Embedded Digital Devices in Nuclear Power Applications (Report INL/EXT-19-55606), U.S. Department of Energy, Office of Nuclear Energy.

D.42 McDermott T.A., Hutchison N., Clifford M., Van Aken E., Salado A. Henderson K., “Benchmarking the Benefits and Current Maturity of Model-Based Systems Engineering across the Enterprise” (Technical Report SERC-2020-SR-001). Stevens Institute of Technology, March 19, 2020.

D.43 Simensen J., Sarshar S., (2016) Digital Instrumentation and Control Asurance – Systematic Literature Review (Report HWR-1184) OECD Halden Reactor Project.

D.44 Gibson M., Elks C., Tantawy A., Hite R., Gautham S., Jayakumar A., Delogos C., (2019) Design, Verification and Demonstration of the SymPLe Architecture and Methodology (Milestone - M2CA-15-CA-EPRI-0703-0221 2019) U.S. Department of Energy, Advanced Sensors and Instrumentation Program.

D.45 Architecture Analysis & Design Language (AADL), SAE International Standards document AS5506A, Nov 2004, Revised Jan 2009. http://www.sae.org/technical/standards/AS5506A.

D.46 Feiler, Peter H. and Gluch, David P. Model-Based Engineering with AADL: An Introduction to the SAE Architecture Analysis & Design Language, Addison-Wesley (2012).

D.47 Neyret, Maxime, “Model-Based Verification of I&C Specifications,” in ANS NPIC&HMIT 2017, San Francisco, CA, USA., 2017.

D.48 J. Yoo, E.-S. Kim, D.-A. Lee, J.-G. Choi, Y. J. Lee, and J.-S. Lee, “NuDE 2.0: A Model-Based Software Development environment for the PLC & FPGA Based Digital Systems in Nuclear Power Plants,” in Integrated Circuits (ISIC), 2014 14th International Symposium on, 2014, pp. 604–607.

D.49 Pakonen, A., Tahvonen, T., Hartikainen, M., Pihlanko, M., “Practical Applications of Model Checking in the Finnish Nuclear Industry,” in 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2017Volume 2, 2017, Pages 1342-1352.

D.50 Wassyng A., Lawford M., Maibaum T., “Software Certification Experience in the Canadian Nuclear Industry: Lessons for the Future,” Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011.

D.51 EPRI 23002000509, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” Electric Power Research Institute, Palo Alto, CA: 2013.

D.52 EPRI 3002012755, “HAZCADS: Hazards and Consequences Analysis for Digital Systems,” Electric Power Research Institute, Palo Alto, CA: 2018.

D.53 EPRI 3002011816, “Digital Engineering Guide: Decision Making Using Systems Engineering,” Electric Power Research Institute, Palo Alto, CA: 2018.

D.54 Thomas J., Lemos F., Leveson N., (2012) Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants (Research Report: NRC-HQ-11-6-04-0060)

D.55 James E. Tomayko, *Computers Take Flight: A History of Nasa’s Pioneering Digital Fly-By-Wire Project,* NASA SP-2000-4224, Washington, DC, 2000.

D.56 Yang Guojun, Xu Yang, Shi Zhengang, and Gu Huidong, *Characteristic analysis of rotor dynamics and experiments of active magnetic bearing for HTR-10GT*, Nuclear Engineering and Design, 237, 2007, 1363–1371.

D.57 D.A. Copinger, D.L. Moses, *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, NUREG/CR-6839, ORNL/TM-2003/223, January 2004.

D.58 A. Melin, R. Kisner, and R. Vidrio, “Embedded Instrumentation & Control for Extreme Environments,” Advanced Sensors and Instrumentation, Issue 5, September 2016.

APPENDIX E DATA COMMUNICATION PROTOCOLS

The information in this appendix does not represent an evaluation of data communication protocols but is a collection of information found during other evaluations provided as an information resource for the reader.

In many cases communication issues may be dealt with at the system level, using existing guidance as required for the system level interactions depending on the nature of the connectivity. NUREG/CR-6082 (ADAMS Accession Number ML063530379) is cited as a source of additional guidance on protocols in revision 6 of section 7.9 “Data Communication systems” in chapter seven of the Standard Review Plan. However, as that was published in 1993, there may be value in updated guidance including the protocols referenced below.

Transmitters with EDDs typically use one or more of several protocols to communicate digitally: Highway Addressable Remote Transducer (HART) Communication protocol, FOUNDATION fieldbus protocol, PROFIBUS PA protocol, or WirelessHART protocol [E.1]. An EDD can be compatible with several communication protocols. For example, the Fisher FIELDVUE DVC6200 Series digital valve controller is available with either the HART 5 or 7, WirelessHART FOUNDATION fieldbus, or PROFIBUS communication protocol.

Manufacturing industries have been implementing IoT concepts for more than 20 years. (IoT is discussed in the other names used for smart devices.) In fact, the HART communication protocol was developed in the early 1990s to provide digital data from smart sensors previously providing one data point [E.2]. The estimated installed base of HART devices is more than 40 million. Other open standards such as EtherNet/IP and Foundation Fieldbus that were developed in the late 1990s enabled placing sensors directly on networks.

IEC 61784 [E.3, E.4, E.5] lists specifications for seven fieldbus technologies (protocols):

1. FOUNDATION Fieldbus (FFB),
2. ControlNet,
3. Process Field Bus (PROFIBUS),
4. P-NET,
5. WorldFIP,
6. INTERBUS, and
7. SwiftNet.

Other communications protocols that support intelligent sensors (and EDDs) include:

- Highway Addressable Remote Transducer (HART)
- Device Net

The HART version of the Rosemont 3144P has an independent circuit that triggers an alarm if the microprocessor fails, whether the failure takes place in hardware or software. A typical EDD transmitter will condition its output signal with its microprocessor, so a failure in the microprocessor cuts off the output signal [E.1].

ET will most likely result in devices or parts of a device communicating to a central processor. Such an arrangement would require a communication protocol to ensure independence. A communications isolator may be sufficient to ensure independence. An advantage of these EDDs is the modular fashion in which they can be connected to central processing units. The advances

in digital communication capabilities have also radically changed the way that the design and specification of such systems must be approached and have created major issues relative to system design and security.

With the connection to a central processor, the information from the devices could be used in different ways such as to balance heat loads, reduce stressors in one loop to extend lifetimes, etc.

API RP 554 is a recommended practice (RP) from the American Petroleum Institute (API) "published to facilitate the broad availability of proven, sound engineering and operating practices."

API RP 554 has been divided into three parts, each focusing on a major aspect of process control systems. The three parts and the areas that they cover are:

- Part 1, "Process Control System Functions and Functional Specifications" [E.6], covers the basic functions that a process control system may need to perform, and describes recommended methodologies for determining the functional and integration requirements for a particular application.

- Part 2, "Process Control System Design" [E.7], covers the hardware and software applied to process control systems and provides recommendations for implementation. Design considerations and references to design practices for control centers and other control system buildings and enclosures are also provided.

- Part 3, "Process Control System Project Execution and Ownership" [E.8], covers project organization, skills and work processes required to execute a process control project and then to own and operate process control systems.

It states that these issues are related to the increased use of EDDs [E.6]:

- *The virtual disappearance of conventional central control room control panels.*

- *Advances in computing power, software standards and communications standards have resulted in many of the functions historically implemented in stand alone process control and historization computers being integrated within the Process Control Systems. This has greatly expanded the scope of Process Control System design and blurred the division between real time control and historization functions and higher-level information systems that provide input to business and maintenance systems.*

- *Advances in field instrumentation design leading to the general use of smart digital field instrumentation. Further advances in fieldbus and related technologies allow these smart instruments to communicate directly with the Process Control Systems or with each other. These instruments not only transfer information about the basic process measurement, but also communicate diagnostic information about the health of the device or other secondary information derived from the primary measurements.*

- *Further developments in standardization of operating systems and software practices have enabled use of standard computer components and peripherals operating on standard operating systems. This has resulted in a developing trend away from control systems applications being implemented on proprietary hardware and software systems, but rather being implemented on standard personal computer, workstation and network communication products running widely available operating systems.*

- *This standardization has reduced the cost and increased the flexibility of the systems. It has also resulted in greater exposure of the Process Control System to external interference and requires additional support to keep the operating systems current and secure.*

- *Security and virus-protection are major concerns of newer Process Control Systems and must be addressed at both the design and operational phases.*

The communication paths to external systems, should have Cyclic Redundancy Checks, handshaking, and other protocol-based features, depending on which devices are attached to the communication modules and how the communication modules are programmed. In such cases, the EDD and any devices it is connected to would need to ensure that failures such as a melting fiber optic cable or otherwise compromised communication pathway will not cause erroneous operation or affect the continued operation of all automatic safety-related or nonsafety systems.

The data communication in an EDD should be similar to that for a system. For example, in its Safety Guide, the IAEA provides the following guidance for a system [E.9]:

- *Each message sent and received via digital data communication should be automatically checked and flagged if errors are identified.*

- *Errors might include corrupted data, invalid data (unplanned messages) or inauthentic messages (messages from unexpected sources).*

- *If communications systems encrypt data or use proprietary protocols, these features should not prevent detection of errors.*

- *The actions to be taken when errors are detected in data communications should be defined in advance.*

- *Actions that might be taken when errors are detected include the automatic rejection of invalid or inauthentic data, the correction of corrupted data, where possible, or the rejection of corrupted data.*

- *The design should ensure that failures of data transmission and of the data communication equipment are detected, that suitable alarms are provided to the operators and that records are made for analysis of performance.*

- *The existence of certain types of error in digital data communication does not by itself constitute a failure in the system as such errors are expected and communication protocols are designed to deal with certain types of error and a range of occurrence rates of errors. Consequently, the application will involve specification of what constitutes a failure of data transmission. The criteria might, for example, specify a maximum allowable time interval between successful transmissions or a maximum error rate.*

- *Features for the detection and correction of errors improve the reliability of signal transmission.*

- *The extent of methods used for dealing with errors and detection of communications failures should be appropriate for the use of the data, appropriate for the frequency of demand for the functions that use the data and balanced against the complexity that is introduced.*

- *If the communication of safety related data malfunctions in any way, the safety system should continue to perform its safety function or go to a safe state.*

E.1 References

E.1 T. Jacobi et al., 'Investigation of Instrumentation Containing an Embedded Digital Device," NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017.

E.2 "10 steps to IIoT success." https://www.plantservices.com/articles/2017/automation-zone-10-steps-to-iiot-success/

E.3 International Electrotechnical Commission, "Digital data communications for measurement and control—Part 1: profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems," IEC 61784-1, Geneva, Switzerland, 2001.

E.4 International Electrotechnical Commission, "Digital data communications for measurement and control—Part 3: Profiles for functional safety communications in industrial networks," IEC 61784-3, Geneva, Switzerland, 2006.

E.5 International Electrotechnical Commission, "Industrial communication networks – Profiles – Part 3-1: Functional safety fieldbuses – Additional specifications for CPF 1," IEC 61784-3-1, Geneva, Switzerland, 2007.

E.6 American Petroleum Institute , "Process Control Systems, Part 1—Process Control Systems, Functions and Functional Specification Development," API Recommended Practice 554, Second Edition, July 2007, REAFFIRMED, NOVEMBER 2016.

E.7 American Petroleum Institute , "Process Control Systems—Process Control System Design," API Recommended Practice 554, Part 2, First Edition, October 2008, Reaffirmed, November 2016.

E.8 American Petroleum Institute , "Process Control Systems-Project Execution and Process Control System Ownership," API Recommended Practice 554, Part 3, First Edition, October 2008.

E.9 International Atomic Energy Agency, "Design of Instrumentation and Control Systems for Nuclear Power Plants," IAEA Safety Standards Series No. SSG-39, Vienna, 2016.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-7273

2. TITLE AND SUBTITLE

Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies

3. DATE REPORT PUBLISHED

MONTH	YEAR
March	2021

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

Muhlheim, M. D., Poore, W. P., Nack, A. M., Wood, R. T., Melin, A. M., Bull Ezell, N. D., Hale, R. E., Holcomb, D. E., Huning, A. J., Halverson, D. S.

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Oak Ridge National Laboratory Managed by UT-Battelle, LLC Oak Ridge, TN 37831-6285

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This report provides a technical basis for evaluating the safe use of EDDs in commercial nuclear power plants (NPPs) in the United States (U.S.), along with relevant observations, based on their classification, functionality, configurability, consequences of failure, and potential for common-cause failures (CCFs), and it reviews how other agencies worldwide, both nuclear and nonnuclear, regulate, approve the use of, and actually use EDDs.

Areas of interest include the types of components in safety-related applications most likely to have EDDs, methods used by other industries and countries to regulate the use of EDDs, and potential issues noted in industry. This information serves to support the technical basis for a graded approach in the selection and use of EDDs. A tangential supply chain issue is the use of replacement parts or parts in upgrades that may contain an undeclared digital device, as it may not meet the requirements for the safety-related application it is being used in.

Other attributes such as reliability (the ability to perform with correct, consistent results), diagnostics, operating experience, and failure modes were reviewed because of their use in risk informing the acceptance of the use of EDDs. Emerging technologies associated with EDDs were noted during this work, and are described in this report.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Embedded Digital Device, EDD, Emerging Technologies

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)

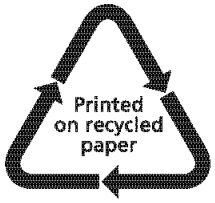
unclassified

(This Report)

unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG/CR-7273

Developing a Technical Basis for Embedded Digital Devices and Emerging Technologies

March 2021