Assessment of Technical Feasibility of Risk-Informed Approaches and Gaps Associated with Further Integrating Risk Insights into Regulatory Reviews for Digital I&C Systems and Components

REPORT ON TASK-1

SUBMITTED TO US NUCLEAR REGULATORY COMMISSION

CONTRACT: 31310018C0013

DATE 9/4/2020

INNOVATIVE ENGINEERING AND SAFETY SOLUTIONS, LLC
GERMANTOWN, MD, USA

PREPARED BY:
MOHAMAD ALI AZARM
SOLI KHERICHA

ACKNOWLEDGMENTS

The authors wish to thank Dr. Yaguang Yang and Mr. Mauricio Gutierrez of the U.S. NRC for their support of this project and their technical comments on the report. We also would like to thank Dr. Ming Li and Mrs. Suzanne Dennis of the U.S. NRC for sharing their technical insights regarding risk-informed regulations (RIR) and probabilistic risk assessment (PRA) methods for digital instrumentation and control (DI&C). We are also indebted to Dr. Tsong Lun Chu, our consultant, for providing insights related to the past NRC research and international studies, as documented in Section 3. Lastly, we would like to thank Dr. Zoran Musicki of the Johnson Space Center (JSC) office of SAIC, for his advice on NASA risk-informed activities and for clarifying some of the related NASA risk-informed requirements.

EXECUTIVE SUMMARY

This report documents findings for Task 1 of U.S. Nuclear Regulatory Commission (NRC) Contract # 31310019C0013. The findings in this report are intended to support NRC's reviews of risk-informed applications for digital instrumentation and control (DI&C) systems. The overall objective of this NRC contract is to provide support in developing the technical basis for integrating risk insights into the regulatory framework for DI&C systems and components. Task 1 of this contract is to assess the technical feasibility of risk-informed approaches and gaps associated with further integrating risk insights into regulatory reviews for DI&C systems and components. To achieve these objectives, this research study performed the following four sub-tasks.

1. Review of the state-of-the-practice including proposed state-of-the-art approaches for integrating risk insights into regulatory reviews by other relevant government agencies and their associated industries outside the nuclear industry (with a focus on I&C systems).

2. A summary of the current practices, lessons learned, and challenges in applying probabilistic risk assessment (PRA) and risk insights to nuclear power plant DI&C systems for operating and new reactors.

3. Identification of the potential regulatory and technical gaps associated with further integrating risk insights into regulatory reviews of DI&C systems and components. In particular, addressing challenges associated with applying Title 10 of the *Code of Federal Regulations* (10 CFR) 50.69 to DI&C systems and using applicable guidance provided in the Standard Review Plan (SRP).

4. Identification of requirements for methods, models, data, or analytical tools that need to be developed to enhance the use of risk insights within the existing risk-informed regulatory framework for DI&C systems.

The review results associated with each of these tasks are summarized in the main body of the report with the detailed discussion of their technical bases provided in the appendices. General findings associated with each of these tasks are provided below.

1. The risk-informed decision-making (RIDM) process for selected non-nuclear industries; civil aviation (Department of Transportation; Federal Aviation Administration—DOT/FAA), chemical industry, National Aeronautics and Space Administration (NASA), and Department of Transportation, Federal Rail Administration (DOT/FRA) were reviewed and found to be similar to NRC's risk-informed framework. All industries promote risk-informed rather than risk-based decision making. PRA is considered a complement to deterministic safety analyses and not a replacement. The deliberation that takes place before a decision is made to utilize the insights from the PRA and the related quantitative results are based on the review of a set of qualitative "deterministic" considerations. These deterministic considerations are designed to ensure that all safety requirements are met. These include design and operational requirements, prescriptive requirements, industrial standards, incorporating past lessons from operational events and resolution of findings from oversight activities. The RIDM process is applied during the design phase for selecting an acceptable design alternative, and the operational phase for management of changes (MOCs). As such,

the risk insights are generated from models with various degrees of sophistication; from qualitative hazard and operational assessment (HAZOP) to detailed state-of-the-art PRA. Such processes have also been used for DI&C systems. Except for NASA, all the remaining three industries rely on safety integrity level (SIL) classification. Reliability data for SIL-certified equipment are used directly as input to PRA (See Appendix A discussion on the reliability data and the common cause failure (CCF) likelihood for SIL-certified equipment).

2. Risk assessment is used as a complement for deterministic safety analyses and not a replacement in the selected four industries. The deliberation that takes place before a decision is made to utilize the insights from the PRA and the related quantitative results are based on the review of a set of qualitative "deterministic" considerations. In addition, industry-specific guidance documents are available; some are more detailed than others. At the process level (but not detailed approaches), all guides are like each other and that of the NRC; with differences in regulatory requirements (e.g., safety goals and use of national and international standards). Appendix A should be consulted for an industry-specific process and major differences.

3. Several special purpose PRAs for specific applications at nuclear power plants (NPPs) related to DI&C systems have been developed. Such studies have been sponsored by both NRC and the nuclear industry for operating and new reactors. These studies were reviewed and are summarized in detail to identify lessons learned and challenges in applying PRA and risk insights to nuclear power plant DI&C systems. These studies highlighted that the required level of detail and the scope of PRAs, driven by the specific applications, vary significantly. PRA methods and data are also dependent on the specific application and the PRA level of detail and scope. PRAs with higher resolutions in level of detail and larger scope introduce new challenges for PRA models and data. The major generic challenges identified for an integrated PRA, which include DI&C, are as follows:

    a. Management of the size and complexity of the PRA that includes DI&C systems by graded approach to the required resolution for PRA modeling and data that are commensurate with the level of detail and the scope demanded by the application.
    b. Inclusion of the hardware and software failure modes to meet the demands of the application. At minimum, two failure modes, failure to respond and spurious actuations are required for PRA of DI&C actuation systems. Additional failure modes could be considered for DI&C control systems (not just actuation). To manage the size and complexity of PRA (Item a), methods are required to prioritize when these failure modes should be explicitly modeled.
    c. Treatment of CCF for hardware and software and those resulting from the interactions of hardware and software. Due to lack of or limited CCF data; compliance with the NRC requirements on defense-in-depth and diversity must be examined before a tailored probabilistic model for PRA use can be developed. The tailored probabilistic model should account for partial and complete diversity and their effect on CCF probabilities. Deterministic guidance for defenses against the CCF triggering causes such as segregation and fault tolerance design (FTD) features have been provided by the NRC and NASA. NRC guidance on defense-in-depth and diversity (D3) requirements provides the best protection against CCF in DI&C systems and they should be considered for estimating CCF

contribution in PRA. Identification and evaluation plays an important role in CCF probability estimates.

d. The faults in a DI&C system are monitored by a self-monitoring algorithm and some faults are recovered before they can cause a system failure (fault coverage, fault monitoring and fault tolerance). To model fault tolerance features in PRA models, it is necessary to classify faults as detectable and non-detectable (also recoverable and non-recoverable).
e. Software provides the capability to integrate several different functions within a DI&C system. Software routinely integrates the control and actuations of many systems, each with a specific impact on plant risk. PRA models of integrated DI&C systems should be decomposed to each function with the associated impact on accident sequences and plant risk.
f. The unavailability of DI&C systems modules could significantly contribute to DI&C system failure probabilities. There are several different contributors to unavailability. PRA models should explicitly model the unavailability contribution for DI&C software and hardware.
g. Interaction of DI&C failures on human reliability analyses (HRAs) that are modeled in PRAs should be understood and documented. Those HRA impacts deemed to be risk significant should be explicitly modeled in PRAs.
h. The uncertainty sources for DI&C systems should be identified and estimated using any available methods (empirically or subjectively). The estimated uncertainties should be incorporated into the PRA model for evaluating their contributions to overall PRA estimates (mean and uncertainties). The uncertainty distributions of the plant risk resulting from PRAs with and without DI&C systems should be documented. Major uncertainty contributors should also be identified. Additional application-specific sensitivity analyses should also be documented.

4. Five Regulatory Guides (RGs) were evaluated to identify the potential regulatory and technical gaps associated with further integrating risk insights into regulatory reviews of DI&C systems and components. These RGs are as follows:

b. RG-1.174: Risk-Informed Licensing Changes [Ref. 1]
c. RG-1.177: Risk-Informed Technical Specifications [Ref. 2]
d. RG-1.200: Technical Adequacy of PRA Results for Risk-Informed Activities [Ref. 3]
e. RG-1.201: Guidelines for Categorizing Structures, Systems, and Components (SSC) in NPPs According to their Safety Significance [Ref. 4]
f. RG-1.205: Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants [Ref. 5]

These RGs can be divided into three groups for identification of the potential regulatory and technical gaps associated with further integrating risk insights into regulatory reviews of DI&C systems and components. These are the following:

- Group 1 RGs: These include RG-1.174, 1.177 and 1.201. These RGs describe a general risk-informing process that can be applied to any system or technology. These RGs are generally supported by more detailed NRC and industry implementation guides. The NRC's risk-informing process includes the following five steps:

    1. Meet the intent of regulations.
    2. Preserve defense-in-depth.
    3. Maintain safety margins.
    4. Utilize risk insight for RIDM and establish control.
    5. Establish assurance of control mechanisms through monitoring.

  Risk insight in Process Step Number 4 addresses the changes in risk results before and after change implementations in RG-1.174. Risk insights can also be incorporated into all five steps in the process. Specifically, risk insights could be used to develop focus guidance for Process Steps 1 through 3, especially for defense-in-depth and protection against CCF by maintaining adequate system redundancy and diversity. To adequately address the needs in all steps, the implementation of these RGs to the DI&C system imposes certain demands on DI&C PRAs. These PRA requirements should be delineated in the related NRC and industry guides.

- Group 2 RGs: This group includes RG 1.205. This regulatory guide provides guidance for risk-informed, performance-based fire protection programs that meet the requirements of 10 CFR 50.48(c). The process for RG 1.205 consists of the following two steps:

    1. The plant should first establish an approved National Fire Prevention Association 805 (NFPA 805) Fire Protection Program (FPP).
    2. A set of risk criteria is defined as the basis for making changes to the approved NFPA 805 FPP without prior NRC approval.

  Step 1 includes both the engineering/deterministic evaluation as well as the base risk assessment. The second step in the process then evaluates the change in risk when there is any deviation from the base or approved NFPA 805 FPP. RG 1.205 is specific to fire hazard. The process for risk management is written generically in a manner that can be applied to all systems including DI&C systems. Specific detailed guidance is also provided by several NRC/Industry reports.

- Group 3 RGs: This group includes RG 1.200. This RG is a high-level guidance document that specifies the attributes for determining whether the technical adequacy of the PRA, in total or in part, is enough to support an application. Meeting the guidance provided in RG 1.200 is sufficient to provide confidence in the PRA results, such that they can be used in regulatory decision-making for light-water reactors. This RG, plus the industry PRA standard endorsed by NRC, describe one acceptable approach for determining the technical adequacy of the PRA and to support the peer review process. Parts of these documents provide system-specific guidance for performing PRAs. The guidance for I&C systems is currently judged to be limited and may require additional instruction to support the specific RGs.

The NRC staff expects license amendment requests (LARs) to utilize diverse types of DI&C upgrades in operating reactors in the near future. The following conclusions from this study are intended to specifically support the license amendment review process.

1. The study found that Group 1 RGs represent a high-level process step that can be applied to any technological systems, including DI&C. Appendix C discusses the process for RGs in detail and identifies the possible needs for enhancing the specific steps within each of the RGs for obtaining the risk insights. However, this should not stop users from following the process as is. We do not anticipate any barrier for following the process described in the Group 1 RGs. The same is valid for Group 2 RGs. The Group 3 RG however should be updated to clarify if the existing state-of-the-practice for PRA for DI&C systems is an acceptable approach for ensuring consistency in use. Appendix B provides the current NRC and industry DI&C PRA practices.

2. The study found that the current guidance documents are not detailed enough to support consistent regulatory reviews for accepting the submitted LARs related to DI&C systems for the three groups of RGs. It was found that PRA guidance as it currently exists (RG Group 3 and the PRA standard) has limited information for the acceptability of DI&C PRA. These guides need to be expanded and enhanced by performing some pilot applications.

CONTENTS

List of Figures

List of Tables

ACRONYMS

A/D	Analog Digital converter
AC	Advisory Circulars
AFM	Airplane Flight Manual
AFMS	Airplane Flight Manual Supplement
AI&C	Analog Instrumentation and Control
ALARA	As Low As Reasonably Achievable
ALWR	Advanced Light Water Reactors
ANS	American Nuclear Society
AOT	Allowed Outage Time
APU	Acquisition and Processing Units
ASAP	Aerospace Safety Advisory Panel
ASARP	As Safe As Reasonably Practicable (related to NASA)
ASIC	Application-Specific Integrated Circuits
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
B&W	Babcock and Wilcox
CCF	Common Cause Failures
CCPS	Consul for Chemical Process Safety
CDP	Core Damage Probability
CCW	Component Cooling Water
CDF	Core Damage Frequency
CE	Combustion Engineering
CFR	*Code of Federal Regulations*
CREAM	Cognitive Reliability and Error Analysis Method
CRM	configuration risk management
CRMP	Configuration Risk Management Program
CSB	Chemical Safety and Hazard Investigation Board
CSRM	Context-based Software Risk Model
CT	Completion Time
D/A	Digital Analog Converter
D3	Defense-In-Depth and Diversity
DAL	Design Assurance Level
DB	Design Basis
DCD	Design Certification Document
DFM	Dynamic Flowgraph Methodology
DI&C	Digital Instrumentation and Control
DID	Defense-In-Depth

DOT	Department of Transportation
DRAP	Design Reliability Assurance Program
Edf	Électricité de France
EMI	Electro-magnetic interference
EOP	Emergency Operating Procedure
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
ESD	Event Sequence Diagram
ESFAS	Engineered safety features actuation system
ESW	emergency service water
ETA	event tree analysis
F&O	Facts & Observations
FAA	Federal Aviation Administration
FDAL	Functional Development Assurance Level
FDS	Fire Dynamic Simulator
FDT	Frequency of downtime per year
FEP	Fire Emergency Procedures
FET	Fault Exposure Time
FMEA	Failure Mode and Effect Analysis
FPGA	Field Programmable Gate Array
FPP	Fire Protection Program
FRA	Federal Rail Administration
FSAR	Final Safety Analysis Report
FTA	Fault Tree Analysis
FTD	Fault Tolerance Design
FV	Fussell Vesely
GE	General Electric
GIDEP	Government Industry Data Exchange Program
HAZOP	Hazard and Operational assessment
HIRA	Hazard Identification and Risk Assessment
HLR	High-Level Requirements
HRCP	Human Rating Certification Process (related to NASA requirements)
HRA	Human Reliability Analysis
HSS	High Safety Significance
I&C	Instrumentation and Control
IAP	Integrated Action Plan
ICCDP	Incremental Conditional Core Damage Probability
ICLERP	Incremental Conditional Large Early Release Probability
IDAL	Item Development Assurance Level
IDP	Integrated Decision-making Panel
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
ISA	Integrated Safety Analysis
IST/ISI	In-Service Testing and In-Service Inspection
LAR	License Amendment Request
LB	Licensing Basis
LCO	Limiting Condition of Operation
LERF	Large Early Release Frequency
LERP	Large Early Release Probability
LOC	Loss of Crew
LOPA	Layers of Protection Analysis
LOV	Loss of vehicle
LOM	Loss of Mission
LSS	Low Safety Significance
LWR	Light Water Reactors
MCR	Main Control Room
MDT	Maintenance Down Time
MFW	Main FeedWater
MOC	Management of Changes
MOP	Measures of Performance
MTTHE	Mean Time to Hazardous Event
MUX	Multiplexer
MVDS	Multi-Version Dissimilar Software
NASA	National Aeronautics and Space Administration
NEI	Nuclear Energy Institute
NFPA	National Fire Prevention Association
NIST	National Institute of Standards and Technology
NPP	nuclear power plant
NPD	NASA Policy Directives
NPR	NASA Procedure Requirements
NRC	U.S. Nuclear Regulatory Commission
NTSB	National Transportation Safety Board
MR	Maintenance Rule
OSRRP	Operational Safety Reliability Research Program
ORNL	Oak Ridge National Laboratory
OSHA	Occupational Safety and Health Administration
PASA	Preliminary Aircraft Safety Assessment
PB	PRA Based
PCS	Plant Control System (1)
PHA	Process Hazard Assessment
PLC	Programmable Logic Controller
PLS	Plant Control System (2)

PMS	Protection and safety Monitoring System
PRA	Probabilistic Risk Assessment
PRAM	Practical Risk Assessment Methodology
PSA	Probabilistic Safety Assessment
PSM	Process Safety Management
PTC	Positive Train Control
PWR	Pressurized Water Reactor
QA	Quality Assurance
QC	Quality Control
QRA	Quantitative Risk Assessment
RAP	Reliability Assurance Program
RAW	Risk Achievement Worth
RBPS	Risk Based Process Safety
RFI	Radio Frequency Interference
RG	Regulatory Guide
RIAC	Reliability Information Analysis Center
RICT	Risk-Informed Completion Time
RIDM	Risk-Informed Decision Making
RISC	Risk-Informed Safety Class (nuclear industry)
RISC	Risk-Informed safety Case (non-nuclear industry)
RIST	Risk Informed Technical Specification
RLV	Reusable Launch Vehicle
RMA	Risk-Managed Actions
RMAT	Risk-Managed Action Times
RMP	Risk Management Program
RPS	Reactor Protection System
RRF	Risk Reduction Factors
RSS	Risk Sensitivity Studies
RTCA	Radio Technical Commission for Aeronautics
RTS	Reactor Trip System
RV	Reentry Vehicle
SA	Safety Assessment
SCAI	Safety Controls, Alarms, and Interlocks
SCI	Safety Critical Item
SGTR	Steam Generator Tube Rupture
SIL	Safety Integrity Level
SMA	Safety and Mission Assurance (related to NASA)
SMS	safety management system
SOW	Statement of Work
SR	Supporting Requirements in relation to ASME/ANS PRA standard
SR	Surveillance Requirements in relation to Technical Specification

SRM	Staff Requirements Memorandum (used in relation to NRC)
SRM	Safety Risk Management (in relation to non-nuclear industry)
SRP	Standard Review Plan
SSC	Structures, Systems, and Components
TPM	Technical Performance Measure
V&V	Verification and Validation
W	Westinghouse

1. INTRODUCTION

1.1 Background

The U.S. Nuclear Regulatory Commission (NRC) staff expects license amendment requests to utilize diverse types of digital instrumentation and control (DI&C) upgrades in operating reactors in the near future. Operating reactors are expected to implement digital systems using existing software-based technologies and field-programmable gate array (FPGA) technologies. The NRC also expects a new generation of non-light water reactor (non-LWR) applications with advanced reactor technologies and highly integrated state-of-the-art digital systems.
The NRC's current I&C regulatory infrastructure is based on the Institute of Electrical and Electronics Engineers (IEEE) design and quality standards and defense-in-depth approaches. Within this infrastructure, the NRC staff routinely applies engineering judgment on issues of safety, informed by operating experience, in evaluating individual designs against regulatory requirements and guidance. In its staff requirements memorandum (SRM), SECY 15-0106, "Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," [Ref. 6] the Commission directed the NRC staff to modernize the NRC's I&C regulatory infrastructure. The NRC staff seeks to establish the technical basis for integrating risk insights into its technical reviews and inspections of digital systems. The use of risk insights may guide (1) the degree to which designs should comply with regulatory standards, (2) the level of detail in license amendments or applications, and (3) the level of NRC regulatory focus in performing reviews and in making decisions.

1.2 Objectives

The overall objective of this NRC contract is to provide support in developing the technical basis for integrating risk insights into the regulatory framework for DI&C systems and components by: (Task 1) assessing the technical feasibility of risk-informed approaches and gaps associated with further integrating risk insights into regulatory reviews for DI&C systems and components; (Task 2, an optional task) as applicable, piloting a risk-informed categorization process that is compatible with (i.e., not inconsistent with) the existing regulatory framework, including Title 10 of the *Code of Federal Regulations* (10 CFR) 50.69, "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors," to classify DI&C systems and components with respect to risk insights and safety significance; and (Task 3) developing recommendations for enhancing the use of risk insights within the existing risk-informed regulatory framework for DI&C systems.

This report documents the results of performing the work and the intended objective of Task 1.

1.3 Report Structure

This study includes four separate activities, as discussed below.

1. Review of the state-of-the-practice, including proposed state-of-the-art approaches for integrating risk insights into regulatory reviews by other relevant government agencies and their associated industries outside the nuclear industry (with a focus on I&C systems). A summary of this review is provided in Chapter 2 with supporting documentation of the findings in Appendix A.
2. A summary of the current practices, lessons learned, and challenges for applying probabilistic risk assessment (PRA) and risk insights to nuclear power plant DI&C

systems for operating and new reactors. A summary of this review is provided in Chapter 3 with supporting documentation of findings in Appendix B.

3. Identification of the potential regulatory and technical gaps associated with further integrating risk insights into regulatory reviews of DI&C systems and components. Addressing challenges associated with applying 10 CFR 50.69 to DI&C systems and using applicable guidance provided in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” the Standard Review Plan (SRP). A summary of this review is provided in Chapter 4 with supporting documentation of the findings in Appendix C.
4. Identification of requirements for methods, models, data, or analytical tools that need to be developed to enhance the use of risk insights within the existing risk-informed regulatory framework for DI&C systems. This is discussed in Chapter 5 based on the findings from Chapters 2 through 4 and Appendices A through C.

2. INTEGRATING RISK INSIGHTS INTO DECISION MAKING NON-NUCLEAR INDUSTRIES

Risk-informed decision making (RIDM) and the use of risk insights in the regulatory structure of selected industries were examined. The selected industries included civil aviation (Department of Transportation/Federal Aviation Administration—DOT/FAA), chemical industries, the National Aeronautics and Space Administration (NASA), and the Department of Transportation/Federal Rail Administration (DOT/FRA). This section summarizes the major findings from this effort based on a detailed discussion provided in Appendix A. Appendix A documents the risk-informed regulatory practices and the associated guidance documents, to the extent possible, for the above four non-nuclear industries. Specific emphasis is made on the use of risk models and data for RIDM and DI&C systems. This research was performed to better identify the challenges for performing risk informing DI&C systems and the associated PRA models and data based on the current practices in four non-nuclear industries.

The risk informing regulatory framework is generally consistent amongst all these industries. The safety during design and commissioning starts with system classification based on accident analyses, followed by prescriptive and engineering requirements, including “development assurance” (i.e., quality assurance and quality control) requirements for each class of systems. In some industries (e.g., FAA and NASA), explicit reliability/risk goals are also defined for each class of systems at the design stage (for example see Figure A-2 in Appendix A for FAA). The safety during operation is maintained through the safety management system (SMS). The SMS includes formal methods for identifying hazards and mitigating risk and promotion of a positive safety culture. The SMS is built by structuring the safety management around four components: safety policy, safety risk management (SRM), safety assurance (SA), and safety promotion. The SRM component provides a decision-making process for identifying hazards and mitigating risk based on a thorough understanding of the organization’s systems and their operating environment. SRM includes decision making for acceptance of risk during operation (for example see Figure A-3 in Appendix A). The SRM also provides input to the design process by identifying ways of incorporating risk controls into processes, products, and services or by redesigning controls where existing ones are not meeting the safety objectives as detected by SA.

Although on a generic level, all industries follow the same framework, each industry has tailored the process to its individual needs. The differences in technologies, severity/consequence of accidents in each industry, and the emphasis of quantitative risk insights vary amongst the industries. A detailed comparison of the risk-informed approaches down to the detailed technical level would be difficult (possibly misleading) and is avoided. A focused comparison, however, is made for six major application areas as discussed below (Sections 2.1 to 2.6). These areas are as follows:

1. Structures, systems, and components (SSC) classification
2. Risk / reliability and regulatory requirements for DI&C
3. Failure and reliability data for DI&C
4. Software failure and reliability data
5. Risk model that includes DI&C
6. Common cause failure (CCF) software and its inclusion in risk models

2.1 Identification and Classification of Risk-Significant SSCs

Identification of risk-significant SSCs (safety critical systems) is generally done during the design stage and with the use of a risk matrix. Any changes in SSC classifications after design and during operations are included in in the management of change (MOC) process. The MOC generally involves the re-evaluation and update of the design process for SSC classification. All industries reviewed rely on a risk management framework similar to what was discussed under SMS.

The classification of safety critical systems is accomplished using the following steps:

1. The risk matrix (See Figure A-4 in Appendix A, for example) is developed for all decisions to be considered. The risk matrix maps the decision impact in terms of severity (consequence) and occurrence frequency for each item under consideration. Although the concept of risk as the product of consequence and probability is embedded in risk matrix, risk is not directly estimated. The consequence associated with the risk matrix could cover several areas (safety, cost, environment, etc.). A separate risk matrix is developed for each consequence with its own associated threshold. The risk matrix developed in this manner can provide a means for comparing the potential effectiveness of proposed risk controls and prioritize risks when multiple consequences are present.
2. The items are graded based on the two attributes: consequence and occurrence frequency. Regions of the matrix are generally divided into four to five regions. Each region is then highlighted by a qualitative index. The indices generally reflect the importance of each region to safety.
3. If the risk as identified in the risk matrix is acceptable after applying specific risk controls for each class of items, then the system may be placed into operation and monitored.
4. If the risk is not acceptable, risk controls or design changes must be developed, and their effectiveness is estimated and monitored in the SA process.

Development of the risk matrix is also discussed in MIL-STD 882E, "System Safety," [Ref. 7]. The risk matrix can be constructed both qualitatively as well as quantitatively, depending on the maturity stage of design and level of PRA fidelity and completeness.

2.2 Risk / Reliability and Regulatory Requirement for DI&C

All non-nuclear industrial sectors, except NASA, have explicitly provided risk-informed regulatory guidance for DI&C systems and relied on the Safety Integrity Level (SIL) classification and certification for both software and hardware to meet the design and operational requirements. NASA mainly relies on its own prescriptive requirements based on the risk-informed classifications of systems. NASA utilizes additional risk controls through risk-informed processes driven by risk insights generated from application-specific PRAs. The extent of the use of quantitative PRA methods compared to other less quantitative methods (e.g., risk matrix) is based on the design maturity, maturity of PRA methods and data, and the availability of detailed design information.

An example of NASA requirements is provided here for further clarification since NASA does not use the SILs classification and requirements. NASA, like other industries, relies on redundancy and diversity of DI&C software and hardware for protection against CCFs. NASA, however, has its own set of guidance. For example, for NASA, diversity in software may include multi-version dissimilar software (MVDS), similar to N-version programing. NASA may also consider partial diversity, such as using diverse technology for both hardware and software as an acceptable approach for meeting diversity requirements depending on the assigned risk-informed system classification (see Section A.4.3 in Appendix A). The ultimate diverse system for NASA could include manual override and control, or if possible, use of an abort function, which may be implemented for a system classified as risk significant.

IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems,” [Ref. 8] provides a set of controlling features for each SIL class. These controlling features include the design specification for the system and its components, certification under specific quality assurance and quality control (QA/QC), operation and maintenance to ensure an acceptable value for CCFs. These features include redundancy, early diagnosis, fault tolerance features, diversity in design, and segregation in operation and maintenance. IEC 61508 also provides risk-reduction factors (RRFs) such that when applied to existing nominal values based on SIL classification would yield the new CCF estimate. IEC 61508 also provides bounds on the nominal estimates for reliability and for the CCF potential of each SIL class item. In effect, a case-specific CCF probability and associated bounds can be estimated using the calculated RRFs.

Although the information in IEC 61508 appears to be quite promising for performing risk-informed applications, the technical basis for these estimates and RRF values is not known and needs to be examined.

2.3 Failure and Reliability Data for DI&C

There is a significant amount of reliability data in the four industries that is considered for the SMS process. The sources of the data from these four industries are identified in Appendix A. A major source of reliability estimates for both hardware and software are reported in IEC 61508 for those systems and components that meet IEC 61508 requirements. The most DI&C-related hardware failure data are available through the chemical sector, NASA, and FAA. The related data sources are identified in Appendix A. A detailed review of these data sources from these three industries was outside the scope of this project. The data used to support the estimates for IEC 61508 is not publicly available and is also considered beyond the scope of our review. Since the design and implementation of positive train control (PTC) for DOT/FRA is in the early stages, we do not expect a rich data environment at DOT/FRA.

2.4 Software Failure and Reliability Data

The use of a risk-informed process like SMS also requires DI&C software failure and reliability data. Estimating the software reliability and failure rate is more challenging than estimating hardware reliability. This is because the software generally performs multiple functions, varies in complexity, and is of various pedigrees. For example, simple software, which is used for a risk-critical safety function where exhaustive testing has been performed, is expected to have an exceedingly small failure rate. A general approach is to define a set of attributes for the software and identify the most important combinations that can provide a generic estimate for the software failure rates. NASA sometimes uses a different approach for estimating the software-specific reliability for safety critical software, which must respond to several different demands under varying conditions (generally referred to as a context-based approach). In this approach, failure rates are estimated from a large number of context-based simulations. Such approaches are resource intensive and are used for limited cases or for research purposes only.

Software reliability data is also reported in IEC 61508 for those DI&C systems (both hardware and software) that meet IEC 61508 requirements. Other sources of software failure data could be found from the detailed accident investigation report. These include the Chemical Safety and Hazard Investigation Board (CSB) for the chemical sector, the National Transportation Safety Board (NTSB) for DOT/FAA and DOT/FRA, and NASA's Aerospace Safety Advisory Panel (ASAP). These reports can form the basis for the lessons learned and insights gained from the past incidents to support the SMS regulatory process.

2.5 Risk Model

Risk assessment and generating risk insights for developing risk controls are important tasks in the SRM part of SMS. Risk guidance, including PRA methods and data, vary significantly amongst the four industries reviewed here. These are briefly summarized below. More detailed information is provided in Appendix A, specifying the PRA guidance documents and the use of methods and data across these non-nuclear industries.

a) There are many chemical facilities in the U.S. and abroad for various applications. However, these facilities have similar components and systems (such as evaporators, chemical reactors, and heat exchangers) that are controlled by DI&C systems. Consequently, failure data, failure causes, and failure rate estimates are generally made at the system or function level. This allows for a simpler risk model of the facility with less level of detail in modeling. Risk models such as Layers of Protection Analysis (LOPA) are sometimes used for generating risk insights. Chemical facilities in most countries, including the U.S., also rely on IEC 61508 for their DI&C systems (both hardware and software). As these systems meet IEC 61508 requirements, the reliability data from IEC 61508 could be used to the extent possible. The consequences of accidents in chemical facilities vary based on the toxicity of the various chemicals they use and the possibility of energetic fires and explosions. The consequence analysis should address both the worker risk as well as the public consequence of accidents. The public consequence analysis is as complex as those for nuclear accidents and involves the evaluation of release magnitude, energy of release, and impact on individuals and the environment. Consequence evaluations for chemical accidents generally require detailed consequence analyses. So chemical industries use simpler PRA models, but complex models for consequence evaluation (called the severity index).

b) NASA and FAA use all conventional risk methods, such as Hazard and Operational assessment (HAZOP), fault tree analysis (FTA), event tree analysis (ETA), event sequence diagram (ESD), and failure mode and effect analysis (FMEA) supported by qualitative engineering arguments. Some dynamic methods, such as Markov and dynamic flow methodology (DFM) are also being researched and piloted at NASA to capture risk during phase transitions. However, there are some differences in addressing data needs for risk assessment. FAA has a large exposure (large number of demand) and a relatively low failure occurrence rate, resulting in a sufficient amount of failure data to support failure rate estimation. FAA also relies on generic estimates from IEC 61508. NASA has a smaller number of demands but extreme service conditions (higher temperature, radiation, etc.), which result in a higher failure rate. NASA generally relies on component-specific reliability data due to unique service conditions to which DI&C systems are exposed.

c) DOT/FRA PRA is somewhere between the chemical industry and NASA/FAA. For cases when the system or the change of the system is not expected to result in any new failure modes and the severity of accident (consequence) of the hazard or failure is not expected to change significantly from the previous design, an abbreviated risk assessment is used. For abbreviated risk analysis mean time to hazardous event (MTTHE) is used for risk-informed decision making. For all other cases, conventional methods such as HAZOP, FTA, ETA, and FMEA supported by qualitative engineering arguments are used.

2.6 Software CCF and Its Inclusion in Risk Models

Understanding and estimating CCFs are important parts of risk assessment and generating risk insights for the SMS process. For the four industries considered, there is extensive discussion on engineering/deterministic methods for determining software criticality and setting requirements for certification similar to practices done within NRC as described in SRP Chapter 7, “Instrumentation and Controls.” All industrial sectors have proposed several protective features against software CCF. Examples of these features include MVDS, early diagnostic and fault tolerance features, diversity in design, and segregation in operation and maintenance. With all these precautionary actions, the potential for software CCF still remains. Some industries use IEC 61508-6 Annex D to estimate the value of the β factor specific to the strategies they have taken against the CCFs. A case-specific CCF probability is estimated using the RRFs as prescribed by IEC 61508-6 Annex D to account for the implemented defenses against CCF. IEC 61511-1 [2015], “Functional Safety - Safety Instrumented Systems For The Process Industry Sector - Part 1: Framework, Definitions, System, Hardware And Application Programming Requirements,” has included an evaluation of the common cause for safety controls, alarms, and interlocks (SCAI) layers. Achieving an RRF value of 10,000 will result in a reduction of 10,000 for base-value of CCF when no credit is given to CCF defenses. Risk-informed studies may set an RRF goal of 1000 and identify the CCF defense mechanisms, which can result in the desired RRF value. However, if the RRF goal (required value) is greater than 10,000, specific analyses beyond IEC 61508 are needed to quantitatively estimate the contribution of CCF.

Incorporation of software in risk models are done with different levels of sophistication and this is still an active area of research. Different ways of incorporating software in risk models could include from adding a single basic event to a fault tree node or as a branch of an event tree to a more complex approach by NASA, which assigns different software failure rates for different functions and different conditions. NASA also discusses a software reliability model referred to as the “Context-based Software Risk Model” (CSRM). The CSRM methodology appears to be in the research stage with a possible limited application to safety critical software. It involves several steps, which include: (1) identification of mission critical software functions, (2) mapping of software-function to PRA event trees, (3) developing the branch heading of event trees down to the point where they can either be represented by basic events or quantified using dynamic models, if needed. Once the models are structured, then minimal cutsets can be generated. The context defined by the sequence or the minimal cutset can help to determine the software reliability for the specific condition for which it should be evaluated.

3. CURRENT PRACTICE AND LESSONS LEARNED FROM APPLYING PRA TO I&C SYSTEMS FOR OPERATING AND NEW REACTORS

An analysis of risk-informed reviews of analog instrumentation and control (AI&C) systems can provide lessons on applying PRA and risk insights to DI&C systems. The existing I&C (i.e., AI&C) systems are perceived as non-dominant risk contributors for the current generation of nuclear power plants. Safety I&C systems, such as the reactor protection system (RPS) and the engineered safety features actuation system (ESFAS), are constructed with redundant and diverse subsystems. In addition, they are built in diverse paths for accomplishing safety functions in the current generation of reactors. Each critical safety function, such as core cooling, can be actuated with a minimum of two diverse means; therefore, it is supported by two sets of diverse I&C systems. Beyond the ESFAS and RPS systems, this level of redundancy and diversity is not available for other I&C systems.

I&C systems, which control the operating plant systems, whose failures can cause plant initiators, do not have similar levels of redundancy and diversity. The same is also true for I&C systems for non-safety systems. Experience data has shown that the contribution of I&C systems to initiators is not insignificant [Ref. 9]. There are only a few initiators that could be caused by I&C failures that are shown to be risk significant in plant-specific PRAs (e.g., loss of service water system, loss of main feedwater). Failure of the I&C system may have to be modeled for the cases when it can result in risk-significant initiators but not for other initiators that are not risk significant (e.g., turbine trip).

There has been a significant amount of studies sponsored by NRC and the Electric Power Research Institute (EPRI) for PRA modeling of DI&C systems, which can be used as the foundation for identifying the related challenges and insights. These studies show that different risk-informed applications require a different scope and level of detail of PRA. Depending on the application needs, the models could vary from a qualitative evaluation to a highly sophisticated, detailed, quantitative model. The challenges and insights should be considered with respect to the application needs.

This section is written in three subsections. A more detailed description of the findings and their technical basis is provided in Appendix B. The first subsection is devoted to EPRI activities and the second subsection summarizes the past NRC studies and some of the international works. The third subsection summarizes the combined list of all challenges and insights for modeling AI&C/DI&C PRA learned from the previous two subsections.

3.1 Challenges and Insights—EPRI Studies

EPRI 1019183, “Effect of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants” [Ref. 10], uses a full-scope, Level 1, internal events PRA for a typical pressurized-water reactor (PWR) and modifies it to include a plant-wide digital upgrade of the I&C systems. The focus of the study was to evaluate the effects of the I&C in the context of the overall integrated plant design as opposed to focusing on the digital system itself (main focus on risk contribution rather than a detailed I&C system model). This is important since the study can address similar issues for the AI&C as well as DI&C. For DI&C and the potential for CCF, the study concludes that the introduction of diversity is of great value when defense-in-depth and diversity are designed in the mechanical and electrical systems that the I&C controls. In this study, EPRI claims that, “If this diversity does not exist in mechanical and electrical systems that the I&C controls, introducing diversity into the I&C system for the purpose of reducing CCF would be of little value."

EPRI 1025278, "Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments" [Ref. 11], also developed guidance on the modeling of DI&C in PRA. Following the previous EPRI report, this report concludes that the modeling of DI&C in a nuclear power plant PRA can be accomplished using many of the same methods used to model AI&C. This is due to the fact that components making up DI&C perform many of the same functions as their analog counterparts (e.g., sensors, signal processors, voting and actuation devices); the difference is that a subset of these functions may be accomplished by different component types (e.g., processors as opposed to electrical/electronic components such as relays or signal converters). The significant change between modeling of digital versus analog systems in nuclear power plant PRA is the inclusion of software and its failure modes. In addition, the report identifies some PRA modeling and data challenges for DI&C systems, which could include advanced diagnostic methods such as the use of watchdog timers, data validation routines, and fault detection and fault tolerance techniques.

EPRI 1025278 also emphasizes that the development of digital I&C modeling in PRA is a joint effort between the PRA analysts and I&C specialists familiar with I&C design. It recommends a nine-step process for performing AI&C/DI&C PRAs. These nine steps are shown in this reference (Figure 2-1 of EPRI 1025278) and it is discussed further in Appendix B. Step 4 in this process expects that the PRA analyst will develop a simplified model using high-level events and "super-components" for I&C failure effects. This crude model is used to screen down the number of I&C systems for which detailed models must be developed based on the assessment of relative importance of the digital system failures. The relative importance of the digital system failures is discussed in Step 5 through importance and sensitivity analysis. It is also important to note that this guide requires that the I&C specialist use detailed digital system design information (e.g., failure mechanisms, defensive design measures) to develop reasonable parameter estimates for use in PRA considering the sensitivity of PRA results to the I&C failure. This is somewhat in contrast to other studies where the PRA analyst takes the lead in developing the estimates with support from I&C engineers. The input of the I&C lead is necessary to group and characterize the data from manufacturer or operational experience as support to the PRA lead.

There are several recommended lessons and challenges identified by EPRI 1025278. A recent paper, "Modeling Digital I&C in PRA: Considering Context and Defensive Measures" [Ref. 12], closely related to this EPRI guide, focuses on the context and defensive measures for PRA modeling of DI&C systems. This article identifies four tasks necessary for software failure evaluation. These are as follows:

1. Development of a digital system reliability model
2. Identification and classification of failure mechanisms
3. Assessment of defensive measures
4. Quantification of residual failure modes and mechanisms

There are also three other citations from EPRI that relate to software data including CCF for modeling DI&C: EPRI 1016731, "Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems," December 2009 [Ref. 13]; EPRI 1021077, "Estimating Failure Rates in Highly Reliable Digital Systems," December 15, 2010 [Ref. 14]; and EPRI 1022986, "Digital Operating Experience in the Republic of Korea," 2011 [Ref. 15]. These are noted here as possible references for future use. It is important to note that these references are the basis of sometimes quoted probability of failure on demand (P) of a computing unit due to unknown functional specifications or design errors. A value of 1.0E-4 per demand is declared in these reports. This estimate, however, is an order of magnitude higher than the estimates recommended by EPRI 1025278 and IEC 61508 (i.e., 1.0E-5 per demand). It could be more applicable to SIL-2 or SIL-3 of IEC-61508 certified software classes.

A summary listing of lessons and challenges identified by various EPRI studies, as interpreted by this review, is given below. It should be noted that the authors of this report could not verify all conclusions made in these reports based on available documentation. They are simply documented for further examination and use. Furthermore, these studies were applicable to existing operating nuclear power plants and the assertions made may not be applicable to new and advanced reactors with passive designs and higher reliance on control systems to maintain the plant within allowable limits.

1. Safety-related software development process for nuclear power plants is generally considered as equal to or better than SIL-4 of IEC Standard 61508. Use of SIL-4 bounds for failure rates could be applied.
2. The modeling of DI&C systems for normal plant control systems may not be necessary since their contribution is mostly included in initiating event frequency and the DI&C contributions are generally not dominant contributors. The contribution of DI&C systems for the balance of plant systems when credited as a mitigation system post-trip may not have to be modeled, since the general practice is either manual control or restricted control. For example, consider the control of a main feedwater (MFW) pump following a reactor trip. Some plants automatically bypass the normal three-element control of feedwater flow in preference to a predetermined flow setpoint or switch to single-element control.
3. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.
4. The plant protection system, such as the reactor trip (RTS) and ESFAS should be a primary I&C focus for the PRA. These systems interact with many different mitigation capabilities and must perform under many different contexts (initiator and accident sequences).
5. The mitigating systems that support critical functions can be a mix of safety-related and non-safety-related systems. Dependencies between these mitigating systems considered in the PRA include not only shared equipment but also interaction of digital systems.
6. Non-safety-related mitigating systems also to be considered in the PRA are generally for accident sequences that go beyond design-basis events. These may include diverse systems required by regulation (e.g., anticipated transient without scram [ATWS] systems) or other plant systems that are capable of backing up the functions provided by the safety systems (e.g., main feedwater, fire system, containment venting, etc.). Whether these systems are affected or controlled by DI&C may vary from plant to plant. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.

7. The support systems (component cooling water [CCW], emergency service water [ESW], chilled water, instrument air, etc.) may include system-specific controls. These controls are generally dedicated to a specific support system and are not integrated across support systems. Simplified PRA models at the module levels may be developed for these systems as a part of support system failure probability estimation.
8. A large number of redundant and diverse indications and displays are available in the control room, the impact of the partial loss of indication and display on operator actions and control may not have to be modeled unless a significant number of them are lost in a scenario (e.g., such as fire). Non-safety-related controls and displays in the control room are designed so that a credible failure will not interfere with automatic protection system functions. Conversely, the manual control systems credited for diversity and defense-in-depth (D3) assessments are independent of the postulated protection system computer failure. Detailed PRA modeling may not be required for such cases.
9. Digital system common cause can have both intra- and inter-system impacts on mitigation systems. CCF events could be initially modeled as a super component finding whether further detailed modeling is necessary.
10. For a plant-wide digital system, the operating system for DI&C (computers) can be common to many plant systems, both mitigating systems as well as normal operating systems. The CCF due to a fault of the computer operating system is generally negligible as long as it is designed to perform cyclically, with few interruptions and is not affected by plant conditions.
11. Similar to the operating system, cyclic operation with transmission of information that is transparent to the values communicated, results in limited potential for communications units to contribute to the failure of the digital system due to CCF.

Some of the challenges for traditional PRA modeling of DI&C that were interpreted from the various EPRI reports are summarized below:

1. Determination of an appropriate level of detail in logic models.

2. Failure mode, failure probabilities and associated uncertainties for DI&C hardware accounting for specific technology, failure modes, fault tolerance and other defensive measures.

3. Failure probability of software is difficult to estimate since the faults are generally designed and are not random. Furthermore, the faults can be eliminated when occurred and detected, and the failure rates are greatly affected by software development and verification and validation (V&V) processes, error checking techniques, and diagnostics (for hardware and software interactions).

4. Inter- and intra-system CCF for software and the computer operating systems when various methods of diversification are used.

This study considers an appropriate level of detail in the PRA models should be commensurate with the needs of the specific risk-informed application. The PRA level of detail should not be discussed in a vacuum. A major focus of this study is the PRA application for SSC classification. The necessary level of detail for this application is addressed in Sections 4 and 5.

3.2 NRC, International, and Vendor Studies

PRA modeling for DI&C systems is discussed in detail as a part of SRP Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors" [Ref. 16]. This document lists several areas that the staff considers to be important and should be reviewed by the NRC for DI&C systems. The SRP does not discuss the guidance or the level of detail for the review.

A subset of these review requirements is considered challenging and is summarized below. Appendix B could be consulted for other items discussed in SRP Chapter 19.

1. The modeling of DI&C systems should include the identification of how DI&C systems could fail and what these failures could affect. The failure modes of DI&C systems are often identified by the performance of failure modes and effects analyses (FMEA). It is difficult to define DI&C system failure modes especially for software because they occur in various ways depending on specific applications. Also, failure modes, causes, or effects often are intertwined or defined ambiguously, and sometimes overlap or are contradictory. Examine applicant documentation to ensure that the most significant failure modes of the DI&C are documented with a description of the sequence of events (context) that need to take place failing the system. The sequence of events should realistically represent the system's behavior.
2. The DI&C reviewer should confirm that DI&C system equipment can meet its safety function in environments associated with accident sequences modeled in the PRA. This is done in collaboration with the reviewer for the PRA and severe accident evaluation that provides input on the expected environments that need to be considered.
3. The PRA reviewer should confirm that the impact of external events (i.e., seismic, fire, high winds, flood, and others) on DI&C has been addressed in the PRA.
4. Coordinate the review of human reliability assessment (HRA) with staff evaluating areas such as main control room design and minimum alarms and controls inventory. If recovery actions are modeled, they should consider loss of instrumentation and the time available to complete such action.
5. Verify that key PRA assumptions for DI&C systems are captured under the applicant's design reliability assurance program (DRAP), which is described in SRP Chapter 17, "Quality Assurance," Section 17.4. The applicant should describe adequately where and how the DRAP captures the DI&C system key assumptions, such as how future software and hardware modifications will be conducted to ensure that high reliability and availability are maintained over the life of the plant.
6. Common cause failures can occur in areas where there is sharing of design, application, or functional attributes, or where there is sharing of environmental challenges. Each of the areas found to share such attributes should be evaluated in the DI&C analysis to determine where CCF should be modeled and to estimate their contribution. The CCF probabilities and their bases should be evaluated and provided based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of defensive measures meant to protect against CCF (e.g., separation and independence, operational testing, maintenance, diagnostics, self-testing, fault tolerance, and software/hardware design/development techniques and processes). Dependencies between hardware and software should be identified.

7. Design features such as fault tolerance, diagnostics, and self-testing are intended to increase the safety of DI&C systems, and therefore are expected to have a positive effect on the system's safety. However, these features may also have a negative impact on the safety of DI&C systems if they fail to operate appropriately. The potentially negative effects of these features should be included in the probabilistic model. An issue associated with including a design feature such as fault tolerance in a DI&C system modeled in a PRA is that its design may be such that it can only detect, and hence mitigate, certain types of failures. A feature may not detect all the failure modes of the associated component, but just the ones it was designed to detect. The PRA model should only give credit to the ability of these features to automatically mitigate these specific failure modes; it should consider that all remaining failure modes cannot be automatically tolerated. A fault-tolerant feature of a DI&C system should be credited either in the PRA logic model or in the PRA failure data, but not both.
8. If a DI&C system shares a communication network with other DI&C systems, the effects on all systems due to failures of the network should be modeled jointly. The impact of communication faults on the related components or systems should be evaluated, and any failure considered relevant should be included in the probabilistic model.

It is clear from the discussion in SRP Chapter 19 that there are many challenges in performing and reviewing the PRA for DI&C systems for new reactors. These challenges are generally consistent with those identified by other non-nuclear industries and regulatory bodies. DI&C systems and their associated PRAs are currently evaluated without any specific and detailed guidance. Developing a PRA test bed and performing some pilot applications and testing could generate more specific guidance to support SRP Chapter 19 review requirements. Additional challenges could be identified when a specific risk-informed application is considered (e.g., SSC classification for DI&C).

Another important challenge for performing the DI&C PRA is the determination of failure modes and their relative contributions. An NRC study at Oak Ridge National Laboratory (ORNL) [Ref. 17] was conducted to investigate DI&C systems and module-level failure modes, using several databases. The databases examined in this reference covered both nuclear and non-nuclear industries and included EPIX, COMPSIS, SPIDR, FARADIP, GIDEP, OREDA, and a civil aviation database. The objectives of the study were to obtain relevant operational experience data to identify generic DI&C system failure modes and failure mechanisms, and to obtain generic insights, with the intent of using the results to establish a unified framework for categorizing failure modes and failure mechanisms. Examples of such insights with their relative fractions of the overall data are summarized below:

a. About 11% of data evaluated involved application-specific integrated circuits (ASICs) and/or field programmable gate arrays (FPGAs). The "Loss of Programmed Memory" appears to be a significant failure mode of such devices. Failure modes of the ASIC cards included "failed passive components" (e.g., "shorted capacitor"), "failed output" (LO or HI), "shorted operational amplifier," and "intermittent loss of power."
b. About 35% of failures in the EPIX data analyzed involved programmable logic controllers (PLCs). Failure modes included "Loss of Communication," "Incorrect Firmware Coding," "Loss of Power," and "Processor Lockup."
c. The EPIX database was found to contain little information on software failure modes. Less than 10% of the records analyzed were attributed to software. In addition, event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure.

Although the findings are useful, the study concluded that the lack of quality and detailed information did not allow the development of a unified framework for failure modes and failure mechanisms of nuclear I&C systems. This study was based on a small sample size of 226 out of 2,263 events. Setting aside the inability to develop unified failure modes due to the lack of quality of a data source, evaluation of a larger sample size could provide some additional information regarding the contribution (fraction of total) of failures of components to the overall failure counts. Such information can be used to scale the reliability data and the associated uncertainties.

The PRA for DI&C systems has mainly been in the research stage at NRC with limited pilot applications performed by the nuclear industries in two areas: upgrades to AI&C systems and DI&C for advanced reactors. The level of detail of most of these PRAs was at module levels. At this level of detail, the PRAs were evaluated using the generic data on DI&C hardware and software. However, there were a few cases where the PRA analyst had to develop models at a much lower level of detail, i.e., consistent with the level at which engineering FMEA was developed (device level consistent with FMEA vs. module level for common PRAs). One such case was reported by Westinghouse Electric Company, which contains several lessons of interest for this study [Ref. 18]. This paper focuses also on the protection and safety monitoring system (PMS) and its interaction with the plant control system (PLS). The PMS serves to perform the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip or engineered safety functions actuation, and component control functions. The PLS performs signal acquisition, calculations, setpoint comparisons, logic calculations, and component control to maintain the plant’s systems during all modes of operation. The interaction between these two systems (shared parameters and actuation between safety and non-safety) was the subject of this study. It should be noted that the interaction between safety and non-safety generally necessitates electrical and signal isolations. Developing PRA models at a detailed level (consistent with the level of FMEA) then becomes desirable for addressing the interaction between safety and non-safety systems. This study identified several important insights and challenges if the DI&C PRA models had to be developed at such level of detail (i.e., at the level of engineering analysis and FMEA). Some of these challenges and insights are identified below.

1. The failure modes tabulated in the FMEA are to be examined and the effects of the failure modes on the PRA success criteria assessed. However, the level of detail of modeling should also consider the available component failure data, which in most cases is not at the level for which the FMEA was developed.
2. Generic data for current operating plants; ESF and RPS systems, was not a direct one-to-one comparison with data needed in this study. The data used in the study were primarily developed using the “217Plus” software tool developed by the Reliability Information Analysis Center (RIAC) [Ref. 19]. It is the only tool that the Department of Defense authorized and supported the effort to collect and analyze data for use in reliability analyses.
3. Both unavailability and failure probabilities were modeled in the DI&C PRA for major components. Design features, such as the self-diagnostics capability, resulted in rapid detection of failures and replacement/repair. Consequently, reducing the unavailability contribution improved reliability.
4. Failure of the manual action using a soft control is modeled via manual CCF of operator workstations, failure of the power supplies to the cabinets supporting the operator

workstations, operator action failure, and failure of the PLS logic from the controller cabinet(s) to the actuated component(s).

5. As PRA models continue to expand to include special hazard events like internal flooding and fire, it is important to distinguish the main control room (MCR) actions from local actions outside the control room. The I&C system models and HRA should ensure that when credit is taken for manual actions from the MCR, the system model includes all components within the associated I&C cabinets that could fail the signal from manually actuating the equipment.
6. The ability to locally start equipment by bypassing the I&C cabinets should not be used as a justification for screening the I&C equipment from failing the actions. A control room action and a local action could be modeled with corresponding I&C failures for the same actuation.
7. Detailed modeling approach for the non-safety-related I&C equipment, the magnitude of circular logic in the model was significantly increased and was much higher than that seen in currently operating PWR PRAs. Somewhat related findings were also reported in NUREG/CR-6997, “Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods” [Ref. 20]. NUREG.CR-6997 found that the ordering of the failures in a sequence could change the outcome. Section 4.3 of this NUREG indicates that in a few simulations, some failure sequences did not cause system failure, but the same set (or a sub-set) of component failures in a different order did result in system failure. At detailed level of modeling of I&C systems, the frequent occurrence of circular logic and the varying impact of ordering of events in a sequence is expected. The treatment of circular logic is well known. The ordering of sequences can be handled via priority gates (logics) and the use of dynamic models for quantification. Neglecting the effect of ordered sequences will result in some degree of overestimation, which in some cases can be tolerable.

The study concluded that it could be more efficient and economically preferable to share plant parameters or actuations between safety-related functions and non-safety-related functions, but it can significantly affect the complexity of the PRA and may reduce defense-in-depth by introducing common failures that are generally evaluated by the PRA.

There have been many international studies regarding DI&C PRAs from where some lessons and challenges could be extracted. Reviews of all these documents were not considered within the scope of this study. Therefore, we concentrated on a major activity related to the development and application of a consensus taxonomy for using traditional PRA methods for modeling DI&C systems.

A major international effort was devoted to consensus development of failure modes taxonomy for reliability assessment of DI&C system for PRAs. NEA/CSNI/R(2014)16, “Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA” [Ref. 21], reports on the activities of an international consensus task group called DIGREL on developing the failure modes taxonomy for the reliability assessment of a DI&C system for PRAs. The purpose of the taxonomy is to support PRA framework for including DI&C systems, therefore, it focuses on high-level functional aspects rather than low-level structural aspects. This focus allows the handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems. A major part of their effort was devoted to developing a hierarchical definition of five basic levels of modeling. At the level of systems, divisions and I&C units, no significant distinction is made between hardware or software aspects. At the module and basic component levels, however, the taxonomy differentiates between hardware and software-related failure modes.

The consensus PRA taxonomy was implemented to develop the guidelines for reliability analysis of digital systems in probabilistic safety assessment (PSA) context, NKS-330, “Guidelines for Reliability Analysis of Digital Systems in PSA Context” [Ref. 22]. This study shows that the choice of the level of abstraction for the modelling of DI&C is of high importance for the results by using a simplified PRA model representing a four redundant distributed protection system. This study also categorizes hardware and software failures as detected and undetected. Detected failures are those discovered continuously by online monitoring while undetected failures are discovered off line. For undetected failures, this study does not differentiate between off-line detection during periodic testing and off-line detection that can only happen due to an actual demand. The study found both detected and undetected failures should be modeled, because they both contribute to system failure probability through unavailability and unreliability. The study suggests that to develop a realistic fault tree model for a digital I&C protection system, it is vital that the chosen fault tolerant design is fully understood and correctly described in the model. The study also attempted to evaluate the impact of the level of detail in PRA modeling on the results by comparing the approaches in four PSAs. A more detailed discussion of the models and results can be found in NKS-361, “Modelling of Digital I&C, MODIG-Interim Report 2015” [Ref. 23].

3.3 Insights and Challenges Identified by Applying Past PRAs

Both the NRC and industry recognize that developing the PRA that includes DI&C systems explicitly should address a set of concerns. These concerns are identified in different citations and they are summarized below:

- Common Cause Failures: new DI&C are internally redundant and there is a potential for introducing CCFs and possibly undesirable failure modes. The CCFs and other undesirable failure modes of DI&C systems that did not exist in the AI&C systems primarily deal with the DI&C software and the interaction of hardware with software. Errors can be introduced to software at different phases through its life cycle which can lead to CCFs. Different requirements exist to improve the pedigree of software development processes and enhance V&V techniques. There are also different contributors to CCF of DI&C hardware including external causes of CCF such as radio frequency interference (RFI)/electro-magnetic interference (EMI). To address these issues, NRC guidance requires defense-in-depth and diversity (D3), [Ref. 24] and evaluation [Ref. 25] for digital upgrades involving the RTS and ESFAS.
- Fault Coverage, Fault Monitoring and Fault Tolerance: The faults in a DI&C system are monitored by a self-monitoring algorithm and some faults are recovered before they can cause a system failure. Protecting a system from catastrophic damage is possible even for a fault that cannot be fully recovered. Multiple channel processing systems might have cross-channel monitoring functions. Independent heartbeat monitoring equipment is sometimes installed to detect response failure of the communication links or individual channels. Software-based intelligence and the flexibility of microprocessors accommodate these sophisticated reliability enhancing mechanisms [Ref. 26]. To model fault tolerance features in an actual reliability model, it is necessary to classify faults as detectable and non-detectable.

- Integration: Although the DI&C systems for support systems and normal plant operating systems (non-safety) are dedicated to a specific task in a specific system, there is significant integration on the safety-related side. Software provides the capability to integrate several different functions within a DI&C system. Software routinely integrates the control/actuations of many systems, each with a specific impact on plant risk. For example, the scram logic software integrates the scram functions for many different physical conditions (e.g., scram due to steam generator tube rupture and scram due to loss of primary flow). It also closely interacts with the ESFAS DI&C system and provides information to the operator's display units. As a result of such an integration, there could be many different failure modes of software, each representing one of many functions performed by the software. Integration of software could also facilitate generation of automated procedure, data, graphs, drawings, alarms, and other information/display to operators in the control room. Integrated DI&C could receive soft or hard commands from the operator as input for several different systems supported by the software. The multi-function integration allowed using DI&C systems provides efficiency but generates complexity due to shared resources. DI&C PRA models, when developed at a level of detail to address the integration, are expected to be complex. It may also require addressing HRA re-evaluation and consideration of operator performance, especially when a DI&C failure reduces the operator's ability to perform their actions inside and outside the MCR.
- Failure modes: DI&C failures modes (i.e., failure modes of DI&C modeled by PRA) are driven by the PRA failure modes of the systems supported/controlled by the DI&C system. For example, if the spurious actuation of a system was not modeled in the PRA and it was screened out, the failure modes of the DI&C system causing spurious actuation does not have to be considered. If a DI&C system supports several systems, unless the spurious actuations is screened out for all the systems, DI&C failure modes causing spurious actuations must be modeled in the PRA. The two failure modes that generally are considered for DI&C systems for actuation (not DI&C for dynamic control) for both hardware and software are failure to respond and a spurious response (actuation). The CCF of these failure modes for all DI&C channels is also to be considered for PRA modeling when necessary.
- Unavailability of single DI&C module: DI&C systems have smart features that could facilitate online testing and repair by setting the system status in a safe mode. Although, there would be no unavailability contribution from these events, the reduced redundancy could increase the failure rates associated with spurious actuation. Other software failures, such as operating system crash, would stop the entire computer system. Since many software problems are transient, a reboot often repairs the problem. This involves rebooting the operating system, running software that repairs the disk state that might have become inconsistent due to the failure, recovering communications sessions with other systems in a distributed system, and restarting all the application programs [Ref. 27]. Another contributor to DI&C unavailability relates to software upgrades either pre-planned or corrective. PRA models should explicitly model the unavailability contribution for DI&C software and hardware.
- Failure of single DI&C module: For a DI&C module, modeling the impact of individual hardware failures on module operation is more challenging than the AI&C train. The existence of fault tolerance, fault diagnostics, and voting systems could eliminate the impact of some failures. For some hardware failures, the interaction of software and hardware should also be considered. The latter specifically refers to memory failures and failure of microprocessors where hardware failure could interact with software and the resulting outcome may be difficult to predict. Methods such as fault injection

techniques [Ref. 28] are designed to discover some of these interactions, and at the same time, evaluate the effectiveness of fault tolerance capabilities to arrest fault propagation. DI&C PRAs may initially address this issue with a combination of empirical data estimation and the use of simple PRA models based on the available engineering and design information.

A complete review of all the references on the lessons and challenges of DI&C PRA is not possible. The focused reviews were selectively limited to those references that used traditional PRA methods and had the most breadth. It is also the opinion of the authors that other lessons and challenges will be identified when the DI&C PRA is used for specific risk-informed applications due to their varying needs for the level of detail and scope. The requirements of some risk-informed applications could be less than others. A plant PRA for DI&C systems constructed such that it allows flexibility for changing the models if needed, could be helpful for testing different risk-informed applications and identifying application-specific lessons and challenges.

4. RISK-INFORMED DECISION MAKING AT NRC

Risk-informed decision making has been used by NRC for the past three decades. During this period, risk information was used to guide the regulator to strengthen requirements, relax requirements, provide efficiency in the regulatory process, and better clarify compliance with the requirements.

In August 1995, the NRC adopted the PRA policy statement [Ref. 29] regarding the expanded use of PRA. This resulted in the use of risk insights in a risk-informed regulatory framework to address several NRC regulatory decisions for current reactors. Additional risk-informed regulatory activities have been implemented by NRC and the nuclear industry for the licensing of advanced reactors (10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”) and the next generation of nuclear power plants.

Risk-informed decision making at NRC was driven by two factors: (1) risk insights and (2) principal deterministic regulatory concepts (such as defense-in-depth, safety margins, and industry standards). The contribution of the PRA quantitative results and insights varies significantly across applications, depending on the PRA maturity, the uncertainties associated with PRA results, and the characterization of the issue being regulated.

4.1 Risk-Informed Applications Related to Changes in Licensing Basis

The current use of the NRC risk-informed regulatory framework is to support decisions to modify an individual plant’s licensing basis (LB). LB includes those licensee commitments that if modified would require NRC approval.

Figure 4-1, reproduced from Regulatory Guide (RG) 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” shows the current set of regulatory guides regarding the risk-informed regulatory framework and their relationships. These RGs are generally intended for risk-informed regulatory changes after the design is completed, the plant is constructed, commissioned, and licensed for operation. The change is assumed to occur during plant operation when a mature PRA supported by operational experience data is available.

The NRC will review applications for license amendments using traditional deterministic methods. The implementation of risk-informed guidance (RG 1.174) and the integration of risk insights to the regulatory framework could either be initiated by the NRC or the licensee. NRC may request an analysis of the risk impact related to the requested change of LB, to demonstrate that the level of protection necessary to avoid undue risk to public health and safety (i.e., “adequate protection”) is maintained. This could happen under special cases in which new information reveals an unforeseen hazard or a substantially greater potential for a known hazard to occur. Licensees may also utilize the risk-informed regulatory framework to further support the acceptability of the requested changes in LB. Such requests are made by licensees due to specific enhanced design and operational features in their plants beyond what is generally credited in traditional deterministic evaluations.

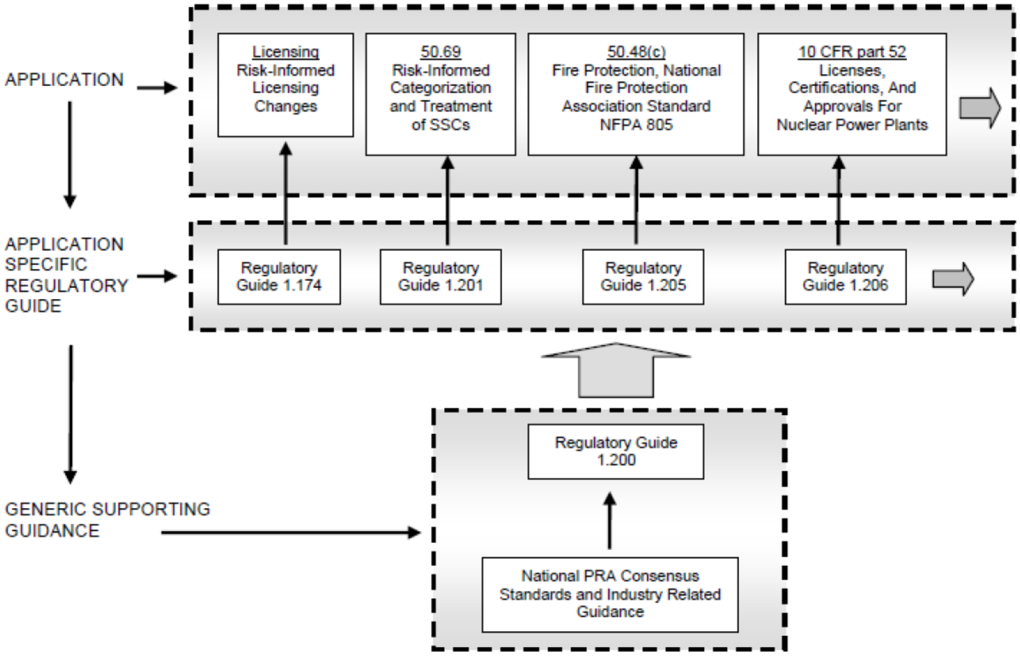

APPLICATION
APPLICATION SPECIFIC REGULATORY GUIDE
GENERIC SUPPORTING GUIDANCE
Licensing Risk-Informed Licensing Changes
50.69 Risk-Informed Categorization and Treatment of SSCs
50.48(c) Fire Protection, National Fire Protection Association Standard NFPA 805
10 CFR part 52 Licenses, Certifications, And Approvals For Nuclear Power Plants
Regulatory Guide 1.174
Regulatory Guide 1.201
Regulatory Guide 1.205
Regulatory Guide 1.206
Regulatory Guide 1.200
National PRA Consensus Standards and Industry Related Guidance

Figure 4-1 Regulatory Guides for NRC Risk-Informed Regulatory Framework and Their Relationships

RG 1.174 lists the following five principles that satisfy regulations and are included in the applications:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption (i.e., a specific exemption under 10 CFR 50.12, “Specific Exemptions”).
2. The proposed change is consistent with a defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the Commission’s Safety Goal Policy Statement.
5. The impact of the proposed changes should be monitored using performance measurement strategies.

The first three principles of RG 1.174 address single failure criteria, defense-in-depth and safety margins (balance between mitigation and control). These deterministic criteria are mainly prescriptive in nature. They do not focus on quantitative risk and reliability values. For example, redundancy and diversity will be treated the same for single failure criteria regardless of the failure probability for a redundant or diverse train. The fourth principle requires quantitative risk analysis and qualitative risk insights. The quantitative risk analysis results are intended to be used for evaluating the risk metrics before and after changes are implemented. The fifth principle is for monitoring and assuring that the operational reliability is maintained within acceptable limits. These principles are like the practices in other industries as reviewed and discussed in Section 2. However, there are some differences in two areas: (1) other industries place less emphasis on meeting the first three criteria if there is a mature PRA and the experience data shows that the risk is maintained, and (2) other industries use application specific risk criteria for risk metrics at different levels (i.e., their safety goals change as technology advances) supported by the latest design and operational data.

4.1.1 Lessons from Applications of RG 1.174

RG 1.174 is a document that can be used for any risk-informed applications that involve changes in the LB. RG 1.174 could also be used for the risk-informed application of DI&C systems like previous applications for mechanical, electrical, and AI&C systems. RG 1.174 clearly prescribes a process for a risk-informed application that can be followed by applicants. There are, however, some observations and lessons identified from the reviews of risk-informed processes in other industries (See Section 2 and Appendix A) and applying PRAs (See Section 3 and Appendix B) that may be considered for their applicability and use. These observations are discussed here.

The numerical risk criteria of RG 1.174 need a fully quantitative process. The user should first evaluate and characterize the impact of the requested changes in terms of quantities that could be used (for example as input data or fault tree changes) within the PRA model and data structures. PRAs should also be detailed enough and be of sufficient scope to allow the identified changes to be incorporated. The uncertainties associated with the impact of requested changes on PRA input and the uncertainties associated with PRA models and data as reflected on risk metrics (CDF/ΔCDF and large early release frequency (LERF)/ΔLERF) should also be evaluated. These are the basic requirements of PRA that are directly related to the PRA level of detail and scope.

This same consideration regarding level of detail and scope of PRA applies to DI&C systems. Approaches relying on PRA importance measures or sensitivity analyses have been used in some case-specific applications to supplement and build confidence that the risk criteria noted in RG 1.174 are met.

RG 1.174 puts significant emphasis on the first three deterministic criteria. The fourth criterion that relates to risk is only examined when the first three criteria are maintained. This is the case even if the PRA is fully developed and supported by well-compiled experience data for the specific application. Risk insights can also be used to streamline the review process for the first three principles by focusing on more risk-significant SSCs. This would increase efficiency and facilitate a graded review of the first three qualitative/engineering principles. Risk-informed prioritization methods can be used to support this objective. Other industries have used qualitative methods such as HAZOP analysis and quantitative sensitivity analyses using the base PRA. Similar approaches could be implemented for risk-informed reviews at NRC. Quantitative methods using the original PRA model without the I&C system combined with sensitivity analysis can provide the initial prioritization of various systems. The process is similar to that of RG 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance,” which is discussed in Section 4.3 for SSC classification.

RG 1.174 relies on specific values for risk criteria. The risk criteria are absolute and not intended to change based on the specific facility designs or applications. The risk criteria are currently the same for operating light-water reactors (LWRs) and advanced light-water reactors (ALWRs). The risk criteria used in other industries changes to account for new designs and the use of new advanced technology. Concepts such as cost benefit analysis and ALARA (As Low As Reasonably Achievable) are not formulated in RG 1.174. NRC, however, considers cost-benefit analysis as a part of PRA policy statement and formally for use in several areas of regulatory decision making. As an example, cost-benefit analysis is required as a part of

10 CFR 50.109, “Backfitting,” or the backfit rule. The Backfit rule examines if the direct and indirect costs of implementation are justified for the facility, in view of the increased protection.

4.1.2 AI&C/DI&C PRA Challenges to Support RG 1.174

As stated, the risk-informed process for RG 1.174 is clearly written and can be implemented for risk-informed applications for any systems, including DI&C systems. Supplemental guidance documents, however, are needed to help maintain the consistent use of RG 1.174. The review of specific guidance documents that support the development of various elements of PRAs (e.g., RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities”) is the focus of this study. RG 1.200 and other PRA-relevant guidance documents are discussed in a separate section. Here we identify the required capabilities of a PRA to support RG 1.174. This will provide a roadmap for examining the PRA guidance documents. The identification of the required capabilities of a PRA is achieved through a detailed examination of the process and the required PRA input (See Appendix C). The following lists the PRA-related guidance documents that are needed to support the application of RG 1.174 to AI&C/DI&C systems:

(1) The ability to evaluate the effect of the changes on PRA models. The effect of the changes on PRA models and data should be determined either by changing the probability data entered PRA, or by changes in PRA models[1].

(2) To the extent possible, the level of detail and scope of the PRA should be able to accept the set of proposed changes defined in Step 1 to minimize the need for changing the PRA models. To do this, PRAs must be detailed enough and of such scope that they can explicitly incorporate the changes. The required level of detail and scope could vary depending on the changes requested. For example, A PRA could have a sufficient level of detail and be of appropriate scope for the proposed design changes but not for certain procedural changes.

(3) The impact of changes on the PRA input and model depends heavily on the different hazards stipulated. All hazards and contributors to risk should be considered. PRAs must have the appropriate scope to evaluate the impact of changes under all hazards, relevant accident scenarios, and possible environmental conditions. The required scope of the PRA also depends on the changes requested. Some changes may require external hazards and others may not. Some applications may be performed without full development of Level 2 scenarios, and some may not.

(4) The ability of the PRA to estimate the risk metrics, e.g., CDF, LERF and the associated changes in an acceptable manner. An acceptable manner is generally defined as meeting the requirements of RG 1.200 and PRA standards [Refs. 3 and 30], peer-review [Ref. 31], and PRA quality control. There is no clear relationship between the categories of PRA standards and the requirements for the risk evaluation of various changes. PRA standards, e.g., PRA Category 2, establish a minimum set of requirements for change evaluation. Additional PRA enhancement or modification would be needed for application-specific use.

(5) The ability of the PRA to estimate the mean values of risk metrics by accounting for all sources of uncertainties [Refs. 32 and 33]. The issue of uncertainties is currently geared towards the overall results of PRAs and does not focus on the uncertainties associated with the effect of changes.

[1] A change in AI&C/DI&C can also introduce some failure modes that are not in PRA (e.g., spurious actuations) or a change may impact an accident sequence that is screened out of the PRA. In such cases, PRA models must be modified to accommodate the specific system failure modes.

4.2 Summary of RG 1.177

RG 1.177, “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications,” addresses risk-informed applications for two categories of technical specifications (TS); limiting conditions for operations (LCO) and surveillance requirements (SRs). A duration that a plant can reside in an LCO condition is limited by allowed outage times (AOTs), which are also referred to as completion times (CTs). Limiting CTs reduces the chance that an accident occurs during the LCO condition. CTs are determined to ensure that enough time is available for recovery and repair while at the same time avoiding unnecessary risk.

Like RG 1.174, RG 1.177 follows five principles:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption.
2. The proposed change is consistent with the defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in core damage frequency (CDF) or risk, the increases should be small and consistent with the intent of the Commission’s Safety Goal Policy Statement.
5. The impact of the proposed change should be monitored using performance measurement strategies.

Technical specification conditions addressed by CTs are entered infrequently and are temporary by nature. The frequency of entry into LCOs is generally unknown/uncertain. Therefore, the following TS acceptance guidelines specific to CT[2] changes are provided for evaluating the risk associated with the revised CT. These are:

1. The licensee has demonstrated that the CT change has only a small quantitative impact on plant risk. An incremental conditional core damage probability (ICCDP)[3] of less than $1.0x10^{-6}$ and an incremental conditional large early release probability (ICLERP)[4] of less than $1.0x10^{-7}$ are considered small for a single TS condition entry (Tier 1).
2. The licensee has demonstrated that there are appropriate restrictions on dominant risk-significant configurations associated with the change (Tier 2).
3. The licensee has implemented a risk-informed plant configuration control program. The licensee has implemented procedures to utilize, maintain, and control such a program (Tier 3).

The above multi-layer guidelines were developed to assure safety and maintain low-risk operation since the overall impact of changing CTs on plant risk is not evaluated since the frequency of occurrence is not known (See Appendix C for more information).

[2] Permanent changes to CT are discussed in this section. There are similar guidelines for a one-time change that is not discussed here.

[3] ICCDP = ((conditional CDF with the subject equipment out of service and nominal expected equipment unavailability for other equipment permitted to be out of service by the TS) − (baseline CDF with nominal expected equipment unavailability)) x (total duration of single CT under consideration).

[4] ICLERP = ((conditional LERF with the subject equipment out of service and nominal expected equipment unavailability for other equipment permitted to be out of service by the TS) − (baseline LERF with nominal expected equipment unavailability)) x (total duration of single CT under consideration).

4.2.1 Lessons from Applications of RG 1.177

Application of risk information to CT and SRs is perhaps one of the most widely used risk-informed application. RG 1.177 is a document that can be used for risk-informed TS application for any plant design and for any system including DI&C systems. RG 1.177 clearly prescribes a process for risk-informed TS application that can be followed by applicants. However, there are some observations and lessons identified from reviews of risk-informed submittals and applying PRAs that may be considered for their applicability. These observations are discussed here.

RG 1.177 is a quantitative risk application like what was discussed for RG 1.174, however with different quantitative risk criteria since conditional risk metrics are used. Use of RG 1.174 instead of RG1.177 would have required an estimation of the overall risk impact of a CT change based on the number of times that the plant enters the LCO and the associated repair times. Currently, such information is not easily available, and they are not used. RG 1.177 therefore implements different quantitative risk criteria but consistent with RG 1.174.

TS components are generally safety related and are modeled in an internal-event PRA with an appropriate level of detail (to some extent in external event PRA, also). Bounding and screening analysis could also be used to account for risk contribution from external events (PRA scope for the application is all hazards). Further control measures for external event risk are generally set by the risk managed actions (RMAs) and the associated risk managed action times (RMAT[5]). For example, the status of offsite power and weather conditions (e.g., the possibility of a hurricane) are considered when LCO related to an emergency diesel generator is entered.

Risk-informed completion time (RICT) for I&C systems is generally used for reactor trip system (RTS) and engineered safety feature actuation system (ESFAS).

A mapping of the number of ways a reactor trip or ESF actuation can occur for each of the postulated plant accidents is identified in Chapter 15 of the final safety analysis report (FSAR). This information is used to determine the level of redundancy in RTS and ESFAS for each accident initiator. For example for steam generator tube rupture (SGTR), the reactor trip and ESF actuation can occur due to low pressurizer pressure and overtemperature ΔT. Chapter 7 of the FSAR should then be consulted on level of redundancy; for example, for overtemperature ΔT, coincident logic of 2 out of 3 would be required to actuate ESFAS. It should also be noted that manual actions (for reactor trip and ESFAS) can be credited in many of the initiators. The redundant signals are generally diverse (e.g., overtemperature ΔT and low pressurizer pressure) with no intra connections between different signal channels.

The RTS/ESF channels are designed with sufficient redundancy such that individual channel calibration and testing can be performed during power operation. In most cases, when a channel undergoes calibration/surveillance, it may be set in a bypass or a trip mode. Placing a channel in trip mode will improve system reliability but could slightly increase the probability of spurious actuation. When a channel is set to trip mode due to LCOs, a two-out-of-three channel trip success criteria becomes a one-out-of-two channel trip success criteria. When channel testing and calibration occurs during an LCO, the possibility of a spurious trip could increase. The ability of in-service testability without causing undue risk (maintaining redundancy and avoiding spurious actuations) is also examined.

[5] See Appendix C for treatment of external event risk and further information on RMAs.

Individual RTS instrumentation channels input to the automatic RTS functions will be evaluated using a bounding method as permitted by NEI 06-09, “Industry Guidance for Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS)” [Ref. 34]. The NEI 06-09 approach for determining RICT is justified due to built-in redundancy and diversity in RTS/ESFAS. Other methods and approaches however should be used to support Tier 2 needs for RMAs and Tier 3 for configuration control (RICT values based on plant-specific configuration at the time of LCO). Conservative approaches are generally used to address Tier 2 and 3 needs.

Treating all I&C components/modules the same as a channel may not be appropriate. A generic channel defined this way will not differentiate between a sensor (instrumentation), signal conditioning circuit, logic channel, and most probably a relay-based actuator (coil). Each of these modules has different failure rates and should not be treated as a logic channel. It is also possible that components such as relays and associated coils have a much higher CCF contribution. Finally, for external events such as fire, when the redundancy in I&C systems could be significantly affected, the impact of RICT may require additional consideration.

4.2.2 AI&C/DI&C PRA Challenges to Support RG 1.177

RG 1.177 allows the use of generic PRA models that were developed for all US vendors (GE, W, CE, and B&W) in NUREG/CR-5500, “Reliability Study: Westinghouse Reactor Protection System, 1984-1995” [Ref. 35]. In other cases, bounding approaches with the use of a surrogate model (such as representing a channel with a single sensor) is used. The RPS PRA model suitable for risk-informed TS should explicitly model RPS failures in response to each specific initiator, e.g., RPS failure in response to overcooling transients, RPS failure to SGTR, RPS failure to turbine trip. The same is true for the ESFAS system. The ESFAS system actuates several different safety systems in response to an accident scenario. An appropriate PRA should model RTS and ESFAS as a support to each initiator and accident class like other PRA support systems.

The equivalent RPS and ESFAS for new reactors and next generation reactors appear to perform additional functions such as providing information for operator display units. The use of software in DI&C facilitates integrating many functions into one system.

The use of conservative approaches such as the surrogate method are also accepted for RG 1.177. Surrogate PRA models are developed based on plant specific information and they can address the risk impact of I&C equipment. Plant specific PRA models however are needed to further decompose the AI&C/DI&C systems and components and to remove conservatisms. The following PRA requirements are specific to the application of RG 1.177 for current and future reactors as it relates to AI&C/DI&C systems. The existing guidance documents related to these PRA requirements should be expanded to address the following concerns more specifically.

Functional vs. Physical System

In some cases, a single I&C system with a defined physical boundary integrates the control/actuations of many other systems in response to a set of accident conditions. Failure to actuate or spuriously actuate one of these systems could uniquely impact the accident progression and can change the risk results. For example, the scram logic software integrates the scram functions for many different physical conditions (e.g., failure to scram due to SGTR, and failure to scram due to loss of flow, etc.). The importance of the overall I&C systems is calculated based on the aggregate risk impact of the failure of each of these systems (either due to lack of actuation or spurious actuation). To estimate this aggregate impact on risk from the overall I&C system, the physical functions performed by I&C systems, including software, should be decomposed to the individual system it actuates. This is a general practice in PRA modeling for evaluating the risk impact of a system that can affect several systems. For example, PRA models the electrical systems or component cooling water systems in the same manner. These are generally referred to as methods for support system modeling, which sometimes require the development of a dependency matrix. The modeling of I&C systems, like a support system, explicitly allows the integration of I&C models into PRA. This would support the development of PRA insights in line with the defense-in-depth concept and provides context to software failure and the associated data and models. Standard PRA methodology and associated tools are fully capable of accounting for overlapping failure mechanisms of the I&C system model when decomposed to contributions for individual supported systems. I&C systems also could be considered as providing supporting information for operator actions. Modeling the I&C system as a support system will also help in modeling appropriate HRA events accounting for the available I&C system in an accident sequence.

PRA Level of Detail

The level of PRA detail for supporting an application ideally should be consistent with the level at which the risk-informed changes are applied. RICT is usually applied at the level of testable module or a major component. This would correspond to the PRA level of detail at the modular level for the AI&C/DI&C system. RICT would impact the unavailability of components and systems by allowing extended maintenance downtime. There are many challenges in modeling the unavailability contributions of the AI&C/DI&C systems due to online diagnostics, fault tolerance, and periodic testing. These features do not contribute to unavailability and in fact they can reduce it. They can detect system faults, therefore facilitating repair and recovery (i.e., reducing downtime and the unavailability). These features need to be addressed in PRA. It should also be noted that some faults are transient and are generally resolved when the system restarts. The duration of downtime for such cases is short and may not challenge the RICT. Generally, the faults that are detectable using defensive measures and early diagnostics could be resolved in a short period of time and do not challenge CT extension through RICT. RICT therefore would be needed for system upgrades, either preplanned or corrective, and major module repair and replacement.

PRA Scope

The application of RICT generally address CDF and LERF for an internal event. The external events are generally treated in a bounding manner. However, the PRA requires the tools and models that can support Tier 2 activities, which include configuration risk management (CRM) and RMAs. This may increase the required scope of the PRA to include other initiators such as fire and flood. The possibility that fire and flood could potentially damage I&C equipment and their support systems is plausible. Failures and the unavailability of I&C systems can also impact operator actions, which could depend on the specific initiator and associated scenarios (e.g., some fire scenarios). In summary, the PRA scope for the current application in operating reactors is considered limited. This may not hold (should be examined) for new reactors.

Other insights and challenges identified in Section 3 for PRA modeling of AI&C and DI&C would also apply to PRA modeling for RG 1.177.

4.3 Summary of RG 1.201

RG 1.201 allows licensees to use a risk-informed process for categorizing SSCs according to their safety significance. SSCs of low safety significance can be removed from the scope of certain identified special treatment requirements.

This RG describes a method that the NRC staff considers acceptable for use in complying with the Commission's requirements in 10 CFR 50.69 with respect to the categorization of SSCs that are considered in risk-informing special treatment requirements. This categorization method uses the process that the Nuclear Energy Institute (NEI) described in Revision 0 of its guidance document NEI 00-04, "10 CFR 50.69 SSC Categorization Guideline" [Ref. 36]. This process determines the safety significance of SSCs and categorizes them into one of four risk-informed safety class (RISC) categories. The provisions of 10 CFR 50.69 allow for the adjustment of the scope of SSCs subject to special treatment requirements (e.g., quality assurance, testing, inspection, condition monitoring, assessment, reporting requirements, and evaluation) based on an integrated and systematic risk-informed process that is discussed in RG 1.201.

The safety significance of SSCs is determined using an integrated decision-making process, which incorporates both risk and traditional engineering insights. The safety functions of SSCs include both the design-basis functions[6] (derived from the safety-related definition) and functions credited for preventing and/or mitigating severe accidents. This results in SSCs being grouped into one of the four categories, as represented by the four boxes in Figure 4-2.

There are two types of functions performed by categorized SSCs, functions required for design-basis (DB) accidents, such as those considered in FSAR Chapter 15 for accident analysis, and PRA-based (PB) accidents, such as all mitigation capabilities accounted for in PRAs. Category 1 SSCs perform a function in DB space and are also risk significant for PB function. Category 2, by design, should not play any role in support of DB accidents but they should be important (risk significant) for PB function. Category 3 is important for DB but not risk significant for PB function. Finally, Category 4 SSCs are neither important for DB nor risk significant for PB function.

The requirements for SSCs in Category 1 are not relaxed. RISC-4 category equipment is not significantly relied on during severe accidents[7]. There is no alternative or special treatment required for RISC-4 category equipment.

[6] As described in FSAR Chapter 15 for current reactors.

[7] Low risk significance generally occurs during PB events when there are many ways to mitigate an accident including a success path, which involves the equipment of interest (mitigation redundancy and diversity is greater than 2) or it could be because the equipment of interest is rarely needed (low frequency of demand, low likelihood of initiator followed by the failure of a low-probability event such as a passive component failure).

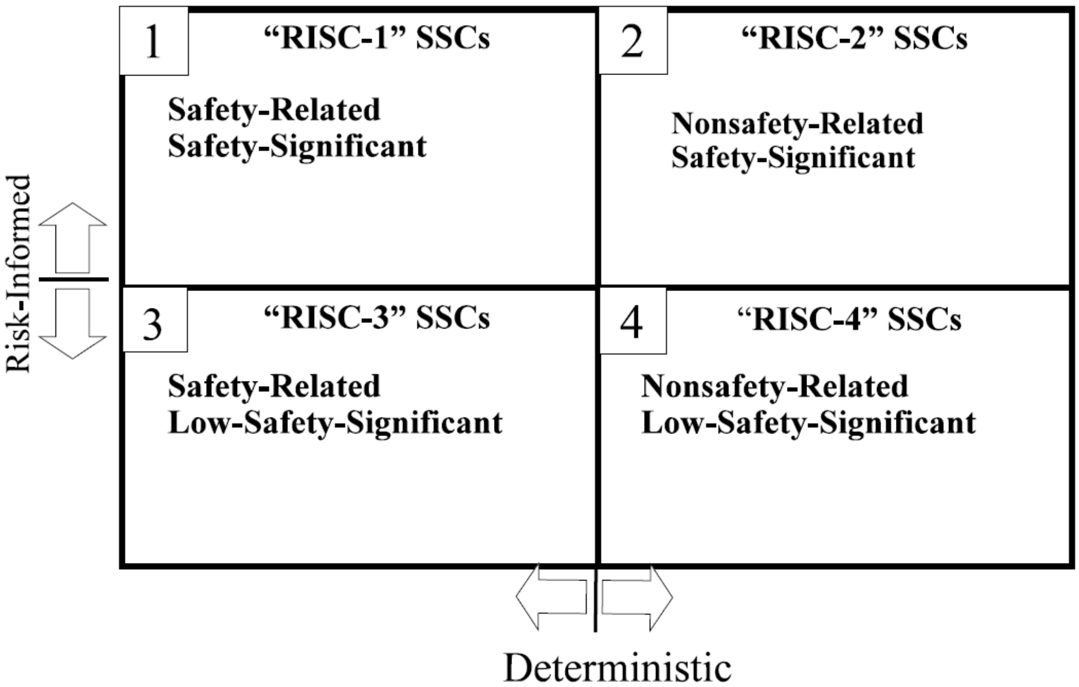


Figure 4-2 Risk-Informed Safety Class (RISC) Categorization (duplicated from RG 1.201)

Alternative requirements for Category 3 SSCs, as stated in 10 CFR 50.69, should ensure, with reasonable confidence, that the SSCs remain capable of performing their safety-related functions under DB conditions, including seismic conditions and environmental conditions and effects throughout their service life.

Alternative requirements for Category 2 SSCs, as stated in 10 CFR 50.69, should ensure that the SSCs perform their functions consistent with the categorization process assumptions by evaluating treatment being applied to these SSCs to ensure that it supports the key assumptions in the categorization process that relate to their assumed performance.
The categorization process would involve several steps. The first step in the process is the initial engineering evaluation of a selected system to support the categorization process. This includes the definition of the system boundary to be used and the components to be evaluated, the identification of system functions, and a coarse mapping of components to functions. The systems functions are identified from a variety of sources, including design/licensing basis analyses, Maintenance Rule assessments, and PRA analyses. The mapping of components is performed to allow the correlation of PRA basic events to system functions.

The second step in the process is to use the PRA to differentiate between the high- versus low-safety significance (HSS and LSS) SSCs. This is currently done using importance measures such as Fussell Vesely (FV) and Risk Achievement Worth (RAW). The PRA-designated HSS components will be categorized as RISC-1 or RISC-2, depending on whether they play any role in DB events.

In the third step, the PRA-designated LSS components will be assigned to RISC-3 and RISC-4, depending on their function during DB.

Finally, in the fourth step, the qualitative deterministic considerations are used to ensure that the PRA assignment of LSS does not contradict with the deterministic regulatory criteria. This is accomplished by three different means: (1) the examination of defense-in-depth (DID), (2) risk sensitivity studies (RSS) and (3) the Integrated Decision-making Panel (IDP).

The current state of practice for PRAs will only explicitly[8] cover a subset of SSCs and a subset of the functions they perform. Some examples of SSCs that are not explicitly modeled are (1) alarms and indications that support the operator actions during an accident and within Emergency Operating Procedures (EOP), and (2) Systems/subsystems modeled as a super component. In the latter case, when a subsystem is modeled as a super component, all its parts are generally assumed to have the same risk significance. For example, some functions, such as the fill and drain functions of an HSS, may be grouped as LSS since they do not support the critical function of that HSS system. These PRA shortcomings are typically compensated by IDP examination. Engineering and qualitative evaluation also classify additional SSCs to supplement the PRA limitations using the three steps (DID, RSS, and IDP) discussed earlier. The qualitative evaluation could identify new HSS components or changing the PRA designated LSS SSCs to HSS.

Defense-in-depth addresses the role of components in preserving DID related to core damage, large early release and long-term containment integrity. The RSS is performed to examine the range of the aggregate impact of changing the treatment of low safety-significant SSCs (mainly RISC-3). The last step of categorization is performed by the IDP. The IDP is a multi-disciplined team that reviews the information developed by the categorization team. The IDP uses the information and insights developed in the preliminary categorization process and combines that with other information from DB and DID assessments to finalize the categorization of functions.

4.3.1 Lessons from Application of RG 1.201

RG 1.201 is a document that can be used for risk-informed SSC classification for any plant design and for any system including DI&C systems. RG 1.201 clearly prescribes a process for risk-informed SSC classification that can be followed by applicants. However, there are some observations and lessons identified from reviews of risk-informed SSC classification in other industries, as well as the nuclear industry, that may be considered for their applicability. These observations are discussed here.

Changes in the component reliability/failure probability due to changes of its SSC classification is not well known (i.e., very uncertain). Estimating the change in plant risk as a result of risk-informed SSC classification as prescribed by RG 1.174, therefore, cannot be viable. RG 1.201 utilizes risk importance measures as the risk insight to be used for risk prioritization in support of classifying the SSCs. RG 1.201 relies on the explicit calculation of importance measures from PRAs. The PRA scope and level of detail limits the number of equipment that could be explicitly evaluated as discussed earlier. As a result, RG 1.201 also relies on qualitative engineering analysis (DID, RSS, and IDP) to classify the components.

The importance measures and the associated criteria used in RG 1.201 were used previously for other applications (e.g., maintenance rule) dealing with conventional electrical and

[8] "Explicit" refers to an element in PRA such as a basic event or an initiator for which risk importance measures can be automatically calculated without any PRA manipulation. There are many additional implicit considerations in PRAs for which the determination of risk importance measures may require PRA manipulation.

mechanical components. FV and RAW importance measures are used. These importance measures are formulated and discussed in Appendix C of this report. The FV measure is directly related to the nominal contribution of the SSC failure to the top-level risk metrics. The higher the contribution, i.e., FV measure, the more important the SSC would be. The RAW importance measure, however, relates to the change in risk if the SSC is unavailable. These importance measures have not yet been used for DI&C systems. Failure of a DI&C system could impact several functions and it generally has much higher reliability than a conventional mechanical and electrical system. The use of importance measures for DI&C systems should be re-examined to ensure that they are appropriate. The use of RAW threshold for DI&C systems and components is discussed in Appendix C. It is shown that the RAW thresholds could depend on the SSC reliability and may need to be adjusted for DI&C systems. Specific thresholds for RAW values should be tested for DI&C system failures including CCF of software or hardware.

RG 1.201 covers all safety and non-safety systems. This differentiation is important when determining the scope of the study and for considering I&C systems (i.e., it is not limited to RTS and ESFAS). A PRA supporting RG 1.201 to the extent possible should include front-line, support and backup systems regardless of whether they are safety related. Including these additional I&C systems to a PRA model would significantly increase the size and the scope of the PRA. The unnecessary increase in scope should be avoided, and the PRA size should be managed properly with appropriate screening criteria and evaluation including well-documented engineering and qualitative safety discussions. The level of detail in PRA modeling should also be commensurate with the importance of the modules evaluated through well-defined screening studies. Similar practices, such as the use of HAZOP analysis for identifying (screening) the critical systems for PRA modeling and risk-informed applications, are used by other industries (see Section 2).

The IDP decisions and the qualitative criteria in SSC categorization play important roles in SSC classification. IDP has identified a large fraction of HSS components[9] for some applications, since the current PRAs may not have sufficient scope and level of detail. An appropriate level of detail could be achieved without significantly affecting the size of PRA models by using efficient PRA prioritization and screening. There are many components that are modeled in PRA as super components. For example, some support functions for the emergency diesel generator, including I&C components, could have been modeled as a super component. The IDP is responsible for breaking down a super component into its individual components (including the associate I&C) for the purpose of SSC classification. Balancing the PRA level of detail with the needs of SSC classification in a practical manner is a challenging task for all systems, including I&C systems.

Another important area for IDP review is the classification of passive components. The failure of passive components not only degrades the system, but if not isolated, can be a source of flooding. The failure of some passive components is self-revealing. For example, the plant could be equipped with a flow and pressure alarm when a pipe breaks. When the failure of a passive component is self-revealing, its unavailability contributions may be insignificant. In some cases, the failure of passive components could result in an internal events flood initiator. I&C systems can provide early warning, such as alarms and indicators, that help the operators detect external events (e.g., fire, flood), in addition to performing an isolation function. The possible use of flooding PRA, the use of risk insights from risk-informed in-service testing and in-service inspection (IST/ISI), and focused sensitivity analyses could be beneficial for passive system

[9] NEI presentation during industry and NEI/NRC meeting on “NEI Lessons-Learned Workshop,” Washington DC, Jan 30-31, 2019.

prioritization. There is currently no guidance regarding the use of external event PRAs for passive components and I&C systems.

The IDPs also classify I&C systems. If the I&C system supports at least one HSS SSC, it could be categorized as HSS[10]. More detailed modeling of I&C systems, which are decomposed to different functions, can better support the IDP evaluation.

4.3.1 AI&C/DI&C PRA Challenges to Support RG 1.201

The PRA of AI&C/DI&C systems supporting RG 1.201 must meet certain requirements and overcome some challenges. These are summarized in this section.

1. Level of Detail: RISC classification of the AI&C/DI&C systems is intended to arrive at a set of programs that are designed to ensure system reliability consistent with the risk significance of the SSCs. The program requirements for RISC-1 through RISC-4 classifications are generally defined for module, channels, trains, and systems. The PRA does not need to be developed at a component level (microprocessor, memory, shift register, etc.). This creates opportunity as well as unique challenges for data collection, which is described next. As far as software is concerned, its model should address (i.e., be decomposed to) the different functions it performs. The overall software failure rate estimates should be split into those instantaneously detectable, those detectable during periodic testing, and those not detectable (see Section 3.3 for a detailed discussion). This again creates a challenge for data evaluation. Also, as discussed in Section 5, the data analyses should categorize the software and hardware failures in several general categories to support CCF evaluation. In some DI&C systems, which are dedicated to one function (such as ventilation control), the software does not have to be broken down to a lower level. In other software performing several functions at several different systems (fully integrated, such as ESFAS), the software model should be decomposed to each of the functions with consideration for the overlapping portion of the software among the supported systems.
2. Data Challenge: The data needs for RG 1.201 should be consistent with the level of detail needed for the associated PRA. Data sources, such as the manufacturer data or RIAC database of 217 plus [Ref. 19], are more detailed than the modeling needs for RG 1.201. The evaluation of operational data, from sources such as GIDEP and EPIX, appears instead to be more promising. The raw data is preferable to analyzed data since the estimates must be categorized to failure types for the unavailability evaluation (e.g., Types A, B, and C as discussed earlier) and CCF evaluation (e.g., coding error, inadequate requirements, interaction between hardware and software, etc.). CCF due to coding errors can be defended against with MVDS techniques. CCF due to coding errors and interactions between hardware and software could be defended against using different technologies such as FPGA versus microprocessors (See discussion in Section 5).
3. Scope Challenge: A PRA to support RG 1.201 should include many front-line, support, and backup systems, including their associated AI&C/DI&C systems. A PRA of such a large scope should be managed properly by appropriate screening criteria and detailed

[10] I&C system or portion of that can support several SSCs, if any of those SSCs is classified as HSS, then that portion of I&C would be considered HSS.

documentation. The PRA modeling detail should be commensurate with the importance of the modules and inclusion in the PRA based on well-defined screening criteria.

4. Use of RAW for CCF of I&C Software and Hardware: Following the discussion on data challenges and the level of detail and the scope, one should differentiate among CCF contributions for each function and for all of the functions performed by the I&C system. Use of the RAW importance measure and its threshold for unavailability contributions of CCFs that are detectable during periodic testing should consider the discussion provided in Appendix C, Section C.2.3.

5. Modeling of Unavailability and Failure Probabilities: Both unavailability and failure probabilities must be modeled for the DI&C PRA. The proper differentiation should be made between unavailability sources and failure probabilities, as discussed in this report. Design features, such as a self-diagnostics capability, allow for rapid replacement of failed devices and reduce the unavailability contribution. Therefore they must be modeled in the PRA.

6. Hazard and Initiators: I&C systems can provide alarms and indicators that help the operators detect plant initiators, especially during internal fires and floods. This is in addition to standard modeling of I&C systems to support major plant safety and support functions. Also, some hazards, such as internal fires and floods as well as external initiating events, could trigger the CCF mechanism for I&C systems. High-energy arcing may also cause CCF of DI&C systems either directly or remotely via EMI/RFI. The availability of a full-scope PRA (internal and external initiators) and the inclusion of I&C systems can reduce the role of the IDP for SSC classification.

7. Human Reliability Analysis: Other important aspects of I&C PRA for SSC classification deal with human system interface. In a digital plan, the information is presented to the operators using digital technology, procedures are computerized, and operator commands are entered into computers and transmitted to the systems (soft versus hard command). Operator interactions would be different with possibly different human error probabilities. In addition, when a DI&C system fails, the operator may have to use manual diverse backup systems and rely on written procedures to perform the necessary actions. PRAs for AI&C and DI&C should consider a revised HRA.

8. Threshold Criteria for Importance Measures: The threshold criteria for advanced reactors with enhanced DI&C systems and passive systems should be piloted to arrive at revised and more meaningful criteria. Developing a PRA test bed for DI&C is needed.

9. Sensitivity and Uncertainty Analysis: The robustness of the risk-informed decisions depends on identifying the major sources of variations and uncertainties. The identification and the evaluation of the impact of these uncertainty sources should be piloted in a DI&C PRA model for an advanced reactor. This requires developing a PRA test bed for DI&C systems.

10. Communication Links and Network System: The failure of communication links and network cables have the potential to contribute to the failure of the digital system due to CCF[11]. Data evaluation focused on communication links and communication units would be needed.

[11] The potential failures of communication links and means for detection is discussed in several places in the report, Specific concerns regarding CCF as a result of harsh environment and fires are highlighted in Appendix C and Item 9 in Section 5 of the main report.

4.4 <u>Summary of RG 1.205</u>

Regulatory Guide 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants,” provides guidance for fire protection programs that meet the requirements of 10 CFR 50.48(c), “*National Fire Protection Association [NFPA] Standard NFPA 805*.”

Prior to the promulgation of 10 CFR 50.48(c), plants typically adopted a standard fire protection license condition. Under this condition, the licensee could only make changes to the approved Fire Protection Program (FPP), without prior Commission approval, if the changes did not adversely affect the plant’s ability to achieve and maintain safe shutdown in the event of a fire. For licensees choosing to adopt NFPA 805, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” under 10 CFR 50.48(c), a set of risk criteria is defined as the basis for making changes to the approved NFPA 805 FPP without prior NRC approval. The criteria (deterministic and risk-informed) duplicated from RG 1.205 are listed below:

a. Prior NRC review and approval is not required for a change that results in a net decrease in risk for both CDF and LERF. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. The change may be implemented following completion of the change evaluation.
b. Prior NRC review and approval is not required if the change results in a net calculated risk increase less than <1E-7/yr for CDF and less than <1E-8/yr for LERF. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. The change may be implemented following the completion of the change evaluation. Change reports need not be submitted to the NRC for these changes.
c. Where the calculated plant change risk increase is <1E-6/yr, but >1E-7/yr for CDF or <1E-7/yr, but >1E-8/yr for LERF, the licensee must submit a summary description of the change to the NRC following completion of the change evaluation. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. If the NRC does not object to the change within 90 days, the licensee may proceed with implementation of the proposed change.

The Nuclear Energy Institute (NEI) has developed NEI 04-02, “Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)” [Ref. 37] to assist licensees in adopting 10 CFR 50.48(c) and making the transition from their current fire protection program to one based on NFPA 805.

The steps for performing a fire PRA that satisfies NFPA 805 [Ref. 38] criteria are provided in NUREG/CR-6850, “EPRI/NC-RES Fire PRA Methodology for Nuclear Power Facilities” [Ref. 39]. The appendices to this report provide an extensive review of the experimental database existing at that time underlying the various steps of the PRA procedure. Since that time, additional fire research has been performed by the NRC and EPRI to enhance the methodology and data in NUREG/CR-6850. The major areas of enhancement were cable fire heat release rates, target damage criteria, and circuit failure analysis. An extensive study was performed under the sponsorship of NRC and EPRI of the status of “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” NUREG-1824 [Ref. 40], in which a set of fire scenarios are established and comparisons made among the NRC’s Fire Dynamics Tool (FDT), EPRI’s FIVE model, NIST’s CFAST zonal model, EdFs MAGIC code and NIST’s Fire Dynamics Simulator (FDS). The information generated from the multi-volume NUREG-1824 was summarized in NUREG-1934, “Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG)” [Ref. 41]. This document also includes eight example fire scenarios and evaluates them using the five different codes (FDT, FIVE, CFAST, Magic and FDS) addressed by NUREG-1824. The report provides a consistent implementation guide. Additional enhancement in the estimates of fire ignition frequencies for reducing fire PRA conservatism is currently being studied by EPRI and the nuclear industry.

RG 1.205 provides a risk-informed justification for licensee amendment of proposed changes to the fire protection program. The specific area of the fire protection requirements that could benefit from risk-informed approaches are Section IIIG on safe shutdown capability, IIIF on automatic detection, and IIID on manual suppression.

Fire events can affect instrumentation in many ways that could result in inaccurate measurements and erroneous indicator readings. As discussed in NUREG/CR-6850, there is generally a limited set of instrumentation and diagnostic equipment such as indicators, lights, alarms, and similar devices considered necessary to support successful operator actions (e.g., such as carrying out the emergency operating procedures [EOPs]). The impact of fire on indicators and alarms could-vary the probability of success for required manual actions in specific Fire Emergency Procedures (FEPs), or to credit certain recovery actions. NUREG/CR-6850 considers these issues in a deterministic and qualitative manner (assuring a minimum set of indicators and alarms are not affected by fire). NUREG/CR-6850 also considers those I&C systems whose failure could cause inappropriate operator actions (act of commission). These limited I&C systems should then be included in a component list for cable tracing. Examples could be the equipment and controls in a remote shutdown panel (or areas), pump room high-temperature alarms, certain plant parameter indicators when reduced redundancy can result from a fire scenario. The identification and tracking of relevant I&C cables are generally mandatory but their inclusion in the fire PRA model is not required.

The fire-induced damage to instrumentation and alarms is specific to each fire area. The fire PRA documents the remaining instrumentation and equipment in each area and justifies their adequacy for supporting operator decisions, with some considerations for cases where conflicting indications may occur. Spurious alarms requiring direct operator response should also be considered separately, to ensure that no additional operator actions could occur due to spurious alarms. NUREG-1921, “EPRI/NRC-RES Fire Human Reliability Analysis Guidelines” [Ref. 42], provides guidance on human reliability analysis during fire, which indirectly addresses some of the issues related to modeling I&C equipment during a fire event. All these considerations are performed deterministically and qualitatively. The~~se~~ considerations are implicitly included in estimating the human failure probability calculations. There is no explicit account of these activities in PRA models and the quantification of scenarios. This distinction is important since if an indicator credited in the fire PRA is not available, the human error probability must be completely re-evaluated and the PRA model re-quantified to estimate the conditional CDF.

4.4.1 Lessons Learned from RG 1.205/NFPA 805

The NRC and nuclear industry have spent significant resources in supporting fire PRAs. As a result, guidance documents for the various PRA elements in NUREG/CR-6850 to support RG 1.205 and NFPA 805 are prescriptive. This could be considered contrary to the original objective of developing a performance-based fire safety program, which was shifting away from the prescriptive requirements. In addition, some level of conservatism has permeated throughout the fire PRA guide to ensure its use for regulatory purposes. One such conservatism was eliminating the concept of severity factor in developing the frequency of meaningful fires in NUREG/CR-6850. NFPA 805 fire PRAs are also resource intensive, indebted to not using the risk screening and experience to focus on important issues. Extensive circuit analysis in search of risk-significant spurious actuations is a good example of an inefficient process. This is done as an engineering exercise to support the regulatory requirements regardless of the risk importance of the spurious actuations of interest. There are other issues such as inconsistency between ignition source heat release rate with the ignition source frequency. Sophisticated uncertainty analysis is performed as a part of the NFPA 805 PRA. Uncertainty analysis may not be as informative when estimates are contaminated with bias (conservatisms). In some cases, the degree of bias (conservatism) is explicitly shown on the estimates (as it is done for some of the fire codes, such as FDS).

Enhanced methods and data are being developed to address many of these challenges and issues, specifically in reducing the conservatisms, by both NRC and industry. In the next section the focus will be on those challenges specific to AI&C/DI&C modeling.

4.4.2 AI&C/DI&C PRA Challenges to Support RG 1.205/NFPA 805

The PRA models developed for NFPA-805 applications do not model I&C systems. NFPA-805 requires that the available instrumentation, indicators, and alarms that operators rely on at each specific fire area be documented.

It is generally assumed that the contribution of I&C failures to CDF and LERF during a fire scenario is small if there is one train and a diverse manual actuation available. Spurious alarms requiring direct operator response are also considered qualitatively in fire PRA and indirectly for human reliability analysis. Current practices generally assure that the failure of I&C is not a significant contributor to fire-induced CDF/LERF for dominant accident sequences. The impact of not modeling I&C systems for non-dominant sequences is not clear. For dominant sequences, the conditional core damage probabilities in fire scenarios are generally around 1.0E-2, whereas the failure probability of I&C systems consisting of one train plus diverse manual initiation is generally around 1.0E-3. For non-dominant sequences, the conditional core damage probability is ~<1.0E-3, therefore the contribution of I&C may not be negligible. The following insights and challenges for modeling I&C systems responsive to the needs of RG 1.205 applications are as follows:

1. Effect of I&C System on Non-Dominant Accident Scenarios: There is a concern that non-dominant accident scenarios could contribute more to the plant risk metrics if a fire affects the I&C systems resulting in higher human error failure probabilities either due to the loss of indication or occurrence of spurious indications and actuations. Developing detailed I&C models during thousands of fire scenarios is resource intensive. PRA-based screening criteria should be first developed to identify the scenarios for which more focused I&C modeling may be needed.
2. Human Error Probability: Fire scenarios could result in failure of instrumentation, instrumentation channels, and component status. These effects could reduce the information available for operator actions, depending on the accident scenario (context-based). Missing, confusing information, spurious alarms, and wrong indications could significantly increase the human cognition of the accident condition. More formal and explicit treatment of human failure probabilities could become necessary in some cases.
3. Spurious Actuation and Partial CCF: AI&C/DI&C are highly redundant and segregated systems. The potential of CCF of all modules of I&C systems due to harsh fire

environments, including smoke, are not highly likely. One or more fire scenarios could impact some of the redundant trains, making the remaining trains more important. For example, there could be three trains of I&C systems: A, B, and C. The majority of the fire scenarios could affect Trains A and C. This makes Train B more important as the only remaining redundancy for these fire scenarios. To ensure the reliability and availability of that I&C train, it should be included in the plant Reliability Assurance Program (RAP).

Fire PRA modeling of AI&C/DI&C may bring additional challenges due to the response of DI&C to possible fire scenarios. The level of conservatism and its role in evaluating uncertainties and estimating the mean value of CDF/LERF is currently under study.

4.5 Summary of RG 1.200

This regulatory guide describes one acceptable approach for determining whether the technical adequacy of the PRA, in total or the parts that are used to support an application, is sufficient to provide confidence in the results, such that the PRA can be used in regulatory decision-making for LWRs.

RG 1.200 utilizes the ASME/ANS PRA, “Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” (currently ASME/ANS-RA-Sa-2009) [Ref. 43], as one acceptable approach for determining the technical adequacy of the PRA via peer review. The primary result of a peer review is to generate the findings and observations (F&Os) recorded by the peer review and the subsequent resolution of these F&Os. Peer reviews are also needed each time a major PRA upgrade has been performed, which may include (1) use of new methodology, (2) change in scope that impacts the significant accident sequences (or the significant accident progression sequences), and (3) change in capability that impacts the significant accident sequences or the significant accident progression sequences. The NRC staff will review the PRA and the status of F&O closures as a part of the review of application-specific, risk-informed submittals. Several of these reviews and the associate requests for additional information (RAIs) were examined to better understand the relation of RG 1.200 with the ASME/ANS PRA standard, application-specific reviews, and the peer review process.

A summary of technical attributes for a Level 1 PRA for internal events is listed in Table 2 of RG 1.200. There is no specific mention of I&C systems in Table 2, although it could be argued that it is implicitly accounted for by other attributes. The first place that instrumentation is explicitly mentioned is as part of equipment selection for performing fire PRA.

Tables A-1 through A-10 of Appendix A of RG 1.200 provide the staff’s position on each requirement in Parts 1 through 10 of the ASME/ANS RA-Sa-2009 PRA standard, respectively. The ASME/ANS PRA standard, however, has some discussion on documenting required information for spurious actuation and/or spurious alarms during fire PRA and their effect on operator acts of commission. For example, if a high-temperature alarm is spuriously induced by fire for a running pump, the operator is expected to shut down the pump. In such a case, the PRA fire models should not credit the pump. The possible recovery of the pump however may be credited using a revised human error probability. It is assumed that RG 1.200 will support those limited instructions in the ASME/ANS PRA standard.

Considerations for PRA modeling for DI&C system are discussed as a part of SRP Chapter 19 (See Section 3 of this report). As noted, SRP Chapter 19 lists several areas that the NRC staff considers important. These areas are expected to be reviewed by NRC staff for DI&C systems.

The SRP does not indicate how and at what level of detail these reviews should be. Some coordination between RG 1.200 and SRP Chapter 19 would be useful.

4.5.1 Lessons Learned from RG 1.200

RG 1.200 attempts to establish the scope and attributes of PRAs needed to address risk-informed applications. This is done generically and independent of the specific needs of each application. It focuses on CDF and LERF, which is consistent with the current risk-informed regulatory framework. RG 1.200 is supported by the ASME/ANS PRA standard, which is also a high-level document that provides specific high-level requirements (HLR) and supporting requirements (SRs) for various elements of PRAs. Its scope includes internal events plus fire and flood, although the emphasis so far has been on internal events. RG 1.200 and the ASME/ANS standard are supported by a series of technical documents that provide detailed instructions (lower-level documents) of how the PRA for each application should be performed.

A combination of RG 1.200, the ASME/ANS standard, and a peer review process [Ref. 44] is an effective and efficient approach for identifying weaknesses in PRAs. The F&Os generated through peer reviews identify specific aspects of the PRA that may need revision. F&Os provide the primary basis for PRA conformance with the state-of-the-practice, areas for focused review, and PRA updates. RG 1.200 and the process of review are based on the state-of-the-PRA practice. It cannot be used for new methods, i.e., PRA methods that are state-of-the-art and beyond. These guides should be updated as PRA methods are enhanced and applied sufficiently to be considered a state-of-the-practice. For example, there is a limited discussion within RG 1.200 about the PRA modeling of I&C systems. RG 1.200 mainly relies on ASME/ANS PRA standard. The consideration of I&C systems in the ASME/ANS PRA standard is generally discussed as support to HRA estimates, recovery actions, or the availability of support systems. Inclusion in the PRA models is generally discussed in an implicit manner. Explicit requirements for PRA modeling of I&C systems as a standalone subject is not currently included in the ASME/ANS PRA standard. This issue is discussed further below.

Parts 1 through 10 of the ASME/ANS PRA standard are written in the form of HLRs and SRs along with examples for specific consideration. One example set of the requirements (HLR, SR, and Example) is shown in Table 4-1 below.

Table 4-1 Illustration of HLR, SR, and Example from ANS/ASME PRA Standard

HLR-AS-B	Dependencies that can impact the ability of the mitigating systems to operate and function shall be addressed.
SR: AS-B; AS-B2:	IDENTIFY the dependence of modeled mitigating systems on the success or failure of preceding systems, functions, and human actions. INCLUDE the impact on accident progression, either in the accident sequence models or in the system models.
Example	*(a)* turbine-driven system dependency on stuck-open relief valve (SORV), depressurization, and containment heat removal (suppression pool cooling). *(b)* low-pressure system injection success dependent on the need for RPV depressurization.

The authors have concluded the following based on preliminary examination and review of the ANS/ASME PRA standard:

1. HLRs appear to be applicable to all systems and perhaps to all plant designs.

2. Some changes are envisioned for supporting requirements to address the required modeling of DI&C PRA more specifically. The SR for some PRA elements; especially Element 3 of the success criteria and Element 4 of the system analysis may be needed. For example, SR-SY-A9 [12]requires that super components be decomposed down to a level of detail when the specific failure mode and recovery action can be determined. Decomposing software to specific functions can be explicitly covered under this requirement. Please note that this was discussed as a PRA requirement for decomposing software earlier in Section 4.3.

3. The new example to highlight major considerations for DI&C PRA should be added to the ANS/ASME PRA standard.

Performing additional DI&C PRAs and PRA applications, including pilot studies, can help to update both RG 1.200 and the ASME/ANS PRA standard.

4.5.2 AI&C/DI&C PRA Challenges to Support RG 1.200 Updates

As noted in the previous section, RG 1.200 and associated documents have limited requirements for modeling I&C systems in PRAs. Requirements for modeling DI&C systems in PRAs for new reactors can be found in SRP Chapter 19. This document lists areas that the staff should review as part of the design certification document (DCD) or FSAR. The SRP does not indicate how and at what level of detail these reviews should be performed.

Updating RG 1.200 requirements to include AI&C/DI&C in the PRA consistent with SRP Chapter 19 is a major challenge that cannot be realized unless NRC and industry jointly develop PRA models for selected pilot plants and perform several risk-informed applications.

[12] The A9 supporting requirement (SR) for the PRA element system (SY).

5. IDENTIFICATION OF REQUIREMENTS FOR METHODS, MODELS, DATA, AND ANALYTICAL TOOLS

Section 4 discusses the state-of-practice for incorporating risk insights within the existing risk-informed regulatory framework for DI&C systems. It concludes that the current NRC regulatory framework sufficiently describes the risk-informing process and it is appropriate for applying risk insights from a DI&C PRA to support regulatory decisions. Section 4 also discusses some observations that could be considered in the future if the need for improving the NRC regulatory framework arises. Two sets of findings (observations) are discussed for each RG in Section 4. The first set of findings identifies possible areas of improvement in RGs for all systems. The second set of findings is specific to the use of the RG for I&C systems. A comprehensive discussion is provided on RG 1.201 as noted in our project objectives. One area that is noted as a part of this discussion relates to the use of PRA insights to help streamline and focus the qualitative/engineering reviews on more important SSCs. This would increase efficiency and facilitate a graded review of the first three qualitative/engineering principles of RG 1.174. Risk-informed prioritization methods can be used to support this objective. Other industries have used qualitative methods such as HAZOP analysis and quantitative sensitivity analyses using the base PRA. Similar approaches could be implemented for graded risk-informed reviews at NRC by prioritizing the SSCs. Quantitative methods using the PRA model without the I&C system combined with sensitivity analysis can provide an initial prioritization of the various systems. This process is similar to the risk-informed process for SSC classification. The SSC classification is discussed in detail in Section 4.3.

This report also concludes that there are some gaps in the current guidance documents, which need to be updated. The study found that the NRC's PRA guidance, as it exists today, may not generate the needed risk insights to completely support the NRC's regulatory framework for DI&C systems.

The discussions in Section 4 provide the basis for all required additional technical needs for risk informing DI&C systems at the NRC. All observations that could be considered for improving the NRC regulatory framework are discussed in Section 4. These observations are not repeated here. The main conclusion from Section 4 is to improve the efficiency of the review and acceptance process of risk-informed applications consistent with their risk significance. This is generally done by performing system classifications (RG 1.201) and tailoring the requirement and the extent of the review for acceptance based on the SSC class. The following items related to the SSC classification of DI&C systems may need additional re-examination:

1. Importance measures and their associated criteria.
2. The role of IDP.
3. PRA guide elaborating on DI&C PRA elements consistent with RG 1.200 and the ASME PRA standard.

Addressing the above issues could be considered the basis for performing a pilot application.

This section is devoted to identifying the requirements for PRA methods, models, data, or analytical tools that are needed for enhancing the use of PRA risk insights. All findings presented here are based on the results from the detailed examination of many documents as noted in Sections 2 through 4 and Appendices A through C.

1. Understanding DI&C System Functions and Failure Modes

I&C systems perform several functions. The failure of each function could have a different impact during plant operation and accident sequences. The DI&C system PRA notebook should describe each function separately. The impact of the failure of each function on plant operation and the mitigation of accidents should be expanded. At a minimum, two failure modes (1) the failure to respond, and (2) spurious actuations, should be discussed. The impact of the different failure modes on major operator actions including those in EOPs should be delineated.

2. Evaluating the Impact of DI&C System Failures

The failure effect of DI&C systems on system functions are often identified by the performance of failure modes and effects analyses (FMEA). The development of FMEAs sometimes requires various levels of engineering analysis and simulations (for example, see Ref. 20 by Chu and Yue). The FMEA should also consider possible software failure modes relating to their effects on each of the functions performed by the software.

Also, failure modes, causes, or effects often are intertwined or defined ambiguously, and sometimes overlap or are contradictory. Examine the applicant documentation to ensure that the most significant failure modes of the DI&C are documented with a description of the sequence of events (context) that need to take place to fail the system. The sequence of events should realistically represent the system's behavior at the level of detail in the model.

3. Integrating DI&C to Risk Model (Accident Sequence and Success Criteria)

The integration of DI&C functional failures into the risk model should be performed with a full understanding of the role of I&C in accident sequences. Specific locations in the event trees and the fault trees, where the functional failure modes are entered, should be clearly identified, and documented in the PRA system notebooks. A detailed description of the sequence of events (context) during the accident and its potential impact of the DI&C functional failure should be discussed/documented. DI&C system/function success criteria for each accident scenario should be specified, including the required response time, if relevant. Diverse systems and backup manual actions should also be documented. To avoid unnecessary modeling of DI&C functions, a set of qualitative and quantitative screening criteria should be specified. It is possible that some of the failures of I&C systems, such as spurious actuations, can result in a unique and new accident sequence. The necessary accident analysis studies commonly conducted for success criteria evaluation should be performed.

4. DI&C Functional Failure Probability Model

DI&C functional failure models should be consistent with the Steps 1 through 3 discussed above, especially FMEA models. In most cases, the fault tree models can satisfy this requirement. If the current fault tree models cannot meet the requirement, more advanced methods should be considered. The failure probability model (e.g., fault trees) should be developed in a hierarchical manner and in a traceable way. The hierarchical structure would allow the future extension of the models a more detailed level by replacing the super basic events with a transfer gate. The level of detail for each DI&C function that could satisfy the current NRC regulatory framework is shown below:

- Input module: sensors, signal conditioning, analog/digital (A/D) converter and multiplexer (MUX)

- Acquisition and processing units (APUs)
- Software for processing
- Voting logics
- Output modules; D/A converter and communication links
- Voting logics including associate software and hardware, if used
- Signal conditioning and actuators
- All I&C support functions, such as power and cooling

DI&C systems are equipped with fault tolerance features, self-checking systems, and other defensive mechanisms. These features should be modeled as well.

5. Hardware Reliability Estimates

To support the PRA quantification of the hardware associated with DI&C, estimates are required for the probability of failure for specific failure modes, estimated unavailability contributions and CCF probabilities (will be discussed separately). The generic estimates as well as estimates from available sources of experience data should be specified. The failure rate estimates should account for fault tolerance features, self-checking systems, and other defensive mechanisms. Detectable failures should be differentiated from undetectable failures [Ref. 45; NEA/CSNI/R (2014)]. The failure rate estimates should include the pedigree of the hardware and differentiate between different SSC classifications. Analytical methods and tools based on Bayes estimation techniques should be used to ensure that the uncertainties are properly captured.

6. Software Reliability Estimates

Software reliability should be estimated at the level of detail consistent with the specific function(s) for control and actuation of the supported systems. Software failure probability should account for the pedigree of the software. The failure rate for critical safety-related software, which has undergone strict requirements, safety-related quality assurance and quality control (QA/QC) programs, and comprehensive testing is expected to be different than non-safety-related software. This difference should be accounted for. The failure probability for the individual functions performed by software should also account for defensive mechanisms such as diagnostic and fault tolerance schemes and software complexity as measured by various parameters. Software failure probability for each function should also account for the environment and sequence of events within the accident (i.e., the context of demand). Software response time to a specific accident sequence (specific context), if it affects the software failure probability, should also be addressed. There are generally three contributors to software failures: design-based errors (an error in design requirements), coding errors, and configuration/updating errors (maintenance). The software failure should estimate the contribution of each of these three sources to overall software failure (also required for software CCF requirements). Generic sources of software reliability data should be identified and examined for their applicability to the specific DI&C systems. Operational data for software failures in similar DI&C systems may be used, however they must be justified for applicability. Uncertainty distributions for software failure rate may be established either through Bayes method or formal expert elicitation.

7. Human Reliability Analysis (HRA)

HRA models should account for the following three DI&C-specific impacts:

- The need for modified or new failure rates for human system interaction when dealing with DI&C systems instead of AI&C systems. Human error rates for simple tasks, such as reading digital meters and digital controls (e.g., flow control), as compared to analog indications should be developed (or shown that the impact of DI&C on HRA is minimal). Modified HRAs may also be needed if the procedures (such as EOPs) are computerized.
- New HRA models and values are needed for backup actions when a DI&C system fails to respond. Operator training and infrequent use of procedures should be explicitly accounted for.
- HRAs must be developed for cases when DI&C system failures result in significant loss or spurious indicators and alarms. Both acts of omission and commission should be addressed. This issue should, at minimum, be addressed as a part of fire and flood PRAs.

8. CCF of DI&C Hardware

Hardware portions of DI&C systems are physical systems and their CCF contributions can be readily accounted for using the current methodology and generic data. Some specific requirements for CCF models are listed below:

- The hardware CCF contributions shall account for the use of different technologies (e.g., FPGA unit versus micro-processors). Different DI&C technologies, however, could be susceptible to the same environmental impact, albeit with different degrees. These common susceptibilities should be modeled with the triggering conditions within PRA models. Hardware CCF shall also account for the use of different manufacturers, procedures, segregation, and staggered testing using the CCF data (no modeling requirement).
- Estimation and modeling of hardware CCF should account for fault diagnostic and fault tolerance schemes.
- Use of CCF empirical data must also differentiate between the specific safety class applications of DI&C systems. The hardware CCF failures and the associated probabilities should differentiate between detectable and undetectable failures.

The current CCF modeling methodology may be applied to DI&C hardware if sufficient data is available. Simpler models may be implemented consistent with the availability of data. NRC has sponsored several ongoing research projects on DI&C CCF methodology and data.

9. CCF of DI&C Software

Software CCF is expected to depend on software classification (safety versus non-safety). The CCF should be estimated for each class separately. Software CCF should account for partial and full diversity. The examples of diversities affecting software CCF that should be addressed explicitly are as follows:

- N-version programming.
- Use of different technology and programming language (FPGA, PLC, microcomputers, etc.).
- Manual backup system, the ultimate defense against errors in requirement specification or meeting the design requirements.

Software CCF causes due to systemic issues might not be detected through periodic testing or monitoring. Other software CCF causes can be detected during periodic testing or continuous monitoring. For these cases, the CCF causes could be identified and rectified (i.e., software is updated). Similar situations could result from continuous monitoring and diagnostic schemes. Plant corrective action program and DRAP effectiveness can be credited for reducing the potential CCF events. In rare cases, software failures can be caused by the interaction between hardware and software if they are not prevented using fault detection/fault tolerance schemes. Hardware diversities, such as diversity in communication link, shall be considered as a part of software CCF evaluation. Software CCF could also result from failure of the operating system. When common operating systems are used, the contribution of the failure of the operating system should be addressed.

10. DI&C System Failures Harsh Environment

DI&C systems are sometimes expected to perform their functions in harsh environments. The harsh environment could occur prior to core damage or post core damage. The intensity of the harsh environment can be estimated for the specific sequence of events (i.e., the context of demand). With a focus on the pre-core damage scenarios in LWRs, the following items should be addressed in DI&C PRAs:

- The impact of fire and smoke during a fire scenario.
- The impact of water spray during a flood or pipe-break scenario.
- The impact of high-temperature steam from pipe breaks.
- The impact of seismic events.
- The impact of high-energy arc flashes (direct contact or via EMI/RFI).

6. REFERENCES

1. RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.”
2. RG 1.177, “An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications.”
3. RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.”
4. RG 1.201. “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance.”
5. RG 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants.”
6. SECY-15-10106, “Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, ‘IEEE standard criteria for safety systems for nuclear power generating stations,’” (RIN 3150-AI98), February 25, 2016.
7. MIL-STD-882E, “System Safety,” Department of Defense Standard Practice, May 11, 2012.
8. IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems,” Seven (7) parts, Commercial Version (CMV), International Electrotechnical Commission, 2010.
9. Jackson, T.W., and Brill, R., “A Study of Nuclear Power Plant Events That Involve Instrumentation and Control Systems,” Proceedings of ICONE 8, 8th International Conference on Nuclear Engineering, April 2-6, 2000, Baltimore, MD, USA.
10. EPRI 1019183, “Effect of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants, December 2009.
11. EPRI 1025278, “Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments,” July 2012.
12. David Blanchard, Thuy Nguyen, and Ray Torok, “Modeling Digital I&C in PRA: Considering Context and Defensive Measures,” ANS PSA 2013, Columbia, SC, September 22 to 26, 2013.
13. EPRI 1016731, “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems,” December 2009.
14. EPRI 1021077, “Estimating Failure Rates in Highly Reliable Digital Systems,” December 15, 2010.
15. EPRI 1022986, Digital Operating Experience in the Republic of Korea, 2011.
16. Standard Review Plan (SRP), Chapter 19.0, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” NUREG-0800, December 2015.
17. K. Korshah, et al., “An Investigation of Digital Instrumentation and Control System Failure Modes,” ORNL/TM-2010/32, Technical Report March 2010.
18. Stacy A. Davis, Heather L. Detar and Yves Masset, “Lessons Learned from the Digital I&C System Modeling of the AP1000 Plant PRA,” ANS PSA 2013, September 22-26, 2013, Columbia SC.
19. 217Plus is a methodology and a software tool that was developed by the RIAC to aid in the assessment of system reliability. It represents the next generation of the PRISM software tool initially released in 1999.
20. T.L. Chu, M. Yue, et al., “Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods,” NUREG/CR-6997, September 2009.
21. NEA/CSNI/R(2014)16, “Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA,” 2/15/2015.

22. NKS-330, “Guidelines for Reliability Analysis of Digital Systems in PSA Context,” Risk Pilot AB, Sweden, and VTT of Finland, February 2015.
23. NKS-361, “Modelling of Digital I&C, MODIG-Interim report 2015,” Risk Pilot AB, Sweden, and VTT of Finland, March 2016.
24. Branch Technical Position (BTP) 7-19, Rev. 7-August 2016, NUREG-0800, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems.”
25. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994.
26. Hyun Gook Kang, et al., “An Overview of Risk Quantification Issues for Digitalized Nuclear Power Plants Using A Static Fault For a DI&C module Tree,” Korean Atomic Energy Research Institute, March 10, 2009.
27. Pierre Rebouus, Taghi M. Khoshgoftaar, “Software Failure; An Overview,” Science direct, advances in computers, 2006.
28. NUREG/CR-7151, “Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems.”
29. 60 FR 42622, “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement.”
30. “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum A,” ASME/ANS RA-Sa-2009, American Society of Mechanical Engineers, March 2009.
31. NEI 17-07 [Rev A], Performance of PRA Peer Reviews Using the ASME/ANS PRA standard, December 2017.
32. NUREG-1855, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making,” March 2009.
33. Electric Power Research Institute, “Guideline for the Treatment of Uncertainty in Risk-Informed Applications: Technical Basis Document," EPRI TR 1009652, Palo Alto, CA, December 2004.
34. NEI 06-09 Rev0-A, “Industry Guidance for Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS),” November 2006.
35. NUREG/CR-5500, “Reliability Study: Westinghouse Reactor Protection System, 1984-1995,” Vol. 2, December 1998. NUREG/CR-550 has several volumes and covers all reactor designs.
36. NEI 00-04 (Rev 0), “10 CFR 50.69 SSC Categorization Guideline,” July 2005.
37. NEI 04-02, “Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c),” Revision 1, September 2005.
38. NFPA, “Performance Based Standard for Light Water Reactor Electric Generating Plants,” NFPA-805, 2001.
39. NRC, “EPRI/NC-RES Fire PRA Methodology for Nuclear Power Facilities,” NUREG/CR-6850 2005.
40. NRC/EPRI, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” NUREG-1824, EPRI-1011999, 2007.
41. “Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG), NUREG-1934, EPRI 1023259, November 2012.
42. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines, NUREG-1921/EPRI 1023001, July 2012.
43. ASME/ANS PRA standard, “Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” currently ASME/ANS-RA-Sa-2009.
44. NEI 17-07, “Performance of PRA Peer Reviews Using the ASME/ANS PRA Standard,” December 2017.

45. NEA/CSNI/R(2014), “Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA,” February 16, 2015.

APPENDIX A. INTEGRATING RISK INFORMATION INTO THE REGULATORY FRAMEWORK BY FOUR NON-NUCLEAR SECTORS

A.1 PREFACE

This appendix provides the technical basis for Chapter 2 of the main report (Vol.1). It documents the review of pertinent references that can help to determine the state of risk informed applications and to identify the challenges of performing PRA for instrumentation and control (I&C) system based on the current practices in four non-nuclear industries.

The main purpose of the regulatory risk-informed decision making (RIDM) process in non-nuclear industries is to allocate the resources in a manner that focuses effort on greater risk contributors. This reduces the potential for assigning the undue amount of resources of managing lower-risk activities.

The risk-informed regulatory framework for these industries generally includes two major processes:

1. All proposed changes and modifications should meet the specific requirements. These regulatory requirements are defined for each class of structures, systems, and components (SSCs). SSC classifications in non-nuclear industries will be discussed in the following sections, SSC classifications are performed using risk insights (e.g., The Federal Aviation Administration [FAA] defines them as design assurance levels or DALs). For each SSC class, commensurate with their risk significance, a set of requirements consistent with the general intent of the industry regulation are defined. The set of requirements include requirements for defense-in-depth, single failure criteria, diversity and use of industry standards. The industry standards and the general regulatory approach include certain level of conservatisms in the form of safety margins. This is similar to Items 1 through 3 of the NRC risk-informed framework, which is detailed in Appendix C.
2. All non-nuclear industries rely on a risk and safety management program for ensuring safety during operation. This formal program is generically referred to as Safety Management System (SMS). SMS is built around four components: Safety Policy (Objectives), Safety Risk Management (SRM), Safety Assurance (SA), and Safety Promotion. A detailed review of SRM and SA will be considered later in this report. The SMS program covers items 4 and 5 of NRC risk informed framework.

In principle, all industries, including the NRC, use a five-element, risk-informed framework. These elements are noted below.

1. Meet the intent of regulations.
2. Preserve defense-in-depth.
3. Maintain safety margins.
4. Control changes in risk.
5. Establish assurance of control mechanisms through monitoring.

These elements are included in a risk-informed decision making (RIDM) process, generally referred to as the safety management system (SMS). The risk analysis parts of risk-informed decision making within the SMS process entails the evaluation of six elements:

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

4. What are the tolerable limits of risk?
5. Is the risk acceptable and if not, what are the possible means to reduce and control risk (alternatives), through design change, regulatory oversight, operational and maintenance strategies?
6. How to select the most efficient alternatives to make the risk acceptable?

Elements 1, 2, and 3 define risk. In non-nuclear industries, elements 2 and 3 above are not generally combined (kept separate) for each scenario in the form of a matrix. In NRC space, risk is generally defined by the products of the measures in Elements 2 and 3 summed over all scenarios.

Elements 4, 5, and 6 could constitute the implementation of RIDM process within the formal framework of SMS. The risk insights supporting these elements could be based on expert judgment, industry specific experience, generic experiences as documented in national and international standards, quantitative estimates from historical data, and finally a model-based, data-driven analysis such as quantitative PRA. The choice of the approach depends on the specifics of RIDM application within the industry sector. If an industry sector does not change the basic design and operation across facilities and over a long period of time, it could accumulate enough operational data to conduct empirical risk estimation, identification of the risk insights, and selection of the beneficial risk-informed practices directly from operational events.

In conclusion risk-informed regulatory decision making can facilitate efficient allocation of resources by applicants for design and operation and regulatory oversight including the extent of regulatory reviews for approval. This is achieved by considerations for scenarios, accident frequency, and consequences. The basis and details of risk-informed regulatory decision making however varies significantly across industries owing to innovation in the design and operation including the consequence and regulatory environment. Comparison of risk-informed practices across industries should be considered in context of the above considerations. The risk-informed approaches at the highest level are generally consistent but at the lower levels of details could be quite different.

A.2 INTRODUCTION

This appendix documents the state-of-the-art and the state-of-the-practice approaches for integrating risk insights into regulatory reviews that are used in non-nuclear agencies or industries. Risk insights are used in many industries. The most relevant industries with approaches that could provide technical insights for improving the DI&C regulatory framework in the nuclear industry are: civil aviation (Department of Transportation; Federal Aviation Administration-DOT/FAA), chemical industries, and National Aeronautics Space Administration (NASA), and Department of Transportation; Federal Rail Administration (DOT/FRA).

It was discovered that the uses of risk insights in regulatory framework are extensive in each of these four non-nuclear industries. Many references and documents were examined to better understand the approaches for integrating risk insights into regulatory reviews. A detailed review of all these documents was considered not to be practical. For this reason, the review process was performed in two stages. In the first stage, large numbers of documents were briefly reviewed (stage 1 review). A smaller set of documents were then selected based on the insights gained from the stage 1 review for further examination. Chapter A.3 briefly discusses the insights from the stage 1 review and identifies the documents selected for each of these four industries.

Chapter 4 discusses the insight gained from the detailed review (stage 2 review). Chapter 4 also elaborates on practices and approaches for integrating risk insights into regulatory reviews in each of the four industries in a detailed manner.

Chapter 5 provides summaries of the state-of-the-practice approaches for integrating risk insights into regulatory reviews for each industry sector, focusing on limited number of attributes that are common and essential for risk informed applications. This allows some comparison across the industrial sectors.

Chapter 6 compares the generic aspects of risk-informed activities across the four non-nuclear industries.

A.3 SELECTION OF RELEVANT DOCUMENTS FOR FURTHER EXAMINATION

Risk insights are used in many industries. The most relevant industries with approaches that could provide technical insights for improving the DI&C regulatory framework in the nuclear industry are: civil aviation (Department of Transportation; Federal Aviation Administration-DOT/FAA), chemical industries, and National Aeronautics Space Administration (NASA),and Department of Transportation; Federal Rail Administration (DOT/FRA). Many documents were briefly reviewed in stage 1 review, and a smaller set were identified for a detailed review (Stage 2 review as discussed in Chapter A.4). All references for stage 1 review; discussed in this chapter (i.e., Chapter A.3), are footnoted to reflect that they were not reviewed in detail. Formal references are noted in section A.7 includes those documents that were reviewed in detail (Chapter A.4 and after). The readers who are interested in detailed discussions may directly go to Section A.4, skipping Section A.3, altogether. Following is a brief discussion for selecting the smaller set of documents for detailed examination.

A.3.1 Integrating Risk Insights into Regulatory Reviews of Civilian Aviation Industry (DOT/FAA)

Guidelines for civil aviation industry [SAE ARP 4754A-2010] have been developed in the context of 14CFR Part 25. SAE ARP 4754A-2010[13] discusses the development of aircraft systems considering the overall aircraft operating environment and functions. This document addresses the development cycle for aircraft and systems that implement aircraft functions. It does not include specific coverage of detailed software or electronic hardware development, safety assessment processes, inservice safety activities, aircraft structural development nor does it address the development of the master minimum equipment list or configuration deviation list. Guidelines and methods for conducting safety assessment process on civil airborne systems and equipment are discussed in a separate report (ARP 4761[14]). More detailed coverage of the software aspects of development are found in RTCA document DO-178B, 'Software Considerations in Airborne Systems and Equipment Certification'. RTCA/DO-178C[15], published in 2012 is the de facto guidance document used in the development of airborne software and was published as an improved revision to RTCA/DO-178B. DO-178C is the safety critical standard for developing avionics software systems developed jointly by the Radio Technical Commission for Aeronautics (RTCA) safety critical working group RTCA SC-167 and the European Organization for Civil Aviation Equipment EUROCAE WG-12.

The purpose of DO-178B is to provide guidelines for the production of software for airborne systems and equipment that performs its intended function with a level of confidence in safety that complies with airworthiness. The guidelines are in the form of objectives for software life cycle processes, which included: descriptions of activities and design considerations for achieving those objectives and descriptions of the evidence that indicate that the objectives have been satisfied. DO-178B defines specific levels of safety criticality, from highest to lowest. The Software Level, also known as the Design (or Development) Assurance Level (DAL) or also "'Item Development Assurance Level"' (IDAL) is determined from the safety assessment

[13] SAE ARP 4754A-2010; Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems*, dated December 21, 2010, can be purchased from the webstore ansi.org/standards/SAE.

[14] SAE document ARP 4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.”

[15] RTCA/DO-178C; guidance document of airborne software, revision to RTCA/DO-178B, 2012.

process and hazard analysis by examining the effects of a failure condition on the system. The failure conditions are categorized by their effects on the aircraft, crew, and passengers. These are:

Level A - Catastrophic: prevent continued safe flight or landing
Level B - Hazardous/Severe-Major: potentially fatal injuries to a small number of occupants [failure rate per hour 10^{-7}]
Level C - Major: impairs crew efficiency, discomfort, or possible injuries to occupants
Level D - Minor: reduced aircraft safety margins, but well within crew capabilities
Level E - No Effect: does not affect the safety of the aircraft at all Coverage of electronic hardware aspects of development are found in RTCA document DO-254/EUROCAE ED-80, 'Design Assurance Guidance for Airborne Electronic Hardware'. Design guidance and certification considerations for integrated modular avionics are found in appropriate RTCA/EUROCAE document DO-297/ED-124. Details for in-service safety assessment are found in ARP5150, 'Safety Assessment of Transport Airplanes in Commercial Service' and ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service. Post-certification activities (modification to a certificated product) are covered in section 6 of this document. DO-254, “Design Assurance Guidance for Airborne Electronic Hardware,” was released in 2000 and it is formally recognized by the FAA in 2005 via Advisory Circulars, AC-152 as a means of compliance. It provides guidance for the design of Complex Electronic Hardware in airborne systems and equipment for use in aircraft or engines. There are three advisory circulars (the third one is currently expired) which are not by themselves regulations, but they describe an acceptable means to comply with regulations[16]. The most pertinent advisory circulars discuss various aspects of safety management system (SMS). These are:

1. AC-120-92B: this document provides a description of regulatory requirements, guidance, and methods of developing and implementing an SMS. SMS is built around four components: Safety Policy (Objectives), Safety Risk Management (SRM), Safety Assurance (SA), and Safety Promotion. A detailed review of SRM and SA will be considered later in this report.
2. AC-23-1309-1E: This AC focuses among other things on Functional Hazard Assessment including Fault tree Analysis. Acceptable methods for Treatment of Common Cause Failures (CCF) are also discussed as a part of SMS. These portions of the document will be examined in detail later in this report.
3. AC-431.35-2A: Note this AC replaces AC 431.35-2 which is canceled. This AC provides guidance concerning applying a systematic and logical system safety process for identification, analysis, and control of public safety hazards and risks associated with the operation of reusable launch vehicle (RLV) and reentry vehicle (RV) systems. This AC also discusses the process of identifying safety critical systems, and events under system safety engineering. This AC will be examined later.

Chapter 4 of Risk Management Handbook, FAA-H-8083-2 (Change 1), was considered for review to better understand how FAA utilizes risk matrix to classify events, and critical systems. FAA-H-8083-2 (Change 1) is an updated version of FAA-H-8083-2, Risk Management Handbook, dated January 2016. The relationship of risk matrix to grades of safety critical systems will be examined (Chapters 4 and 5 only).

[16] 14 CFR Applicable Sections. Title 14 CFR 23.1301, 23.1309, 25.1301, 25.1309, 27.1301, 27.1309, 29.1301, 29.1309, 33.28, 33.75, 35.23, and 35.15.

Section A.4 (of this appendix) provides details of our findings from reviews of all FAA related documents.

A.3.2 Integrating Risk Insights into Regulatory Reviews of Chemical Sector

US Chemical Safety Board (CSB), is an independent federal agency charged with investigating industrial chemical accidents. Headquartered in Washington, DC, the agency's board members are appointed by the President and confirmed by the Senate. CSB is authorized by the Clean Air Act Amendments of 1990 and became operational in January 1998. CSB makes recommendations to plants, regulatory agencies such as the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA), Department of Homeland Security industry organizations, and labor groups. CSB is a non-regulatory and independent of other agencies so that its investigations might, where appropriate, review the effectiveness of regulations and regulatory enforcement[17].

The main regulatory bodies for chemical industries are EPA and OSHA under Labor Department. There is quite an overlap between EPA and OSHA requirements. The main difference is that; EPA requirements are focused on protecting the public and the environment external to the facility, whereas OSHA requirements focus on the facility and workers (people on site). In the Clean Air Act Amendments of 1990, Congress required OSHA to adopt the Process Safety Management (PSM) standard (see OSHA 3132 and 3133) to protect workers and required EPA to protect the community and environment by issuing the Risk Management Plan Rule (RMP) (see https://www.epa.gov/rmp).

At the core of EPA regulatory compliance is the Risk Management program (RMP). RMP guidance is designed to provide technical instructions on how to determine if a chemical facility is subject to 40 CFR Part 68, and how it can comply with 40 CFR Part 68. An important part of RMP is a hazard identification and assessment referred to as Process Hazard Assessment (PHA). PHA used by EPA typically generates quantitative results especially for consequence analyses although in most cases are categorized into several bins.

Similarly, the core of OSHA regulatory compliance is Process Safety Management (PSM). PSM and RMP were written to complement each other in accomplishing the Congressional goals of Clean Air Act Amendments. "OSHA believes that a process hazard analysis is the cornerstone of any effective program for managing hazards," 55 Fed. Reg. 29,514 (1990; see preamble to proposed rule on Process Safety Management). In general, the terms "chemical process hazard assessment" and "hazard assessment" are used to encompass both the hazard identification process and the hazard quantification process.

Another important resource for chemical safety which involves a description of the best practices is found in Consul for Chemical Process Safety (CCPS). CCPS promote risk-based process safety (RBPS) to support compliance with RMP and PSM. CCPS RBPS is not a regulatory requirement; however, it does provide a helpful guidance for process safety program.[18] CCPS also recommend a series of best practices for safety and reliability through a series of references (generally publicly available books for purchase). Details of CCPS RBPS guideline could be found in a book that could be publicly purchased.

[17] IESS reviewed one of the CSB investigation reports. We found it quite detailed and we think NRC will benefit from reviewing the pertinent investigation report and keep liaison with CSB.

[18] Please see https://www.aiche.org/ccps/resources/publications/summaries/summary-guidelines-risk-based-process-safety for guidance of CCPS RBPS best practices.

General RMP guidance can be found in "General Guidance on Risk Management Programs for Chemical Accident Prevention (see https://www.epa.gov/rmp/guidance-facilities-risk-management-programs-rmp#general)". Chapter 7, 9, and Appendix D of RMP guidance are considered for further review. Chapter 7 of RMP guidance deals with Prevention program (Program level 3; see discussion below), Chapter 9 is on risk management plan and mostly focused on the required periodic or event-based updates of PHA and other elements of prevention program and Appendix D deals with OSHA guidance on PSM.

Program Levels are defined in Chapter 2 of RMP guidance. The three program levels that are defined below:

> **Program 1:** Processes which would not affect the public in the case of a worst-case release (in the language of Part 68, processes "with no public receptors within the distance to an endpoint from a worst-case release") and with no accidents with specific offsite consequences within the past five years are eligible for Program 1, which imposes limited hazard assessment requirements and minimal prevention and emergency response requirements.
>
> **Program 2:** Processes not eligible for Program 1 or subject to Program 3 are placed in Program 2, which imposes streamlined prevention program requirements, as well as additional hazard assessment, management, and emergency response requirements.
>
> **Program 3:** Processes not eligible for Program 1 and either subject to OSHA's PSM standard under federal or state OSHA programs or classified in one of ten specified North American Industrial Classification System (NAICS) codes are placed in Program 3, which imposes OSHA's PSM standard as the prevention program as well as additional hazard assessment, management, and emergency response requirements.

Program 3 (or Program Level 3) appears to be the most applicable to regulatory environment of commercial nuclear power plants.

The second most important resource of the CCPS is a book on Guidelines for Risk Based Process Safety, CCPSRBPS as discussed earlier. A summary and topics of discussions can be downloaded from the CCPS site; (https://www.aiche.org/ccps/resources/publications/summaries/summary-guidelines-risk-based-process-safety). This book is examined to identify the use of risk insight in the chemical regulatory framework (see Section A.4.2).

The third resource which has a closer focus on Digital I&C is entitled, "Guidelines for Safe Automation of Chemical Processes, 2nd Edition, CCPS, ISBN: 978-1-118-94949-8 December 2016 648 Pages[19].An important discussion in this book is related to the safety classification of Instrumentation and control "SCIA" which considered relevant to 10 CFR 50.69. Review of this book could be beneficial; however, it could be beyond the scope of this task. Limited reviews of couple of chapters are envisioned at this time. See https://www.wiley.com/en-s/Guidelines+for+Safe+Automation+of+Chemical+Processes%2C+2nd+Edition-p-9781118949498.

[19] "Guidelines for Risk Based Process Safety," 768 pages, ISBN: 978-0-470-16569-0, John Wiley, March 2007.

Section A.4.2 of this appendix provides details of our findings from reviews of all related documents for chemical industries.

A.3.3 Integrating Risk Insights into Regulatory Reviews for NASA (Aerospace Industry)

NASA policy directives (NPDs) set forth NASA's governance framework, the principle and structure through which the Agency manages mission, roles, and responsibilities. High level guidance in NPDs and relevant Code Federal Regulations on personal safety and environment are transformed to a set of requirements that are published in NPRs (NASA Procedure requirements). Guidance is provided in various NASA handbooks, safety standards, and guidebooks which describe an acceptable method to comply with NPRs.

A set of NPRs and NASA handbooks are considered for detailed review, in the hope that the review of these limited set (selected documents) would provide a perspective of NASA safety activities. The set selected is based on preliminary review of a larger number of NASA documents and private conversation with several colleagues (associated with NASA safety programs). The selected set of documents discussed below deemed relevant to USNRC's risk-informed regulatory framework in general and digital I&C in specific.

1. NPR-8000-004B: This NPR provides the requirements for risk management for the Agency, its institutions, and its programs and projects as required by NPD 1000.0; NPD 7120.4; NPD 8700.1, and other Agency directives. Risk management includes two complementary processes: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM).
2. NPR 8715.3D: This NPR provides the basis for the NASA Safety Program and serves as a general framework to structure more specific and detailed requirements for NASA Headquarters, Programs, and Centers. This NPR is directed toward safety requirements and to augment requirements for occupational health and environmental health of personnel and activities. Occupational safety and health requirements that implement 29 CFR Part 1960, are specified in NPR 8715.1. Environmental requirements are specified in NPD 8500.1. Specific Sections of this NPR is of interest for detailed review. These sections are mainly related to risk and hazard evaluations and control. It would at minimum include Chapters 1 and 2.
3. NPR 8705.2C: The subject of this NPR is Human-Rating Requirements for Space Systems. A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards, and manages safety risk associated with human spaceflight, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations. Human-rating is not and should not be construed as certification for any activities other than carefully managed missions where safety risks are evaluated and determined to be acceptable for human spaceflight. Section 2.3 (specifically 2.3.6 and 2.3.7) of NPR 8705.2C discuss safety goals (thresholds) and requirements for identifying risk significant contributors as a part of Human Rating Certification Process (HRCP) requirements. Section 3.2 specifically discusses System Safety Requirements including single failure tolerance (passive systems are exempted). Higher margin requirements are set when single failure tolerance requirement is not met. There are also discussion and requirements for diversity vs. redundancy.

4. NASA/SP-2010-580: NASA System Safety Handbook, Volume 1, System Safety Framework and Concepts for Implementation. This handbook describes a holistic approach to safety management. This handbook considers measures of aggregate safety risk and to ensure wherever possible that there be quantitative measures for evaluating how effective the controls are in reducing these aggregate risks. Secondly, the handbook stresses the necessity of developing controls that are derived to reduce known risk also providing some protection against broad categories of risks (including risks that cannot be easily characterized). Thirdly, the handbook always strives to treat uncertainties as an integral aspect of risk and as a part of making decisions. This document is considered for a more detailed examination. The primary focus will be on Chapters 3 and 5.
5. NASA/SP-2014-612: NASA System Safety Handbook, Volume 2 System Safety Concepts, Guidelines, and Implementation Examples. This handbook aimed at the development of a more objectives-based assurance approach, in which the decomposition of top-level safety and mission success objectives into concrete sub-objectives and associated strategies are discussed. This is used to form the basis for the planning and review of assurance activities. Chapter 3 on System Safety Framework, Chapter 5 (sections 5.2 and 5.3), and Chapter 6 for developing Risk-Informed Safety Case are selected for more detailed review.

There are several other NASA documents that are more focused on RIDM and quantitative risk assessments. Several of these documents were also reviewed. Examples are:

- NASA/SP-2010-576 discusses NASA's approach to risk-informed decision making (RIDM).
- NASA/SP-2011-3421 develops the PRA procedure guide for estimating the probabilities associated with several different undesirable accidents. Chapter 9 of this documents is devoted to software risk and reliability techniques

Section 4.3 of this appendix provides details of our findings from reviews of all NASA related documents.

A.3.4 <u>Integrating Risk Insights into Regulatory Reviews for DOT/FRA</u>

A small portion of the rail/train regulations that considered most pertinent to the objective of this project as contained in 49 CFR Part 236 was reviewed. In response to a fatal train collision in September 2008, Congress passed the Rail Safety Improvement Act (RSIA) of 2008, which updated the Code of Federal Regulations (CFR) to require Positive Train Control (PTC) to be installed along every passenger rail corridor prior to December 31, 2015. In October 2015, the statutory deadline for PTC implementation was extended to 2020, provided that certain milestones were met and approved by the FRA by December 2018.

PTC is a redundant and diverse system that is used along with existing safety and signaling systems. PTC is intended to prevent:

- Train-to-train collisions
- Over-speed derailments
- Incursions into established work zone limits and
- The movement of a train through a mainline switch in the improper position

PTC is a communications-intense technology. It transmits data between trains and communication towers using wireless Internet, GPS, and encrypted radio transmissions. It requires tens of thousands of sensors to be installed on train tracks and locomotives and a data center to analyze the information. PTC uses the sensors and integrated monitoring systems to track key movement on trains and conditions on rail tracks in real time to identify potentially hazardous situations. If an unsafe situation arises, PTC automatically will trigger a train's braking system in order to prevent an accident, such as a train-to-train collision. This is a complete processor based (digital I&C) system.

49 CFR 236 Subpart H[20] is considered for further examination. This subpart discusses the safe operation of processor-based signal and train control systems, subsystems, and components that are safety-critical products, as defined in §236.903, and to facilitate the development of those products. It prescribes a minimum set of performance-based safety standards for safety-critical products, including requirements to ensure that the development, installation, implementation, inspection, testing, operation, maintenance, repair, and modification of those products will achieve and maintain an acceptable level of safety.

49 CFR 236 Subpart I [21] (prescribes minimum, performance-based safety standards for PTC systems required by 49 U.S.C. 20157, this subpart, or an FRA order, including requirements to ensure that the development, functionality, architecture, installation, implementation, inspection, testing, operation, maintenance, repair, and modification of those PTC systems will achieve and maintain an acceptable level of safety. This subpart also prescribes standards to ensure that personnel working with, and affected by, safety-critical PTC system related products receive appropriate training and testing. Due to prescriptive nature (not risk informed) and specificity of the guidance to PTC, this Subpart was not considered for further examination.

49 CFR 236, Appendix B[22] is considered for further examination. It discusses a minimum set of criteria to be considered for risk assessment/hazard evaluation of safety critical products through. The set of criteria discussed are instructional (qualitative, not quantitative criteria) requirements that risk assessment should meet. It discusses the requirements for constructing risk matrix, hazard identification and assessment.

49 CFR 236, Appendix C[23] is considered for further examination. This appendix provides safety criteria and processes that the designer must use to develop and validate the product that meets safety requirements of this part. FRA uses the criteria and processes set forth in this appendix to evaluate the validity of safety targets and the results of system safety analyses. It specifies safety principles, system safety under normal operating conditions, system safety under failures, and requires no single failure point for safety critical systems. This includes single hardware failures as well as multiple hardware failures that may occur at different times but remain undetected (latent) and react in combination with a subsequent failure at a later time to cause an unsafe operating situation. This appendix also makes references to IEC

[20] 49 CFR 236 Subpart H; "Standard for Processor-Based and Train Control Systems," 3/7/2005, http://federal.elaws.us/cfr/title49.part236.subparth.
[21] 49 CFR 236 Subpart I; "Positive Train Control (PTC) System," 1/5/2010, http://federal.elaws.us/cfr/title49.part236.subparti.
[22] 49 CFR 236 Appendix B, "Risk Assessment Criteria," 1/15/2010; http://federal.elaws.us/cfr/title49.chapterii.part236.appb.
[23] 49 CFR 236 Appendix C, "Safety Assurance Criteria and process," 1/15/2010, http://federal.elaws.us/cfr/title49.chapterii.part236.appc.

(International Electrotechnical Commission) standards. So, it appears that they rely on Safety Integrity Levels (SILs) as described by IEC standards.

A Practical Risk Assessment Methodology (PRAM) for analyzing railroad accident data and assessing the risk and benefit of safety-critical train control systems is reported in a report by FRA; DOT/FRA/ORD-09/15[24].This report documents in simple steps the algorithms and data inputs that are required to calculate the collective risks associated with a proposed system (such as a positive train control system). The proposed system must be designed such that quantitative hazard rates do not exceed the reference safety target. These hazard rates, called tolerable hazard rates, form a key part of the safety requirements specification for the proposed system. A software tool has been developed for use by risk analysts/safety engineers to implement the steps of PRAM in an iterative manner. This document is also selected for further examination.

[24] DOT/FRA/ORD-09/15, "A Practical Risk Assessment Methodology for Safety-Critical Train Control Systems," 7/1/2009, https://www.fra.dot.gov › elib › document.

A.4 EXAMINATION OF SELECTED DOCUMENTS TO GAIN INSIGHT IN RISK- INFORMED REGULATORY FRAMEWORK

This section discusses the Risk-Informed Regulatory Framework for the four non-nuclear industries (FAA, Chemical, NASA, and FRA), by further examination of the selected documents. The selected documents are discussed first, followed by a summary section identifying the important insights for risk-informed regulatory framework gained from each industry sector.

A.4.1 Risk-Informed Regulatory Practices of Civilian Aviation Industry (DOT/FAA)

ARP 4754A [Ref. 1] describes the aircraft and/or system development assurance process. This process results in identifying appropriate Development Assurance Level (DAL)[25]. Process for DAL determines the rigor required for development, the verification and validation activities for complex hardware and software. Functional Hazard Assessments are central to determining safety importance of the software and hardware and assigning DAL. Based on the DAL assigned, requirements for testing and other verification methods are specified. For certification plan two levels of assurance are determined: The Functional Development Assurance Level (FDAL), and Item Development Assurance Level (IDAL). Risk insights are relied on for justification of these levels as will be discussed shortly. The required processes to meet the associated objectives of the ARP 4754A should also be developed for FAA concurrence.

Example application of ARP 4754A, as discussed in NASA/CR-2015-218982,[Ref. 2], shows on how qualitative hazard analysis are used. There are generally five steps involved. These are:

1. Functional decompositions are performed
2. Hazardous Functional Failures are identified
3. For each failure at a flight phase, failure condition/hazard description along with impact on aircraft/crew is defined. Impacts are classified to Catastrophic, Hazardous, Major, and Minor based on Engineering Judgment.
4. Safety objectives are defined
5. FDALs are assigned to meet safety objectives

General definitions of impact or severity classification (item 3) are provided below:

Catastrophic: Failure conditions which prevents continued safe flight, for example, loss of all attitude display, loss or incorrect airspeed, inability to determine the correct airplane heading.

Hazardous (Severe Major): Large reduction in safety margins or functional capabilities, excessive increase in crew workload, for example, erroneous airspeed require crew to cross-check with standby airspeed instrument to recognize condition.

Major: Significant reduction in safety margins or functional capabilities; for example, Crew must rely on standby instrument for attitude reference information due to loss of operating redundancy (not erroneous signal).

Minor: Slight reduction in safety margins, slight increase in crew workload, or inconvenience to occupants; for example, crew must engage to routine manual thrust control due to loss of auto-thrust control.

[25] This is similar to SSC classifications in nuclear industry.

These analyses steps are performed based on engineering judgment and qualitative hazard assessments. ARP 4754A does not rely on Quantitative Risk Assessment (QRA) at this stage. Qualitative hazard assessment is used for classification of FDAL/IDALs. Issues such as Common Cause potential is also dealt with through deterministic assessment and generally documented in Preliminary Aircraft Safety Assessment (PASA).

For system Level analysis, recommended practices contained in ARP-4761 [Ref. 3] are used. More detail guidance for ARP- 4761 for electronic and computerized systems are provided in DO-254 [Ref.4] and DO-178B [Ref.5]. DO-297 [Ref. 6] is used for Integrated Modular Avionics. Figure A-1 shows the relationship between these different documents.

DO-254, “Design Assurance Guidance for Airborne Electronic Hardware,” was released in 2000 and formally recognized by the FAA for regulatory compliance in 2005. It provides guidance for the design of complex electronic hardware in airborne systems, and equipment for use in aircraft or engines as well as detailed guidance for change control (see Section 7.2 of DO-254). It also discusses what is required before COTS (Commercially-off-the-Shelf) equipment can be used for FDAL systems.

DO-178 is the established software counterpart of DO-254. Both DO-178 and 254 highlight the importance of Common Cause Failures (CCFs) and provide guidance to protect against them. For example, DO-178 recognizes that software CCF can be controlled by Multi-Version Dissimilar Software (MVDS). MVDS is a system design technique that involves producing two or more modules of software; each providing the same function, but in a way that avoid some common sources of errors in the components. In some documents, MVDS is also referred as N-version programming for software diversity.

The guidance provided in DO-254 and DO178 is mainly process oriented, deterministic, prescriptive, and instructional. They focus on life cycle processes which start by determining the DAL and associated requirements, and follow through planning, design processes, verification/validation, configuration management, process assurance and certification. These documents include detailed information important to airplane designer. Risk insights and lessons from the past reliability performance of the system have been incorporated in the form of prescriptive guidance into these documents. Furthermore, DAL classifications and class specific requirements make sure that the resources are efficiently assigned based on the qualitative understanding of risk and hazards. Quantitative risk-informed and reliability-based approaches relying on the associated methods/data are also recommended but not mandatory, for aviation industry. These recommended practices which are not mandatory, are mainly provided under Advisor Circulars (ACs).

AC-23.1309 [Ref. 7] sets forth an acceptable means of showing compliance with Title 14 of the *Code of Federal Regulations* (14 CFR), § 23.1309, through Amendment 23-62: for equipment, systems, and installations in 14 CFR part 23 airplanes. As discussed earlier, Advisory Circular contains recommended practices which are not mandatory. This AC provides specific guidance on the relationship of classes of safety and their expected quantitative reliability performance. This is shown in Figure A-1 below (reproduction of Figure 2 in AC-23-1309).

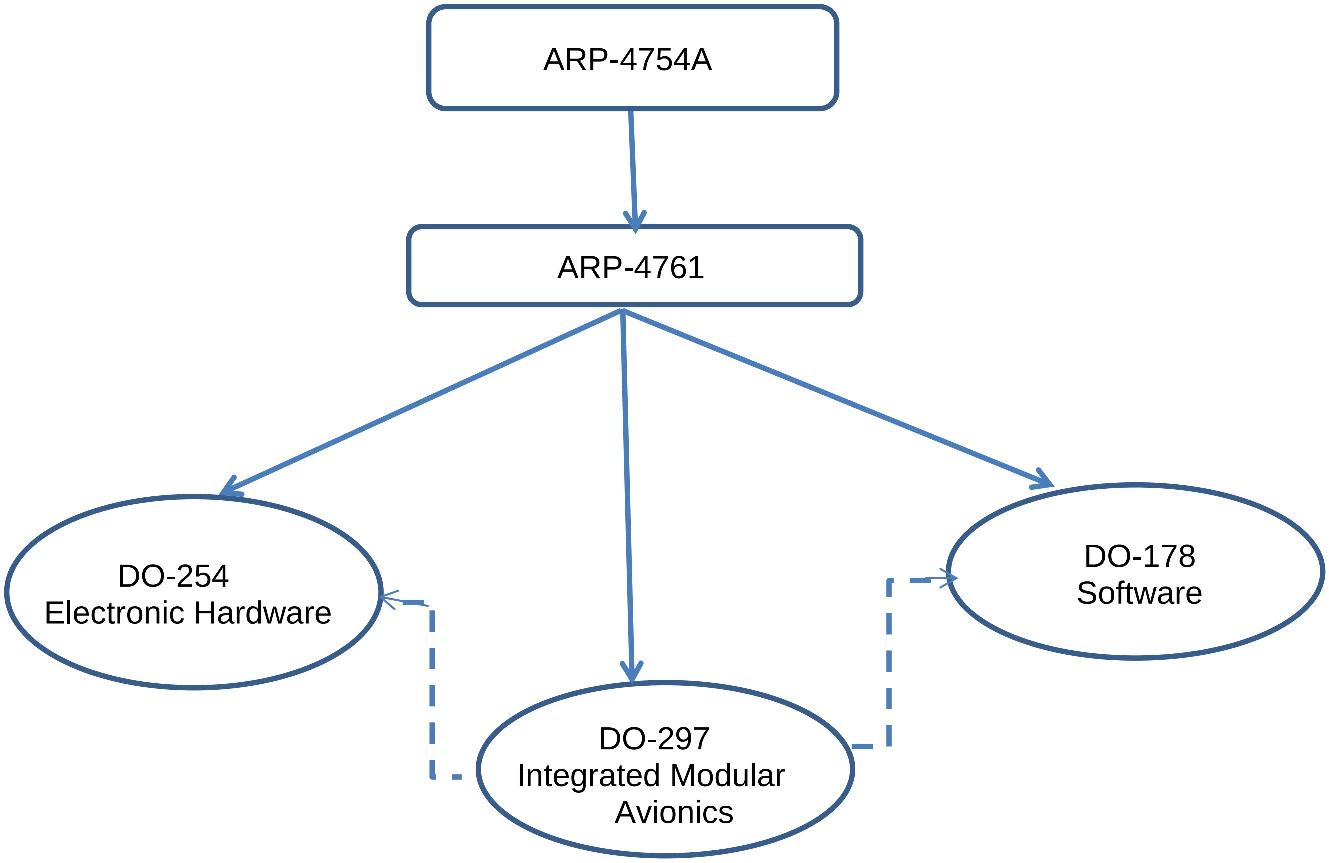


Figure A-1 Relationship of ARPs and Standards (DOs)

RELATIONSHIP AMONG AIRPLANE CLASSES, PROBABILITIES, SEVERITY OF FAILURE CONDITIONS, AND SOFTWARE AND COMPLEX HARDWARE DAL

Classification of Failure Conditions	**No Safety Effect**	**<----Minor----->**	**<----Major---->**	**<--Hazardous--->**	**< Catastrophic>**
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety	Large reduction in functional capabilities or safety	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to	Fatal Injury or incapacitation
Classes of Airplanes:	**Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development Assurance Levels (Note 2)**				
Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.
Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for Primary System (P) and Secondary System (S). For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.
Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.
Note 4: Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria.

Figure A-2 Reliability Targets versus DAL Safety Classes (reproduced from Ref. 7)

The notes to the table refer to classes of DAL. The requirements for Classes A, B, C, D, and E are defined in references 4 and 5 for hardware and software. For example, for level D devices RTCA/DO254 do not require a review of the life cycle data. Also note the table differentiates for the level of assurance between primary and secondary system (secondary system may require crew actions, i.e., manual operation of a diverse system). Note 3 also indicate that no single failure should result in catastrophic failure condition. Single failures also include potential for undetectable multiple failures and Common Cause Failures (CCFs) of redundant DI&C software and hardware. A secondary system diverse from that of primary system is usually relied upon in FAA but it requires manual actions.

Hardware: AC 23.13091E provides some specific recommendations for the types of analysis required for hazardous and catastrophic failure condition caused by hardware failures. The recommended analyses are both quantitative and qualitative. The analyses furthermore depend on the system complexity. Methods such as Fault Tree Analysis (FTA) supported by reliability estimates derived from service data are used for quantitative assessment. Human Reliability Analysis (HRA) in terms of crew and maintenance errors is also modeled. The equivalent of emergency procedures in airline industry is called AFM/AFMS (Airplane Flight Manual and Manual Supplements). AFM and availability of flight instrumentations are considered for estimating the crew failure rate. This is important especially for cases when failures of DI&C impact available information. Quantitative assessment shall be supported and be consistent with qualitative engineering analysis. In this regard, the following excerpts from reference 7 are noted below.

(1) For simple and conventional installations (that is, low complexity and similarity in relevant attributes), it may be possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for the assessment will be the degree of redundancy, the established independence and isolation of the channels, and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many airplanes may be sufficient when a close similarity is established regarding both the system design and operating conditions.

(2) For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may also be possible to assess a hazardous or catastrophic failure condition as being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. A high degree of similarity in both design and application is required.

AC 23.13091E recognizes that the accepted probability of failure for hazardous and Catastrophic conditions derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense, and specific studies are necessary to ensure that independence can either be assured or deemed acceptable. The recommended assessment of “common cause failures” is divided into three areas of study as noted in AC 23.13091E. These are:

(a) Zonal safety analysis. *This analysis has the objective of ensuring that the equipment installations within each zone of the airplane are at an adequate safety standard regarding design and installation standards, interference between systems, and maintenance errors.*

(b) Particular risk analysis. *Particular risks are defined as those events or influences outside the systems concerned (e.g., fire, leaking fluids, bird strike, tire burst, HIRF (High Intensity Radiative Field) exposure, lightning, uncontained failure of high energy rotating machines, etc.). Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects, or influences, which may violate independence.*

(c) Common mode analysis. *This analysis is performed to address other sources of common mode failures of the events that were considered in combination for a given failure condition. The effects of specification, design, implementation, installation, maintenance errors, manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered.*

Software: AC 23.13091E provides some specific recommendations for the types of analysis required for hazardous and catastrophic failure conditions caused by software failures (Levels A, B, and C). The requirements (or objectives) for each software level is discussed in DO-178. The level of effort to comply with the objectives of DO-178 will vary based on software criticality. The level of effort is also proportional to the size of the software under consideration. DO-178 defines five software levels, each related directly to the failure condition that can result from anomalous behavior of the software. For each software level a set of objectives must be met and verified. The number of these objectives depends on software level; for example, 71 objectives for level A and 26 for level D.

Similar to the guidance for hardware failure conditions, AC 23.13091E divides the software systems into simple and complex. Direct inspection and other direct verification methods capable of completely characterizing system performance and exhaustively test the software for detecting possible errors made during the design and development of system are considered appropriate for simple software.

For more complex or integrated systems, exhaustive testing may either be impossible because all the systems states cannot be determined, or it may be impractical due to the number of tests that must be accomplished. For these types of systems, compliance relies on diversity in software (MVDS). The software and complex hardware reliability approaches are graded (i.e., associated DALs). DALs should be determined by the severity of potential effects on the airplane in case of system malfunctions or loss of functions (i.e., depending on their risk contributions).

Safety Management System (SMS) includes formal methods for identifying hazards and mitigating risk, and promotion of a positive safety culture. SMS is built by structuring ~~your~~ safety management around four components: safety policy, safety risk management (SRM), safety assurance (SA), and safety promotion. The SRM component provides a decisionmaking process for identifying hazards and mitigating risk based on a thorough understanding of the organization's systems and their operating environment. SRM includes decision making for acceptance of risk during operation. SRM is also a design process, a way to incorporate risk controls into processes, products, and services or to redesign controls where existing ones are not meeting the safety objectives as detected by SA. SA and SRM perform two main functions; continuously monitoring and measuring safety performance of operational processes and attempt to maintain or improve the level of safety performance.

AC 120-92B [Ref. 8] provides a description of regulatory requirements, guidance, and methods of developing and implementing an SMS. It should be noted that SRM/SA process (or SMS process) is required by 14 CFR Part 5. Figure A-3 (duplicated from Reference 8) shows the safety management decision making processes (SRM and SA). SRM/SA process evaluates the risk of a finding and decides if the risk is acceptable. This is done by preparing a risk matrix, either in a qualitative or a quantitative manner. Acceptable regions of the risk matrix then are determined based on a set of criteria (e.g., tolerable risk criteria). There are some specific characteristics of risk matrix that are identified below:

1. The risk matrix is developed using the severity of the outcome (consequence) and probability of occurrence. Although the concept of risk as the product of consequence and probability is embedded in risk matrix, risk is not directly estimated. A risk matrix developed in this manner can provide a means to compare potential effectiveness of proposed risk controls and prioritize risks where multiple risks are present.
2. If the risk as identified in risk matrix is acceptable, then the system may be placed into operation and monitored in the SA process.
3. If the risk is not acceptable, risk controls must be developed, their effectiveness estimated and monitored in the SA process.
4. Chapter 4 of Reference 9 illustrate that the risk assessment of an event should consider specific conditions when the event occurred (rather than an average condition). It identifies for example the pilot fitness for duty (such as amount of sleep, feeling ill or feeling great), phase of flight (cruise, landing, etc.), weather conditions (e.g., visibility), and other important factors affecting pilot or system performance.

An example of qualitative risk matrix duplicated from AC 431.35-2A [Ref. 10] is provided below. Note that multiple severity index may be considered in such analysis (effect on operation, crew, public, and financial loss). FAA requires a three-pronged approach for accident prevention in RLVs (Reusable Launch Vehicles) and RVs (Reentry Vehicles) due to potential of accidents impacting public health and safety as well as property. The three safety-related elements reflected in the FAA's safety strategy for RLV and RV missions and licensing are as follows:

- Acceptable public risk as determined through a calculation of the individual and collective risk, measured by expected number of casualties.
- Logical, disciplined system safety process to identify hazards and to mitigate and control risks.
- Operational requirements.

FAA uses a systematic process for the identification and control of safety systems and their operation to ensure that the analysis results directed by AC 431.35-1 are maintained. The high-level process described in AC 431.35-2A is similar to FAA risk-informed approaches discussed in other ACs with the following differences.

1. Flight Safety Systems (FSS) limits or restricts the hazards to the uninvolved public by initiating and accomplishing a controlled ending to vehicle flight, thereby, preventing the vehicle from reaching a populated area in the event of a failure. Expendable launch vehicles launching from the United States typically use a flight termination system (FTS) as the FSS to end the flight whenever the launch vehicle strays outside of a predefined envelope.

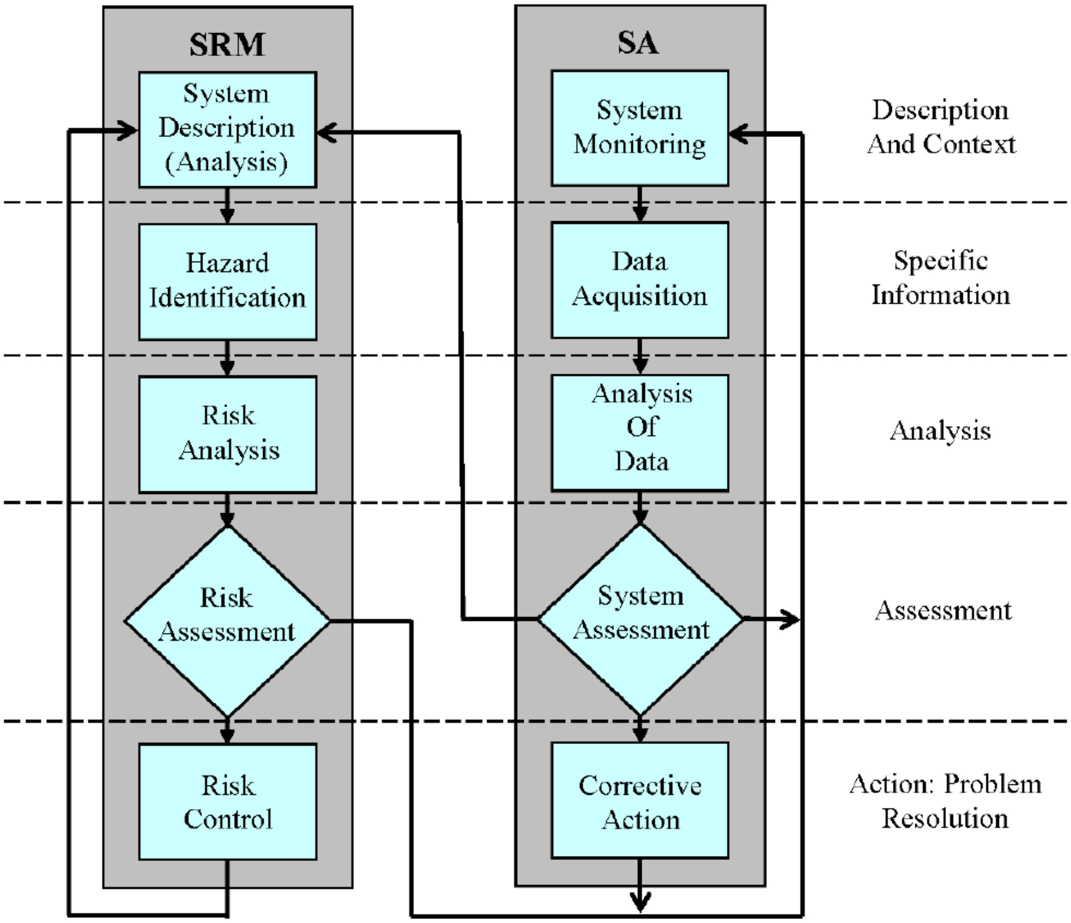
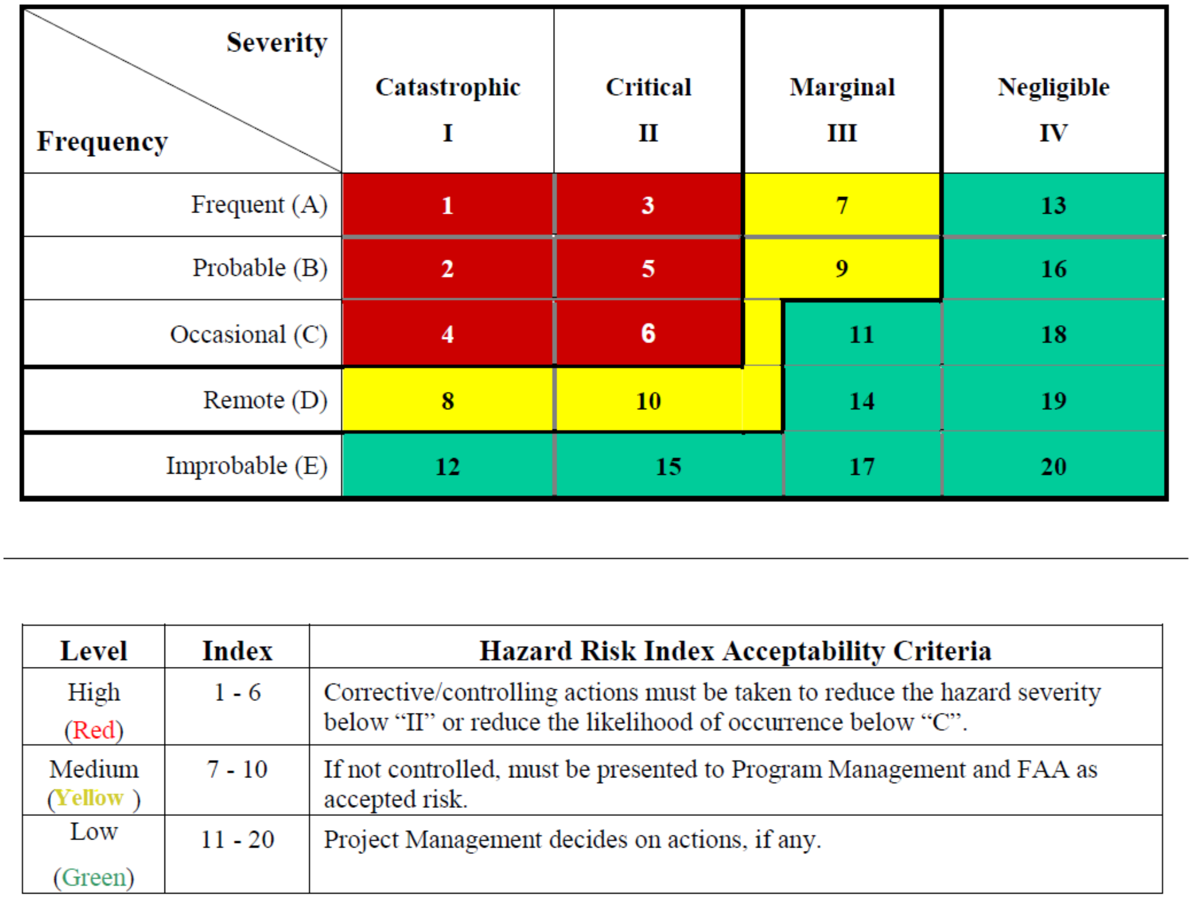


Figure A-3 Relation of SRM and SA (duplicated from AC 120-92B)



Severity Frequency	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)	1	3	7	13
Probable (B)	2	5	9	16
Occasional (C)	4	6	11	18
Remote (D)	8	10	14	19
Improbable (E)	12	15	17	20

Level	Index	Hazard Risk Index Acceptability Criteria
High (Red)	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below "II" or reduce the likelihood of occurrence below "C".
Medium (Yellow)	7 - 10	If not controlled, must be presented to Program Management and FAA as accepted risk.
Low (Green)	11 - 20	Project Management decides on actions, if any.

Figure A-4 Example of Risk Matrix (duplicated from AC 431.35-2A)

2. A flight hazard area analysis identifies any regions of land, sea, or air that must be monitored, publicized, controlled, or evacuated to control the risk to the public from debris impact hazards. The system safety process will identify when the public is potentially at risk based on safety-critical failure modes and events and if a flight hazard area analysis is necessary.

AC 431.35-2A includes specific quantitative criteria for hazard likelihood and severity. The hazard likelihood in this AC is somewhat different than criteria discussed in other FAA documents. This is shown below.

Table A-1 Hazard Severity

DESCRIPTION	CATEGORY	MISHAP DEFINITION
Catastrophic	I	Death to uninvolved public or safety-critical system loss.
Critical	II	Severe injury or illness to the uninvolved public, or major safety-critical system damage.
Marginal	III	Minor injury, illness, or safety-critical system damage.
Negligible	IV	Less than minor injury, illness, or safety critical system damage.

Table A-2 Hazard Likelihood

DESCRIPTION	LEVEL	INDIVIDUAL ITEM
Frequent **($X>10^{-1}$)**	**A**	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in any one mission.
Probable **($10^{-1}>X>10^{-2}$)**	**B**	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in any one mission.
Occasional **($10^{-2}>X>10^{-3}$)**	**C**	Likely to occur sometime in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in any one mission.
Remote **($10^{-3}>X>10^{-6}$)**	**D**	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in any one mission.
Improbable **($10^{-6}>X$)**	**E**	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in any one mission.

These differences could be justified based on the potential for public consequences (fatalities, injuries, and property damage) associated with LV/RLV accidents[26].

A.4.2 Risk-Informed Regulatory Practices of Chemical Sector

In the Clean Air Act Amendments of 1990, Congress required OSHA to adopt the Process Safety Management (PSM) standard (see OSHA 3132 [Ref. 11] and 3133 [Ref. 12]) to protect workers. Separately the Clean Air Act Amendment required EPA to protect the community and environment by issuing the Risk Management Plan Rule (RMP). In these documents OSHA identifies the process hazard analysis (PHA) as the cornerstone of any effective program for managing hazards. A PHA is an organized and systematic effort to identify and analyze the significance of potential hazards associated with the processing or handling of highly hazardous chemicals. A PHA provides information that will assist employers and employees in making decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. For a simple system that have been used over many years with little or no changes, such as a standard boiler or heat exchanger, a PHA checklist would suffice. For more complex system, the PHA is more involved and it must be documented and understood by the team members and reviewers. In general, PHA methodology is strongly dependent on engineering judgment to identify potential improvement in system design and operation. PHA also relies on FMEA evaluation to address the following items:

- Potential failure modes (i.e., open, closed, on, off, leaks, etc.),
- Consequence of the failure; effect on other components and effects on whole system,
- Hazard class, (i.e., high, moderate, low),
- Probability of failure,

[26] Although this is referenced by FAA, it could be applicable to NASA and perhaps future space force. It is currently issued for FAA.

- Detection methods; and
- Remarks/compensating provisions.

Multiple concurrent component failures (i.e., CCFs) are also included in the analysis, mainly based on analyses of past operational data and identification of associated causes. FTA may be used but generally in qualitative manner to identify the multiple component failures with significant impact on process operation or functional failures (such as generating minimal cut sets).

At the core of EPA regulatory compliance for chemical sector is Risk Management program (RMP). RMP guidance is designed to provide technical instructions on how to determine if a chemical facility is subject to 40 CFR Part 68 [Ref. 13], and how it can comply with it. Chemical facilities are categorized to three programs based on the specific characteristics of the facilities in 40 CFR Part 68. For example, the facilities closer to commercial nuclear power plant is characterized as program 3 when one considers the potential public consequences of an accident. The following subparts of 40 CFR Part 68 are pertinent to this study:

- Subpart B-Hazard Assessment
- Subpart D- Program 3 Prevention Program
- Subpart G – Risk Management Plan (RMP)

The focus of Subpart B, Hazard Assessment, is on developing offsite consequences under the worst case (upper bound) and alternative case (expected or likely case). Subpart B requires that the operator of the facility review and analyze the most recent accident histories in the past five years, and to show that operational or process changes that resulted from investigation of these accidents have been considered as a part of process design.

A major part of Subpart D for program 3 is the prevention program. Prevention program is a process hazard analysis. Subpart D recognizes that the process hazard analysis shall be appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process. In addition, it highlights the importance of detection methods such as process monitoring and sets emphases on control, instrumentation, alarms, interlocks, and specific purpose hazard detection hardware (such as hydrocarbon sensors for early warning system to mitigate or control releases). Operational practices to ensure systems and equipment (mechanical, electrical, I&C, etc.), including testing, maintenance, and inspection are discussed under a part entitled “mechanical integrity”.

Subpart G requires that the operator submit a single RMP document that includes the identification of stationary sources and regulated substances in the facility, the accidental release prevention and emergency response policies, the five-year accident history, the emergency response program and planned changes to improve safety.

The purpose of Risk-Based Process Safety-RBPS [Ref. 14] is to help organizations design and implement more effective process safety management system. The RBPS approach recognizes that all hazards and risks in an operation or facility are not equal; consequently, apportioning resources in a manner that focuses effort on greater hazards and higher risk is appropriate. This requires that the facility risk be understood and its relations to integrity and reliability of process safety systems and functions are delineated. It also requires an understanding of how the process safety and operational activities including safety culture within the organization can influence the integrity and reliability of process safety systems and safety functions, all the way to the facility risk.

Once hazards have been identified and associated risks have been analyzed, the acceptability of the risk must be judged. Acceptable risk or tolerable risk is defined in several different ways. For example, some chemical companies may judge a risk is acceptable if the system conforms to a minimum standard, such as a regulation or code. Other companies may require that risks meet internal tolerable risk criteria or even be reduced as low as reasonably practicable (ALARP). Some companies may judge certain consequences is to be unacceptable under any circumstances and require that the process be relocated or abandoned unless an inherently safer alternative can be found. This can be best illustrated by an example shown in RBPS using a qualitative risk matrix shown here in Table A-3. Immediate actions usually involve facility shutdown followed by modifications to reduce the frequency or the consequence to portion of the matrix that is acceptable. ALARP (As Low As Reasonably Practical) regions of the matrix refer to areas where improvement will be justified based on engineering practicality or the associated cost and benefit. The frequency associated with the risk is based on exposure period to risk and not the facility operating period. Finally, the portion noted as actions required at first opportunity generally refers to changes made at the next facility outage.

Table A-3 Example of Risk Matrix for Illustration Only

Frequency	Serious damage in immediate area	Serious damage inside a battery limit (a zone boundary)	Serious damage site wide	Serious damage offsite
More than 1 per year	ALARP	Actions required at first opportunity	Immediate	Immediate
Once every few year	ALARP	ALARP	Actions required at first opportunity	Immediate
Once in facility’s lifetime	No action required	ALARP	ALARP	Actions required at first opportunity
Not expected during the facilities lifetime	No action required	No action required	ALARP	ALARP

The most common risk-informed applications are SCAI (Safety Controls, Alarms, and Interlocks), asset integrity, and Management of Change (MOC).

The design and operation of SCAI relies heavily on the risk insights gained from Hazard Identification and Risk Assessment (HIRA). Early identification of potential loss events and analysis of their likelihood and consequence is essential to making process design changes to reduce the process risk. The initial process hazard shall be performed at early stages of design. As design progress further in its lifecycle, it would be harder to make inherently safer process design changes. Late stage analysis often results in SCAI being the only practical risk management solution.

Asset integrity helps ensure that equipment is properly designed and installed in accordance with specification and remains fit for use until it is retired. Asset integrity requirements and activities focus on safety critical components and systems that are important for preventing and mitigating catastrophic release of hazardous material or sudden release of energy. Qualitative risk matrix resulting from Hazard and Operational assessment (HAZOP) analysis is generally considered for identifying the safety critical SSCs (Systems, Structures, and Components) to be considered for asset integrity assessment. For I&C systems [Ref. 15] including software and digital hardware, Safety Integrity Level (SIL) classes as determined by IEC 61508, and life cycle in 61511, are used. A safety instrumented system (SIS) is one of the most important layers of protection against accidents and hazards in the process industries. Based on the SIL identification study, the SIL class for each critical loop is identified. Safety requirement specifications are prepared, and before finalizing procurement and implementation at the site, SIL verification of the identified SIL level is carried out, as per IEC 61508. Furthermore, SIL validation is carried out at the site for all SIL-certified loops.

The MOC process helps ensure that changes to a process do not inadvertently introduce new hazards or unknowingly increase risk of existing hazards. The MOC element includes a review and authorization process for evaluating proposed adjustments to facility design, operations, organization, or activities prior to implementation. This is done to make certain that no unforeseen new hazards are introduced and that the risk of existing hazards to employees, the public, and/or the environment is not unknowingly increased. Risk matrix is usually developed for each MOC. This could result in developing additional risk control measures to ensure that the MOC risk resides within the acceptable regions of the risk matrix. MOC process also requires risk metrics to be monitored. It also includes steps to help ensure that potentially affected personnel are notified of the change and those pertinent documents, such as procedures, process safety knowledge, and other key information, are kept up to date.

A.4.3 Risk-Informed Regulatory Practices of National Aeronautics and Space Administration (NASA)

To reduce the effort and better focus the resources, author privately communicated with a colleague; Dr. Zoran Musicki[27] of SAIC office of Johnson Space Center. Dr. Musicki provided much insightful information on what to review and provided supplemental information which has been incorporated throughout this Section.

The objectives of the NASA Safety Program are to protect the public from harm, ensure the safety of employees, and the overall success rate of missions and operations through preventing damage to high-value equipment, property and environment (both earth and extraterrestrial). NASA meets these objectives by (1) predicting safety performance and monitoring leading indicators, (2) through inspection and mishap investigations, (3) through a strong network of oversight and internal auditors including the Aerospace Safety Advisory Panel (ASAP), and (4) through prediction and management of risk. The ASAP reviews and evaluates program activities, systems, procedures, and management policies and provides assessment of these areas to NASA management and Congress. It is in this role that the ASAP provides independent advice on NASA safety issues to the Chief, Safety and Mission Assurance, and to the Administrator (https://sma.nasa.gov/codeq).

NPR 8715.3D [Ref. 16] emphasizes the importance or risk assessment, risk management, and risk acceptance in NASA decision making for Safety and Mission Assurance (SMA). Quantitative methods are generally used to evaluate probabilities, consequences, and

[27] Dr. Zoran Musicki, a senior PRA analyst at SAIC, Houston division on NASA contracts, currently working on Orion and Gateway projects.

uncertainties, whenever possible. Qualitative methods are used to characterize hazards and engineering evaluations including failure modes and effect analysis. The qualitative methods provide valuable input to the risk assessment and supporting information for decision making process. The results of the risk assessment along with the results of system safety analyses form the basis for risk-informed decision making. The concept of failure tolerance is also discussed in this NPR. Failure tolerance is the ability of a system to perform its function(s) or maintain control of a hazard in the presence of failures of its subsystems. Failure tolerance is accomplished through like or unlike redundancy (diversity). NPR 8715.3D also requires that sufficient safety margins under all conditions to be assured. Safety margins are the difference between as-built factor of safety and the ratio of actual operating conditions to the maximum operating conditions specified during design.

NPR 8715.3D also discusses the requirements for hazard analysis. Hazards analysis involves the application of systematic and replicable methods to identify and understand hazards, and to characterize the risk of mishaps that involve hazards. MIL-STD-882E [Ref. 17] describes the systems engineering approach to hazard analysis. NASA also requires that hazard analysis to document a characterization of the severity of the consequences associated with the accident scenarios (scenario-based modeling) that have been identified. This characterization is expressed quantitatively in the form of a set of numerical parameters that best represent the magnitudes and types of the adverse consequences. The possible consequences could include public safety, environmental contamination (for earth or other planetary bodies), or loss of astronauts, loss of flight system, etc.).

This document promotes risk-informed rather than risk-based decision making. It considers the use of probabilistic risk assessment as a complement for deterministic safety analyses and not a replacement. The deliberation that takes place before a decision is made utilizes the insights and results of both the qualitative "deterministic" analyses and the probabilistic risk assessment. Possible conflicts between the results shall be resolved during deliberation.

NASA requires RIDM throughout the design cycle, however, recognizes that at early stages of design, sufficient information may not be available to perform meaningful quantitative risk assessment. It therefore recommends a graded approach for RIDM at different stages of design as shown in Table A-4.

Table A-4 Graded Use of Risk Information and Insights

Ranking	**Scope (The level of rigor and design are commensurate with the level of design maturity)**
I	Probabilistic risk assessment supported by qualitative system safety analysis
II	Qualitative system safety analysis supplemented by probabilistic risk assessment where appropriate
III	Qualitative system safety analysis

Similar process for safety and risk reviews for design cycle are also applicable to design and operational changes (change reviews). This is done when systems are changed during their life cycle to enhance capabilities, improve safety, provide more efficient operation, and incorporate new technology.

NPR 8705.5A [Ref. 18] provides basic requirements for performing a probabilistic risk assessment (PRA) for NASA programs and projects. The technical details associated with performing a PRA for NASA can be found in NASA/SP-2011-3421 [Ref. 19].

NASA uses PRA results and insights for three main objectives:

(1) As a means to support the acceptability of design given it meets all other deterministic requirements, and
(2) As a means to support efficiency. For example, Appendix C of NPR 8705.5A states that; “Risk importance measures determined by the PRA can be used to optimize procedures and resource allocations during operation.”
(3) As a supporting tool for Human-Rating Certification which focuses on crew safety during mission (See NPR 8705.2C [Ref. 20]).

The requirements contained in NPR 8705.5A are similar to those of USNRC for use of PRA results, however the practices are not exactly the same. For example, some NASA practices are:

- The use of PRA at different level of complexity are mandated to the extent possible throughout the design, operation, and decommissioning (system/facility life cycle phases). It is stated that a well-designed PRA should be structured and developed incrementally to be suited to "grow" though the life-cycle phases

- Independent Peer Review (IPR) is generally carried out by a team of independent peers who were not involved in the study. The reviews are generally comprehensive but limited to high priority areas of PRA [ranking 1 PRAs; see NPR 7120.5 and NPR 8705.4].

The use of PRA results in quantitative risk-informed regulatory framework relies on common understanding of what is “sufficiently safe”. If there is no safety goal, PRA applications will be limited to PRA insights and relative comparison. When safety goals are not defined, alternative means of assurance could rely on qualitative criteria including redundancy, diversity, and safety margins; or quantitative criteria such as relative risk comparisons, and PRA generated risk importance measures. NASA has declared some specific numerical safety goals; for example for loss of crew for transportation system missions to the International Space Station, it uses the mission success probability of space shuttle at the end of its operational life. This will be discussed later as a part of NASA System Safety Handbook, Vol. 1, NASA/SP-2010-580 [Ref. 21]. NASA also relies on “as safe as reasonably practicable (ASARP)” concept. There are also several other numerical safety goals that have been accepted by NASA through consensus. These are generally based on comparison of what has been achieved at NASA missions. For example, for P(LOC); (loss of crew – meaning loss or debilitating injury to at least one crew member), the current consensus goal is something on the order of 1 in 200 mission. There is also Probability of Loss of Mission P(LOM) requirement for the Gateway lunar outpost (~on the order of 1 in 30 per year or over its 15-year lifetime). For the unmanned Orion missions (Artemis 1); the P(LOV) is targeted to be less than 1 in 100. It generally appears that NASA has circumvented defining a set of formal safety goal by allowing the responsible project managers and NASA headquarter to carefully determine their project safety goals based on comparison to what was achieved before.

NASA/SP-2010-576 [Ref. 22] discusses NASA’s approach to risk-informed decision making (RIDM). As stated in this document, the RIDM process addresses the risk-informed selection of decision alternatives to assure effective approaches to achieving objectives, and the CRM (Continuous risk management) process. It is important to note that RIDM is different than PRA applications discussed earlier under NPR 8705.5a, which were based on the risk insights (e.g., PRA importance measures and PRA relative prioritization). In RIDM a set of alternatives are determined, the associated risks are compared amongst them and against a set of safety goals. Selection of alternatives to be subjected to RIDM evaluation is done through deliberation and set of NASA specific performance commitments. The next step after selection of alternatives is developing PRA with sufficient level of details that allow alternatives to be compared with each other and against a set of goals and objectives (safety, technical feasibility/success probability, and cost/schedule objectives). NASA relies on variety of methods to probabilistically estimate the probability of success for the set of objectives of interest. The methods could be as simple as statistical estimation, knowledge-based extrapolation, sophisticated probabilistic simulations of deterministic models, and/or traditional PRA technics. Furthermore, uncertainties are explicitly considered within RIDM framework (i.e., allowing to estimate the probability that if alternative 1 is superior to alternative 2).

NASA/SP-2011-3421 [Ref. 19] develops the PRA procedure guide for estimating the probabilities associated with three specific objectives: Loss of Crew P(LOC), Loss of Vehicle (P(LOV), and Loss of Mission P(LOM).

NASA has several databases that can be relied on in supporting a NASA PRA. NASA also considers data from other industries such as those from nuclear power (e.g., EPIX/RADs) , Government-Industry Data Exchange Program (GIDEP), International data, and military handbooks on reliability predictions. A selection of NASA specific data collection systems includes:

- NASA incident reporting system including Problem Reporting and Corrective Action (PRACA)
- Center-specific Problem Reporting systems (to record pre- and operational anomalies)
- The Spacecraft On-Orbit Anomaly Reporting System (SOARS)
- The Problem Report/Problem Failure Report (PR/PFR) system
- Incident, surprise, and anomaly reports
- PRA and reliability analysis archives (e.g., Shuttle, ISS)
- Apollo Mission Reports
- The Mars Exploration Rover Problem Tracking Database
- Results of NASA expert elicitation

NASA proposes graded approach to HRA, starting with screening values followed by more detailed human reliability models commensurate with the risk importance of the action. The HRA guide heavily relies on THERP (Technique for Human Error Rate Prediction). Other methods such as CREAM (Cognitive Reliability and Error Analysis Method) and NARA (Nuclear Action Reliability Assessment) have been discussed as well. Screening values, shaping factors and even dependency values if available (e.g., THERP has them but CREAM does not) are tabulated for various tasks to help users.

NASA/SP-2011-3421 devotes Chapter 9 to software risk and reliability techniques. Software failures become more important for NASA environment since in some cases the timeframe available for a needed action is too short to permit a human (operator's) decision, the actuation of launch abort is determined by an intervention logic encoded in software. NASA utilizes several techniques that are linked together via one risk modeling framework which is referred to as "CSRM" (Context-based Software Risk Model). NASA also recognizes that software failures have contributed to a large fraction of major mission failures. Most of these mishaps caused by software faults have been the result of erroneous or incomplete design logic and/or functional specifications [i.e., can be classified as design error]. Furthermore, the more sophistication and integration introduced could result in a higher probability of logic errors and not meeting specifications. The CSRM model of software failure uses a logic and probabilistic formulation that can represent both “unconditional” and “conditional” software failures, as well as “recoverable” and “critical” ones. The CSRM methodology involves several steps which include: (1) identification of mission critical software functions, (2) Mapping of software-function to PRA event trees (3) developing the necessary models for each branch heading of the event trees down to the point where they can be either represented by basic events or quantified using dynamic models if needed. Once the models are structures then minimal cut sets can be generated which can help to define the condition for which the software reliability should be evaluated. It is our opinion that the application of such methodologies to nuclear power industries may require review of a large number of minimal cut sets.

Safety system handbooks (SSH) volumes 1 [Ref.21] and 2 [Ref. 23] focus on a holistic approach of identifying risk drivers, determining the controls directed toward preventing or mitigating the risk drivers, estimating the reliability and effectiveness of the controls. This holistic approach starts with hazard evaluation at early stages of design and continues through PRA models during various phases of design and modification. The SSH volumes 1 and 2 also briefly discuss the process of continuous risk management (CRM) during the operation and at the end of life decommissioning. The report advocates a proactive risk-informed approach to system safety. It discusses on how a risk-informed safety case (RISC) can be made. RISC includes making an explicit set of claims about the system(s), for example, the probability of an accident or a group of accidents is low compared to some standard or constraint. RISC claim is generally supported by a combination of qualitative and quantitative assertions. These could include: (1) representative operating history, (2) test results, (3) redundancy and diversity in design, (4) results of PRA analysis with clear declaration of assumptions and judgments used in the analysis. It generally suggests that there are three types of safety arguments that can be used jointly to support safety claims:

- Deterministic arguments: The application of predetermined rules to derive a true/false claim, given some initial assumptions (e.g., demonstration of compliance to a specification or safety requirement, assertion of known physical attributes such as physical laws and material properties, etc.).
- Probabilistic arguments: Quantitative statistical reasoning that establishes a probabilistic claim. For example, to substantiate a claim that the probabilities of loss of mission P(LOM) for some system is X, a probabilistic argument would reason statistically from evidence to quantify P(LOM). This generally translates in establishing a confidence level to the probabilistic estimate; for example, P(LOM)<X with ninety percent (90%) confidence.
- Qualitative arguments: Compliance with rules that have an indirect link to the desired attributes (e.g. compliance with industry standards, crediting of staff skill and experience, etc.).

NASA risk models sometimes referred to as Integrated Safety Analysis (ISA) is a complete set of analysis that starts at concept development and early design, the RIDM process during design, and in later phases during the design and implementation of CRM process. ISA is a proactive investigation into the ways that the system can fail, the likelihood of such failures, and their consequences. ISA includes both hazard-centric (e.g., external initiators) and non-hazard-centric (internal initiators) for identifying and characterizing potential accident scenarios. ISA process is used to determine the Safety Critical Items (SCI) during the design phase. ISA estimates the risk contribution from and performance of SCI with a high degree of confidence relying on technically defensible models and data. For noncritical or lower value systems, ISA relies on a graded approach based on their risk importance.

Some systems are designed to an initial minimum tolerable level of safety. However, they are expected to undergo safety growth during operation and ultimately meet stricter safety goals. In such cases, RISC must make a case that a program of continuous improvement is planned or in place that has a reasonable expectation of producing the requisite safety improvement. In other words, the RISC must provide a roadmap towards the satisfaction of the goal in terms of the plans, and commitments necessary for making that level of safety come true.

As a part of verification requirement, NASA requires that a set of measures of performance (MOPs) and technical performance measures (TPMs) to be specified. The MOPs and TPMs are used to judge the overall system safety. Typical MOPs for probabilistic requirements might include the computed probability of loss of the system and the mean failure rates of major subsystems or components for specified conditions. For deterministic requirements, the applicant may have to prove that the design meets the specification of tolerating two-failures; reliance on manual actions are credited. Proof of other design specifications such as environmental qualification (e.g., accelerations, temperature, pressure, radiation) should be supported by testing/analyses.

An important aspect of NASA program is the Continuous Risk Management (CRM) during the product life cycle. CRM is used to manage the aggregate risk that threatens the achievement of performance requirements. It does so base on a given set of performance requirements and decision maker risk tolerance levels, analyzing identified risk scenarios with possible mitigations and with follow-up monitoring, documentation, and communications.

The activities conducted as part of CRM comprise the following steps:

1. Identify: The purpose of the ‘Identify step” is to capture stakeholders’ concerns regarding the achievement of safety requirements and other performance requirements. These concerns are recorded as individual risks in a risk database. Each individual risk is articulated as a risk statement that contains a condition, a departure, an asset, and a consequence.

2. Analyze: The objectives of the “Analyze step” are to estimate the likelihoods of the departure and the magnitudes of the consequence for each individual risk, to evaluate the timeframe available for preventive or mitigative action, to characterize the uncertainties, to calculate the aggregate risks of not meeting specified thresholds and goals at different project milestones, and to determine which departure events and parameters within the models are the most important contributors to each aggregate risk (i.e., P(LOC), P(LOV), P(LOM), etc.).

3. Plan: The objective of the “Plan” step is to decide what action, if any, should be taken to reduce the safety risks and other mission execution domain risks that are caused by the aggregation of identified individual risks. The possible actions are: Accept, Mitigate, Watch, Research, Elevate, and Close.

4. Track: The objective of the “Track” step is to acquire, compile, and report observable data to follow the progress of the implementation of risk management decisions, and their effectiveness once implemented. The tracking task of CRM serves as a clearing house for new information that could lead to a new risk item, a change in risk analysis, a

change in a previously agreed-to plan, or the need to implement a previously agreed-to contingency.

5. Control: When tracking data indicates that a risk management decision is not impacting risk as expected, it may be necessary to implement a control action. Control actions are intended to assure that the planned action is effective. If the planned action becomes unviable, due either to an inability to implement it or a lack of effectiveness, then the Plan step is revisited, and a different action is chosen.

6. Communicate and Document: Well-defined, documented communication tools, formats, and protocols assure that individual risks are identified in a manner that supports the evaluation of their impacts on performance risk and that those that impact multiple organizational units (i.e., crosscutting risks) are identified, enabling the coordination of risk management efforts. Risk management decisions and their rationales are captured as part of the institutional knowledge of the organization.

Steps 1, 2, and 3 are developed by RIDM for planning and interface with CRM. The CRM process concentrates on steps 4, 5, and 6.

During the CRM process, there could be discovery of an emergent issue (new risk contributor) which could require rebaselining of the system safety cases. NASA Risk Management handbook: NASA/SP-2011-3422 [Ref. 24] provides guidance on how to resolve issues discovered during CRM. It recommends evaluating the criticality of individual discovered risks; by developing new risk scenarios or modifying the existing ones that can challenge the safety case assumptions and results. Proposing alternative fixes and prioritize them using a risk matrix type of approach supported by deliberation. Additional guidance is also provided for tracking and controlling the effectiveness of mitigations features; and for communicating and documenting all risk information necessary to an effective RM process.

For adverse situations that are outside the CRM purview; for example, poorly defined or missing requirements and requirements creep, it may be necessary to revisit RIDM and system engineering activities. The purpose here is to make sure that the RIDM and system engineering process lead to the derivation of all relevant performance requirements. The decision to rebaseline the requirements as a result of a finding through CRM, would be documented in the risk database and in the RRD (Risk Response Document) that it generates.

A.4.4 <u>Risk-Informed Regulatory Practices of Rail Industry (DOT/FRA)</u>

FRA (Federal Railroad Administration) utilizes the requirement for minimum performance standard (see 49 CFR part236.909 [Ref. 25]) for developing a product safety plan (PSP) to ensure that with a high degree of confidence that the introduction of the product will not result in risk that exceeds the previous condition. FRA meets this requirement relying on risk assessment. However, FRA proposes two types of risk assessments: full and abbreviated.

An abbreviated risk assessment is used if: (i) No new hazards are introduced as a result of the change; (ii) Severity of each hazard associated with the previous condition does not increase from the previous condition; and (iii) Exposure to such hazards does not change from the previous condition. A full risk assessment is required otherwise. A full risk assessment performed under this subpart must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This includes risks associated with the previous condition which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature (probability of occurrence or severity) is nonetheless affected by the change. The full risk assessment should estimate the total residual risk for the expected remaining life cycle after implementation. Risk levels must be expressed in units of consequences per unit of exposure. In all cases exposure must be expressed as total train miles traveled per year over the relevant railroad infrastructure. Consequences must identify the total cost, including fatalities, injuries, property damage, and other incidental costs, such as consequences of hazardous materials transport. The risk assessment must have a supporting sensitivity analysis. The analysis must confirm that the risk metrics of the system are not negatively affected by sensitivity analysis input parameters including, for example, component failure rates, human factor error rates, and variations in train traffic affecting exposure. In this context, "not negatively affected" means that the final residual risk metric does not exceed that of the base case or that which has been otherwise established through MTTHE (Mean Time to Hazardous Event) target. The sensitivity analysis must document the result for worst case failure scenarios and the most likely failure scenarios. We will discuss this later.

49 CFR Part 236 (Subparts H [Ref.26] & I [Ref.27] and Appendices B [Ref.28] & C [Ref.29]) refer to a set of references for deciding on acceptability criteria. These include the guidance provided in AREMA Manual[28], IEEE standards1483 and 1474 and MIL STD 882. FRA also uses international standards such as IEC 61508, EN50128[29], and EN50129.

AREMA document in specific plays an important role in deciding if the abbreviated risk analysis should be performed in lieu of full risk assessment. For example, it is stated that abbreviated risk assessment may be used to show that the requirements are met if the product is developed in accordance with:

(A) AREMA Manual Part 17.3.1 (Communications and Signal Manual of Recommended Practices, Recommended Safety Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications).
(B) AREMA Manual Part 17.3.3 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications).
(C) AREMA Manual Part 17.3.5 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications);

The various standards and AREMA manual were not reviewed and not considered within the scope of this project. These can be assumed to be like chapter 7 of SRP[30] guidance at NRC.

49 CFR Appendix B; risk assessment Criteria [(28)], requires that the risk metric shall be expressed with a high degree of confidence in appreciation of uncertainties involved. It is also stated that each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis.

[28] AREMA (American Railway Engineering and Maintenance-of-way Association) Manual Part 17.3.5 (Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications).
[29] EN50128 are for railway applications by CENELEC Standards. They relate to communication, signaling, and processing system.
[30] Standard Review Plan for the Review of Safety Analysis Report for Nuclear Power Plants: LWR Edition (NUREG-0800); Chapter 7 Instrumentation and Control USNRC.

For the full risk assessment, the total societal cost of the potential numbers of accidents assessed for both previous and new system conditions must be computed for comparison. An abbreviated risk assessment must, as a minimum, clearly compute the MTTHE for all the hazardous events identified for both previous and current conditions. The comparison between MTTHE for both conditions is to determine whether the product implementation meets the safety criteria as required by subpart H or subpart I of 49 CFR 236 as applicable.

49 CFR Appendix B also describes the scope of the risk analyses (all systems, functions, and human errors that must be modeled). The railroad risk assessment may use various techniques, such as reliability and availability calculations for subsystems and components, Fault Tree Analysis (FTA) of the subsystems, and results of the application of safety design principles as noted in Appendix C to this part.

For processor-based systems, it requires that MTTHE be calculated for each processor-based subsystems/components. The MTTHE calculation must consider the rates of failures caused by permanent, transient, and intermittent faults accounting for the fault coverage of the integrated hardware/software subsystem or component. Also included are some unavailability contributors such as Pre-planned (phased interval) maintenance, and restoration of the detected failures.

Software fault/failure analysis must be based on the assessment of the design and implementation of all safety-related software including the application code, its operating/executive program, COTS software, and associated device drivers, as well as historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The software assessment process must demonstrate through repeatable predictive results that all software defects have been identified and corrected by process with a high degree of confidence.

49 CFR Appendix B also requires the applicant to document all assumptions and results such that it can permit later comparison with in-service experience. For example, the railroad shall document any assumptions regarding software defects. The information then should be used to project the likelihood of detecting an in-service software defect. These assumptions shall be documented in such a form as to permit later comparisons with in-service experience.

Appendix C of 49 CFR 236 [Ref.29]; Safety Assurance Criteria and Processes, provides safety criteria, and processes that the designer must use to develop and validate the product that meets safety requirements of this part. Appendix C of 49 CFR 236 is a comprehensive document and it specifies all required design criteria and design features. A small set of these requirements have also direct relationship to risk assessment. These are noted below:

- The product must be shown to operate safely under single hardware failures as well as multiple hardware failures that may occur at different times but remain undetected (latent) and react in combination with a subsequent failure at a later time to cause an unsafe operating situation.
- There shall be no single point failures in the product that can result in hazards categorized as unacceptable or undesirable. Occurrence of credible single point failures that can result in hazards must be detected and the product must achieve a known safe state that eliminates the possibility of false activation of any physical appliance.
- If one non-self-revealing failure combined with a second failure can cause a hazard that is categorized as unacceptable or undesirable, then the second failure must be detected

and the product must achieve a known safe state that eliminates the possibility of false activation of any physical appliance.

- The issue of common Cause/Common Mode Failures (CCF/CMF) should be recognized as a part of multiple failures (see the last two bullets). The use of redundancy in which two or more elements perform a given function in parallel and when one (hardware or software) element checks/monitors another element (of hardware or software) to help ensure its safe operation are identified as CMF. Common mode failure relates to independence, which must be ensured in these instances. When dealing with the effects of hardware failure, the designer shall address the effects of the failure not only on other hardware, but also on the execution of the software, since hardware failures can greatly affect how the software operates.
- Design diversity and self-checking concept requires that all critical functions be performed in diverse ways, using diverse software operations and/or diverse hardware channels, and that critical hardware be tested with Self-Checking routines. Permissive outputs are allowed only if the results of the diverse operations correspond, and the Self-Checking process reveals no failures in either execution of software or in any monitored input or output hardware. If the diverse operations do not agree or if the checking reveals critical failures, safety-critical functions and outputs must default to a known safe state.
- N-version programming concept requires a processor-based product to use at least two software programs performing identical functions and executing concurrently in a cycle. The software programs must be written by independent teams, using different tools. The multiple independently written software programs comprise a redundant system and may be executed either on separate hardware units (which may or may not be identical) or within one hardware unit. A means is to be provided to compare the results and output states of the multiple redundant software systems. If the system results do not agree, then the safety-critical functions and outputs must default to a known safe state.

This appendix also specifies all the applicable standards such as IEC 61508, EN series, IEEEs, and AREMA as discussed earlier.

A Practical Risk Assessment Methodology for Safety-Critical Train Control System [Ref. 30] formalizes the practical risk assessment methodology (PRAM) for railroad industry. It provides examples and detail discussions on hazard identification, use of traditional PRA methods such as ET/FTA for scenarios development, use of historical data for estimation and quantification, and finally consequence aggregation on a monetary basis (including fatality and injury cost). These methods are similar to what generally have been used in NRC. The report does not discuss the specific issues associated with software and hardware reliability. However, it appears they significantly rely on reliability guidance and risk reduction factors (for CCF/CMF) used in IEC 61508 like other industries. Furthermore, there is no clear demarcation in the report between the abbreviated and full risk analysis as required by FRA regulation discussed earlier.

The report discusses the use of cumulative risk (aggregated over all hazards and scenarios) for RIDM on accepting a design. Simply stated, if the cumulative risk estimated using the acceptable methods that comply with all prescriptive requirements is below a baseline value, then the design is accepted. The baseline value is generally based on the risk associated with the existing design; evaluated using a detailed risk assessment methodology supported by data. When such information is not available an agreed upon tolerable risk by DOT/FRA will be used as the base value. This document (PRAM) does not address the issue of uncertainty. It does not include all risk-informed decision processes during design such as determination of safety-critical systems (hardware and software). These issues however have been discussed in other DOT/FRA references as discussed here.

DOT/FRA relies on standards such as IEC 61508 for DI&C systems. FRA utilizes risk matrix for most of decisions that must be made during design stage.

A.5 SUMMARY OF REGULATORY FRAMEWORK IN SELECTED FOUR INDUSTRIES

This section summarizes discussions provided in Sections A.3 and A.4 for the four industrial sectors, with a focus on the use of risk insights and risk results, for risk-informed regulatory framework. These summaries are furthermore focused to the extent possible on risk informing DI&C. A table was also developed for each industry to guide the discussion. This table consists of rows identifying the important elements of risk informed decision making for risk-informing of DI&C systems. These summaries are at a high level to maintain their generic nature. The table focuses on three major areas; (1) Risk-informed regulatory activities in design such as SSC (System, Structure and Components) classification, (2) PRA tools, method, and data to support risk informed regulatory activities, and (3) Risk-Informed Operational Safety and Reliability program (OSRRP). OSRRP includes all regulatory activities during operation (i.e., after design completed) to ensure that the risk controls are effective in maintaining acceptable risk levels. OSRRP includes oversight and monitoring program, significant event assessment (including precursor studies), safety risk management, safety assurance, continuous risk management, etc. All four industries that were reviewed as a part of this study, have similar risk-informed regulatory framework; like SMS process, although they may have been referred to by different names. SMS also includes elements similar to NRC programs such as Design Reliability Assurance Program (DRAP/RAP), Maintenance Rule (MR), operational event assessment and feedback (e.g., Bulletins, Generic letters, and generic issue management system), and risk informed changes during operation such as risk informed technical specifications.

A.5.1 <u>Summary of Risk-Informed Regulatory Framework for Civilian Aviation Industry (DOT/FAA)</u>

DOT/FAA utilizes the risk-informed results and insights during the design, licensing, and operation of civilian airplanes. Qualitative and some quantitative risk results are incorporated into a risk matrix framework and are used for determining safety critical SSCs. Risk insights are also incorporated in DID (Defense-in-depth) using redundancy and diversity concept for various accident sequences. Risk-informed decision making (RIDM) is generally used when an issue arises during operation. Quantitative risk assessment (QRA) is used for RIDM and the results are compared to estimates available for rate of accidents per flight hour from the most recent data. These rates are categorized based on phase of flight, failed systems, and the number of fatalities.

FAA has a rich environment for failure data which are used as a part of QRA. FAA also utilizes both traditional PRA methods such as ET/FTA and some dynamic methods such as Markov modeling. We could not identify any specific document that explicitly addresses uncertainties in QRA. Uncertainties might have been addressed qualitatively and through sensitivity analyses by some guidance documents that we were not able to identify.

CCFs is addressed for both software and hardware using prescriptive requirements; driven by risk insights and past histories of failures, including identification of past lessons (i.e., good practices.). A graded approach is generally used based on the complexity of the software or hardware system. For example, for simple software that can be exhaustively tested, the CCF requirements focus on testing adequacy to ensure independence without a requirement for installing a diverse system. For those systems, when independence cannot be assured, diverse and backup systems are considered consistent with their DAL specifications (determined by risk matrix at design stage). Such systems are sometimes referred to by FAA as complex or integrated system. FAA also heavily relies on diagnostic and monitoring systems for revealing failures (fault coverage) and redundancy and diversity including MVDS (multi-version dissimilar software) for failure prevention.

FAA requires the design to tolerate multiple failures either caused by CCF or by aggregation of several failures that cannot be individually detected. The extent of design tolerance against multiple failures for a system commensurate with its DAL specification. This generally leads to a design with some degree of diversity to protect against CCF of software and hardware.

The safety during operation is maintained through SMS process. SMS process first evaluates the risk of a finding through inspection, accidents and events, or performance indicators. This is done by preparing risk matrix; either a qualitative or quantitative, and determination of the acceptable region in the risk matrix. If the risk resides in regions of risk matrix that requires additional controls, the controls are specified, and their combined potential effectiveness is evaluated through risk matrix (changes in design or operation). Once placed into operation it will be monitored in the SA (Safety Assurance) process. Changes in design and operation could also take place by other factors, industry feedback or changes in requirements,

In addition to SMS system, all flights accidents will be reported and examined in a detailed fashion by NTSB (National Transportation Safety board).

The generic table includes the summary of the risk-informed regulatory treatments of various challenging issues pertinent to DI&C is provided for DOT/FAA in Table A-5. All information included in this table is from the discussion provided in Section A.4 and the associated references.

Table A-5 Summary Table for Risk-Informed Regulatory Activities Pertinent to DI&C of DOT/FAA

Technical & Regulatory Challenge	**Summary for DOT/FAA Regulatory Framework**
Risk Management System and risk-informed regulatory framework for design acceptance	
Risk Management system and risk-informed regulatory framework for design acceptance includes:	The decision measures are based on occurrence probability and consequence in the form of risk matrix. Several different consequences are generally considered. A single value for risk is not directly used (Risk Matrix is used). All decisions are made based risk contribution (surrogate to Fussell Vesely (FV) measure). The two major decisions made during design are: 1. SSC Classification at Design stage This is based on qualitative and quantitative evaluation of occurrence probability and consequence. This is generally done by developing risk matrix at various stages of design; starting with qualitative risk matrix based on Preliminary Hazard Assessment to quantitative risk matrix using formal PRA methods (see AC 23.13091E section 4.1). 2. Redundancy, Diversity, and Defense in depth (DID) Redundancy is decided upon using both qualitative and quantitative risk matrix (see the examples provided earlier). DID

Technical & Regulatory Challenge	**Summary for DOT/FAA Regulatory Framework**
	and diversity are also handled through risk matrix with some consideration on system complexity. See the discussion below on Software CCFs for complex system when exhaustive testing and verification is not possible.
Quantitative and qualitative criteria (Safety goals)	The qualitative and qualitative goals are defined specific to the class of airplanes and based on risk matrix (occurrence probability and severity/consequence). We did not find any specific cumulative safety goal criteria. There are however some estimates available for rate of accidents per flight hour. These rates are categorized based on phase of flight, failed systems, and the number of fatalities. Comparative analyses to these targets are generally made to address the cumulative risk effect.
Related to Risk Model and Data as it Pertains to DI&C Systems	
Failure Data	Rich environment; lots of service data on hardware failure, crew maintenance errors, and pilot errors. A detailed accident database including the investigation reports produced by NTSB is also available. There are some indications that FAA has strong Human Reliability Analysis Program, but it was not reviewed.
Common Cause Failures:	1. Software CCFs For simple and conventional installation perform exhaustive testing/inspection. Maintain redundancies as required by hardware design to comply with risk matrix. For complex system or integrated system, when independent cannot be ensured, diverse systems including MVDS should be considered according to risk matrix and DAL specification. 2. Hardware CCFs The recommended assessment of “common cause failures” is divided into three areas: Zonal safety analysis, external and environmental stressors, and through common mode matrix evaluation. These are done in addition to quantitative PRA results.
Uncertainty Analysis	Generally, not addressed explicitly. However, it is implicitly addressed by two different methods. (1) the thresholds in Risk Matrix are determined with some appreciation of the magnitude of uncertainty, and (2) limited sensitivity analysis of embedded assumptions
Risk Analysis Methods used	All conventional methods such as Hazard and Operational assessment (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagram (ESD), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments. Some dynamic methods such as Markov modeling is also used to capture the risk during flight phase transitions.

Technical & Regulatory Challenge	**Summary for DOT/FAA Regulatory Framework**
Operational Safety & Reliability Program (OSRRP)	
Safety Management System (SMS) for DOT/FAA	The SMS process first evaluates the risk of a finding through inspection, accidents and events, or performance indicators. This is done by preparing risk matrix; either a qualitative or quantitative, and determination of the acceptable region in the risk matrix. If the risk is identified is in regions of risk matrix that requires additional controls, the controls are specified, and their combined potential effectiveness is evaluated through risk matrix. Once be placed into operation it will be monitored in the SA (Safety Assurance) process. If the risk as identified in risk matrix is acceptable then the system may be placed into operation without change but it will be monitored in the SA process since it constituted a significant event (possibly minor risk increase). It is important to note that the risk assessment for SMS considers specific conditions when the event occurred (rather than an average condition). It identifies for example the pilot fitness for duty (such as amount of sleep, feeling ill or feeling great), phase of flight (cruise, landing, etc.), weather conditions (e.g., visibility), and other important factors affecting pilot or system performance. It is therefore expected to be different than average risk estimate done as a part of design.

A.5.2 Summary of Risk-Informed Regulatory Framework for Chemical Industry

Chemical sector practices are risk informed and relies on Risk Management program (RMP). RMP guidance is designed to provide technical instructions on how to comply with the requirements in 40 CFR Part 68. The following subparts of 40 CFR Part 68 are pertinent to high risk chemical facilities (program 3):

- Subpart B-Hazard Assessment
- Subpart D- Program 3 Prevention Program
- Subpart G – Risk Management Plan (RMP)

Most of the systems in chemical sector and their associated controls have changed little over time (relief valves, heat exchangers, evaporators). Chemical industry has a rich experience database and an impressive compilation of lessons learned. It is also important to note that they started using the DI&C systems almost three decades ago. The qualitative risk analysis is limited mainly to HAZOP, LOPA (Layer of Protection Analysis), and some ETA, and FTA evaluation. Most of the innovations are in process control and automation. Chemical industries use Risk Matrix plus the use of SIL classes and requirements for design, safety, and reliability of DI&C. The chemical sectors per EPA requirements perform the worst case and most likely analysis for catastrophic accidents (including the consequences of accidents). Uncertainties are implicitly addressed in consequence analysis (worst case and best-case analyses). For DI&C systems reliability bounds are defined in IEC 61508. CCFs are controlled by considering all controlling features designed in the systems and operation (redundancy, early diagnosis, fault tolerance features, diversity in design, and segregation in operation & maintenance). A case specific CCF probability is estimated using the risk reduction factors (RRFs). The basis for these risk reduction factors were not reviewed in detail. For the DI&C systems, the RRFs however derived mostly from IEC 61508. Chemical plants also rely heavily on operational feedback to improve safety. They are usually equipped with strong programs for performance indicators, accident investigations (including CSB examination), and measurements of large number of risk metrics.

The generic table and summary of the risk-informed regulatory treatment of various challenging issues pertinent to DI&C is provided for Chemical Industry in Table A-6.

Table A-6 Summary Table for Risk-Informed Regulatory Activities Pertinent to DI&C of Chemical Industry

Technical & Regulatory Challenge	Summary for Chemical Sector Regulatory Framework
Risk-informed regulatory framework for design acceptance and operational safety management system	
Risk Management system and risk-informed regulatory framework for design acceptance includes:	Risk insights and results gained from Hazard Identification and Risk Assessment (HIRA) are used against tolerable risk criteria using the risk matrix concept to identify when the existing design and operational practices must be enhanced. The Chemical plants also have to defend against the past operational mishaps (they are required to review five-year of major accident history and defend against them during design). Chemical industries use Risk Matrix and deterministic and prescriptive instructions for their regulatory framework during design. Specific to DI&C, they use a combination of Risk Matrix plus the use of SIL classes and requirements for design (see Section A.4.1; Figure A-4 and the discussion on AC 431.35-2A). Chemical industries rely on accident investigations (including CSB examination) and measure a large number of parameters and risk metrics for monitoring.
Quantitative and qualitative criteria (Safety goals)	Acceptable risk or tolerable risk is defined at minimum by the prescriptive requirements. Internally defined TR (tolerable risk) and sometime concepts such as low as reasonably practicable (ALARP) are implemented.
Related to Risk Model and Data as it Pertains to DI&C Systems	
Failure Data	Rich environment; lots of service data on hardware failure, crew maintenance errors, and pilot errors. Good and detail accident database including the investigation reports produced by CSB (Chemical Safety Board). Several databases such as Process Equipment Reliability Database (PERD). Industry wide generic reliability and CCF data for SIL certified hardware and software.

Technical & Regulatory Challenge	**Summary for Chemical Sector Regulatory Framework**
Common Cause Failures:	1. Software/hardware CCFs reduction practices Chemical sectors use the LOPA method and other engineering qualitative methods to identify the potential for CCF; they consider an Independent Protection Layer (IPL). Common cause failure is a significant issue with programmable controllers, since so many control tasks reside in the same equipment. Multiple tasks can be affected by a single equipment failure due to software, or configuration faults due to single human error. When integration cannot be avoided, use of diverse software, hardware, and interfaces for the safety system to reduce the risk of systematic and common cause failures are utilized. For integrated equipment performing both process- control and safety applications, functional separation should ensure that a failure of the process control system cannot cause a failure of any safety functions. Although the architecture is often marketed as a single manufacturer solution, the functionality can be achieved with diverse technologies (e.g., two controllers or a hardwired system and a controller) and with diverse manufacturers (i.e., two different controllers). Consideration should be given to diversity of the equipment used for the process control and safety systems. Use of diverse logic solver technologies can reduce the likelihood of common cause failures and systematic failures. Segregation of redundant process control SSCs and signals to redundant modules has been proven to increase the availability of the process control system by making it more tolerant to CCFs. The engineered features may involve using fault tolerant architectures, implementing diagnostics that switch operation to back-up equipment, or designing the system to fail to the safe state when failure is detected. 2. CCF estimates/ evaluation Chemical Sector generally applies a method such as the one described in IEC 61508-6 Annex D to estimate the value of β factor. A case specific CCF probability is estimated using the risk reduction factors (RRFs). The basis for these risk reduction factors was not investigated in this study. IEC 61511-1 [2015] has included evaluation of the common cause for SCAI layers. Once the RRF requirement is greater than 10,000, the analysis needs to quantitatively estimate the systematic contributions to CCFs.
Uncertainty Analysis	Uncertainties are implicitly addressed in consequence analysis (worst case and best-case analyses) and the reliability bounds as defined in IEC 61508.
Risk Analysis Methods used	All conventional methods such as Hazard and Operational assessment (HAZOP), Layer of Protection Analysis (LOPA),

Technical & Regulatory Challenge	**Summary for Chemical Sector Regulatory Framework**
	Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments are used.
Operational Safety & Reliability Program (OSRRP)	
Operational Safety Management	The risk management plan at design includes: 1. The accidental release prevention and emergency response policies at the stationary source. 2. The stationary source and regulated substances handled. 3. The general accidental release prevention program and chemical-specific prevention steps. 4. The five-year accident history. 5. The emergency response program. 6. Planned changes to improve safety. The most common applications are risk informed SCAI (Safety Controls, Alarms, and Interlocks), asset integrity, and Management of Change (MOC). Risk insights and results gained from Hazard Identification and Risk Assessment (HIRA) are used against tolerable risk criteria using the risk matrix concept to identify when the existing design and operational practices must be enhanced. The Chemical plants also rely heavily on operational feedback to improve safety. They usually equipped with strong programs for performance indicators, accident investigations (including CSB examination), and measurements of large number of risk metrics. The risk-informed insights are gained from experience for most of the conventional systems, the use of standards (e.g., SIL certified SSCs) are generally used to meet compliance. Chemical plants also rely heavily on operational feedback to improve safety. They usually equipped with strong programs for performance indicators, Chemical plants also rely heavily on operational feedback to improve safety. They usually have a strong program for performance indicators, accident investigations (including CSB examination), and measurements of large number of risk metrics.

A.5.3 Summary of Risk-Informed Regulatory Framework for National Aeronautics and Space Administration (NASA)

NASA risk informed framework consist of four elements. These are: (1) predicting safety performance and monitoring leading indicators, (2) through inspection and mishap investigations, (3) through a strong network of oversight and internal auditors including the Aerospace Safety Advisory Panel (ASAP), and (4) through prediction and management of risk. NASA's risk-informed practices follow generally the same concept as Nuclear Regulatory commission. NASA also relies on both deterministic and probabilistic risk insights. The deterministic criteria are based on defense in-depth, sufficient safety margins, and tolerance for failures. NASA also heavily relies on the process of CRM during the operation and at the end of life decommissioning. This process is like SMS process discussed for FAA. There is also large overlap of PRA techniques and data between NASA and NRC. NASA's probabilistic criteria are based on the past accidents. These probabilistic criteria/goals will change as the design improves and accident rates drop. NASA use of PRA for design acceptance and identification of safety critical items heavily depends on maturity of the PRA and design. During operational phase of space systems, such as deciding if a mission is a “go” or “no-go” is based on mission specific PRA results. PRAs are also used to help choosing the best candidate among several possible alternatives and justifying design or operational changes and enhancements.

Similar to NRC, NASA utilizes all conventional methods such as Hazard analysis, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments. NASA also uses more advanced dynamic models when necessary. NASA utilizes several techniques that are linked together via one risk modeling framework which is referred to as “CSRM” (Context-based Software Risk Model). Under CSRM software failures are considered condition dependent. The conditions are defined by PRA models and software functions are mapped to event trees. NASA performs risk assessment and considers both internal failures as well as those failures caused by external stressors (Internal and external initiators). NASA approach to uncertainty analyses is similar to USNRC. It accounts for parametric uncertainties in an explicit manner. NASA uses deterministic criteria such as safety margins, and Defense in-depth for other sources of uncertainties in addition to performing risk-based sensitivity analyses.

NASA relies on both industry generic data (including those from US-NRC) as well as NASA specific data (see the table A-7 below for detail). We could not find NASA specific database for CCF.

Table A-7 below summarizes major NASA practices that are relevant to risk-informed regulation.

Table A-7 Summary Table for Risk-Informed Regulatory Activities Pertinent to DI&C of National Aeronautics and Space Administration (NASA)

Technical & Regulatory Challenge	**Summary for Chemical Sector Regulatory Framework**
Risk-informed regulatory framework for design acceptance and operational safety management system	
Risk Management system and risk-informed regulatory framework for	A combination of risk-informed, and general deterministic design criteria is implemented. The deterministic design criteria are similar to NRC's defense in depth, safety margins, and single failure criteria tolerance (for some critical subsystems

Technical & Regulatory Challenge	**Summary for Chemical Sector Regulatory Framework**
design acceptance includes:	they require two-failure tolerance but crediting the human actions). The use of risk-informed decision-making using PRA varies depending on the maturity of design and the PRA. For example, PRA is less relied on at the early stages for defining safety critical equipment and systems. However, as the PRA and design matures the role of PRA is increased.
Quantitative and qualitative criteria (Safety goals)	NASA has declared some specific numerical safety goals; for example, for loss of crew transportation system missions based on the mission success probability achieved in the past (generally at the end of life when the design and operation was fully matured). NASA also relies on as safe as reasonably practicable (ASARP). In addition, there are several informal numerical safety goals that have been accepted by NASA through consensus and comparison of what has been achieved before.
Related to Risk Model and Data as it Pertains to DI&C Systems	
Failure Data	NASA relies on both industry generic data as well as NASA specific data. A selection of NASA specific data collection systems includes: •NASA incident reporting system including Problem Reporting and Corrective Action (PRACA) • Center-specific Problem Reporting systems (to record pre- and operational anomalies) • The Spacecraft On-Orbit Anomaly Reporting System (SOARS) • The Problem Report/Problem Failure Report (PR/PFR) system • Incident, surprise, and anomaly reports • PRA and reliability analysis archives (e.g., Shuttle, ISS) • Apollo Mission Reports • The Mars Exploration Rover Problem Tracking Database • Results of NASA expert elicitation NASA uses variety of HRA models and quantification techniques including THERP to address the human error probabilities for all human interaction with DI&C systems including manual actuation of diverse systems (Chapter 8 of NASA-SP-2011-3421). It also appears that NASA relies on industry wide including the NRC and international database on generic CCF data (no specific database was found). Aerospace Safety Advisory Panel (ASAP) plus the precursor program also plays an important role in evaluating findings from inspections, incidents, and accidents.

Technical & Regulatory Challenge	Summary for Chemical Sector Regulatory Framework
Common Cause Failures:	Similar to approach currently used at USNRC. No specific discussion on modeling and data for evaluating CCF contributions for DI&C was found. NASA believes most of the residue errors left in software are due to design and specification errors, so the software failures are highly dependent. NASA relies on diverse manual actions and if possible, on abort systems to reduce the risk associated with software CCF.
Uncertainty Analysis	Approach is similar to USNRC, Accounts for parametric uncertainties in an explicit manner. Relies on deterministic criteria such safety margins, Defense in-depth, etc.) for other sources of uncertainty. PRA based sensitivity analyses are also used to highlight most important uncertainty contributions.
Risk Analysis Methods used	All conventional methods such as Hazard analysis, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments are used. NASA also uses more advanced dynamic models when necessary. NASA utilizes several techniques that are linked together via one risk modeling framework which is referred to as "CSRM" (Context-based Software Risk Model). Under CSRM software failures are considered condition dependent. The conditions are defined by PRA models and software functions are mapped to event trees.
Operational Safety & Reliability Program (OSRRP)	
Operational Safety Management	NASA has formal continuous risk management (CRM) program throughout the product life cycle. NASA requires that a set of measures of performance (MOPs) and technical performance measures (TPMs) to be specified and tracked. The MOPs and TPMs are used to judge the overall system safety. Typical MOPs for probabilistic requirements might include the computed probability of loss of the system and the mean failure rates of major subsystems or components for specified conditions. When a risk deviation or an emergent issue is discovered by CRM, there would be a formal program for justifying proposed resolutions, implementing it, and monitoring its effectiveness.

A.5.4 Summary of Risk-Informed Regulatory Practices of Rail Industry (DOT/FRA)

A limited number of documents were reviewed for DOT/FRA regulatory framework with a focus on PTC system. DOT/FRA has used risk/reliability insights in developing the prescriptive requirements and relies on quantitative risk assessment results for acceptance. DOT/FRA requires abbreviated risk assessment in lieu of full risk assessment when the change is not expected to distort the risk. This is done to ensure efficiency and not to allocate unnecessary resources. DOT/FRA relies heavily on standard and guidance. Some of these standards and guidance are risk-informed (either quantitatively or qualitatively). Examples of such standards/guidance are AREMA manual, IEC 61508, and MIL-STD 882C. Regulatory requirements to protect against CCF/CMF are experienced driven and prescriptive. It relies on redundancy and diversity including N-version software techniques. The risk and reliability insights are incorporated via the use of IEC 61508 as recommended by the regulation. Risk analysis is quantitative and conventional risk analysis methods such as FTA/ETA are used. PTC is a new system and does not have accumulated sufficient reliability data. Generic reliability data from other applications and manufacturer data are generally used to support quantitative risk analysis. Uncertainties are addressed by requiring the applicant to provide an upper bound estimate and a high confidence mean estimate of risk. They also require sensitivity analysis to make sure that the upper bound is reasonable. There is no requirement for the applicant to use the risk analysis during the design process. Risk results and insights are used after design but before installation for acceptance decision. DOT/FRA has programs similar to operational risk management (called Risk Reduction Program). Risk Reduction Program is not specific to PTC and it was not examined here. Table A-8 below summarizes major DOT/FRA practices that are relevant to risk-informed regulation.

Table A-8 Summary of Risk-Informed Regulatory Framework for Federal Rail Industry (DOT/FRA)

Technical & Regulatory Challenge	Summary for Rail Sector Regulatory Framework
Risk-informed regulatory framework for design acceptance and operational safety management system	
Risk Management system and risk-informed regulatory framework for design acceptance includes:	Use of risk insights during the design process are mainly prescriptive (e.g. Single failure criteria, redundancy, and diversity). There is implicitly some reliance on quantitative risk insights when using standards such as IEC 68015. There is no requirement for the applicant to use the risk analysis during the design process. Qualitative hazard analysis and use of risk matrix could be used if needed. Risk results and insights are used after design but before installation for acceptance decision.
Quantitative and qualitative criteria (Safety goals)	Baseline criteria for a new product are determined either by using the performance of the existing (old) product if available, or the use of tolerable performance baseline. Tolerable risk is determined based on what is practical and cost efficient. It appears that abbreviated risk analysis is performed first before deciding on full risk analysis. For abbreviated risk analysis Mean Time to Hazardous Event (MTTHE) is used for risk-informed decision making. For full risk analysis, the criteria

Technical & Regulatory Challenge	Summary for Rail Sector Regulatory Framework
	are based on cumulative risk, where the consequences are expressed in an equivalent monetary value.
Related to Risk Model and Data as it Pertains to DI&C Systems	
Failure Data	This review focused on Positive Train Control System, fairly a new system with little or no data. Manufacturer data and generic data from IEC 68015 or MIL-STD could be used.
Common Cause Failures: .	Defenses against CCF/CMF including redundancy, diversity, N-version software, etc. are prescribed as a part of Appendix C to 49 CFR 236. Specific instructions also provided for cases when multiple failures could occur when failures are not revealing. Reliance on fail safe systems and diversity is emphasized. No information is available on quantitative CCF/CMF. It appears that they may rely on IEC 61508-6 Annex D to estimate the value of β factor and risk reduction factors (RRFs).
Uncertainty Analysis	Addressing uncertainties is an explicit part of regulation. They explicitly require two estimates; an upper bound estimate and a high confidence mean estimate of risk. They also require sensitivity analysis to make sure that the upper bound is reasonable. The risk-informed decision is generally made by comparing upper bound against the baseline criteria.
Risk Analysis Methods used	All conventional methods such as Hazard and Operational assessment (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments are used. For abbreviated risk analysis MTTHE is used for risk-informed decision making. If full risk analysis is required, then all accident consequences are translated to an equivalent monetary value.
Operational Safety & Reliability Program (OSRRP)	
Operational Safety Management	We did not find explicit requirements for OSRRP, or risk management during operation. However, FRA under an initiative (around 2005) embarked on risk reduction program (RRP) which has many common elements with OSRRP. As a result, FRA employees monitor the railroads' compliance with the regulations through inspections including direct observations and audits of the railroad records and analysis of data (e.g., accidents, incidents, reportable events, etc.). Analysis of this data, along with information from FRA inspectors, contributes to the identification of gaps in the regulations. Another feedback mechanism is though NTSB detail examination of severe accidents.

A.6 GENERIC INSIGHTS FOR DI&C RISK-INFORMED REGULATORY FRAMEWORK FROM REVIEWING THE PRACTICES AT DOT/FAA, CHEMICAL SECTOR, NASA, AND DOT/FRA

This section discusses some of the generic aspects of risk-informed activities across the industries examined in this document. It was generally concluded that all the examined industries use a RIDM process like each other and that of NRC risk-informed regulatory framework. The RIDM process is a combination of engineering evaluation, lessons from past experiences and use of good practices, national and international standards, and all combined with the risk insights. Based on the discussion provided in Sections 4 and 5, eight (8) generic areas are identified and discussed below. A brief comparison has also been made to the equivalent processes in USNRC.

1. <u>IDENTIFICATION AND CLASSIFICATION OF RISK SIGNIFICANT SSCS</u>

Identification of risk significant SSCs (safety critical systems) are generally done during the design phase and with the use of risk matrix. Any changes in SSC classifications done after design and during operations are included in MOC (Management of Change) process which is covered under SMS framework. MOC generally involves the re-evaluation and update of design process for SSC classification.

Classification of safety critical systems is generally done using the following steps:

1. The risk matrix is developed using the severity of the outcome (consequence) and probability of occurrence for each item under consideration. Although the concept of risk as the product of consequence and probability is embedded in risk matrix, risk is not directly estimated. A risk matrix is developed to compare potential effectiveness of proposed risk controls and prioritize risks when multiple risks are present.
2. The items are graded based on consequence and occurrence frequency. Regions of the matrix are generally divided in to four to five classes which constitute the importance of the items or functions being considered.
3. If the risk as identified in risk matrix is acceptable after applying specific regulatory treatments for each class of the items, then the system may be placed into operation and monitored.
4. If the risk is not acceptable, risk controls or design changes have to be developed, their effectiveness estimated and monitored in the SA process.

Development of risk matrix is also discussed in MIL-STD 882. Risk matrix can be constructed both qualitatively as well as quantitatively depending on the maturity stage of design and level of PRA fidelity and completeness.

The concept of risk matrix is not used in risk-informed design of current LWRs (conventional PWRS and BWRS). However, some effort has recently started to formalize the concept risk-informed framework during design for the new reactors as published under technology neutral framework described in SC-29980[31].

[31] SC-29980-102 (Draft Rev A), "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Safety Classification and Performance Criteria for Structures, Systems, and Components."

PRAs for advanced reactors include some traditional PRA modeling of DI&C. The most notable of these PRAs is AP-600/1000 which was performed mainly prior to completion of SC-29980. More recently a fully integrated PRA is reported as a part of DCD for NUSCALE and APR-1400 design which have attempted to perform risk-informed SSC classification including software and hardware associated with DI&C.

2. RISK-INFORMED REGULATORY TREATMENT OF DI&C SSC CLASSES

All industrial sectors, except NASA, included in this report have explicitly provided risk-informed regulatory guidance for DI&C systems and made references to SIL classification and certification for both software and hardware at design stage. NASA implicitly discussed reliance on prescriptive criteria and use of PRA; based on the PRA maturity and the certainty of the design.

Also depending on the significance classification of the systems or function, all industrial sectors rely on redundancy and diversity of DI&C software and hardware for protection against CCFs. Redundancy and diversity may include MVDS (i.e., N-version programing) for software and redundant channels of different designs (or technology) for hardware. Examples of diversity could also include backup systems such as manual override and control, or if possible, use of an abort function.

IEC 61508 (SILs) provide a set of features/specifications for designed and systems operation for maintaining acceptable values for CCFs. These features include redundancy, early diagnosis, fault tolerance features, diversity in design, and segregation in operation & maintenance. IEC 61508 also provides risk reduction factors (RRFs) such that when applied to existing nominal values based on SIL classification would yield the new CCF estimate. Bounds of failure probabilities are also defined in IEC 61508 for a given SIL item and for potential for CCFs. In effect a case specific CCF probability and associated uncertainties can be estimated using the calculated RRFs. Although the information in IEC 61508 appears to be quite promising for performing risk-informed applications (before and after risk estimates), the basis for this information including risk reduction factors needs to be examined.

For NRC, the design requirements for the equipment in nuclear power plant ultimately depends if they are categorized as safety. Safety equipment needs to provide an especially high degree of assurance that it will perform to design (compliance with 10 CFR 50 Appendix A Design Requirements and Appendix B Quality Assurance Requirements), and with other related rules and guides. Safety equipment is thus 'pedigreed' and different from other off-the-shelf commercial grade equipment.

3. Reliability Data for DI&C Hardware

There is significant amount of reliability data in the four industries that were reviewed in this study. This is in addition to reliability estimates reported in IEC 61508. The most amounts of data for various DI&C hardware is available through chemical sector and FAA. NASA has a limited set of data for special applications under unique service conditions. NASA also utilizes other sources of data. Some of data sources used by NASA overlaps with the data sources commonly used by nuclear industry. The design and implementation of PTC for DOT/FRA is at early stages. We do not expect rich data environment at DOT/FRA.

4. Software Reliability Data

The software reliability estimates for different SIL classes are reported in IEC 61508. Other sources of software failure data could be found from detailed accident investigation report. These include CSB for chemical sector, NTSB for DOT/FAA and DOT/FRA, and ASAP (Aerospace Safety Advisory Panel) for NASA. These reports can form the basis for the lesson learned and insights gained from the past incidents.

Software reliability data is just the input to software reliability modeling. There are several different software reliability models. All these models require that the data to be reduced for a set of important parameters, such as specification of demands (context), failure modes, failure detections, software design features, software quality, and software complexity.

5. Risk Models

There are significant differences in risk models used for various applications in the four industries reviewed here. These are briefly summarized below.

a) There are many chemical facilities in US and abroad with similar systems. Consequently failure data, failure causes, and failure rate estimates may be available at the system or function level. This allows for a simpler risk model of the facility without the need of a detailed PRA. However, consequence part of chemical facilities is quite complex and require detailed case specific consequence analysis. So generally chemical industry uses simpler PRA models for likelihood estimation and complex evaluation tools for accident consequence analysis. Chemical industry for the likelihood part of PRA could rely on methods such as LOPA.

b) FAA has a large exposure (large number of demand) and a relatively low failure occurrence rate. NASA has significantly less number of demands (missions) than FAA but higher failure rates. All conventional methods such as Hazard and Operational assessment (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagram (ESD), and Failure Mode and Effect Analysis (FMEA) are supported by qualitative engineering arguments. Some dynamic methods such as Markov and DFM (Dynamic Flowgraph Methodology) are also being researched and piloted to capture the risk during phase transitions.

c) DOT/FRA PRA is somewhere between the chemical industry and NAS/FAA. For cases when the system or the change of the system is expected not to result in any new failure mode, and the severity of accident (consequence) of the hazard or failure is not expected to change significantly from previous design, abbreviated risk assessment is used. For abbreviated risk analysis MTTHE is used for risk-informed decision making. For all other cases, conventional methods such as Hazard and Operational assessment (HAZOP), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Mode and Effect Analysis (FMEA) supported by qualitative engineering arguments are used.

6. Software CCF and Risk Model

For all the industries, there is extensive discussion on engineering/deterministic methods for determining software criticality and setting requirements for certification like the practices done within USNRC as described in SRP chapter 7. All software errors resulting from errors in software requirements, specifications, or errors caused by lack of software configuration control and inadequate management of changes are examined. The industry has proposed several protective features against software CCF. They recognize that software CCF can be controlled by Multi-Version Dissimilar Software (MVDS), as well as early diagnosis, fault tolerance features, diversity in design, and segregation in operation & maintenance. With all these precautionary actions, the potential of CCF among software remains. Some industry use IEC 61508-6 Annex D to estimate the value of β factor specific to the strategies they have taken against the CCFs. A case specific CCF probability is estimated using the risk reduction factors (RRFs). IEC 61511-1 [2015] has included evaluation of the common cause for SCAI (Safety Controls, Alarms, and Interlocks) layers. Once the RRF requirement is greater than 10,000, the analysis needs to quantitatively estimate the systematic contributions to CCFs.

Incorporation of software to risk model are done with different level of sophistication from adding a single basic event to a fault tree node or as a branch of event tree. To a more complex approach by NASA which assigns different software failure rates for different functions and different conditions within a framework which is referred to as “CSRM” (Context-based Software Risk Model). The CSRM methodology involves several steps which include: (1) identification of mission critical software functions, (2) Mapping of software-function to PRA event trees (3) developing the branch heading of event trees down to the point where they can be either represented by basic events or quantified using dynamic models if needed. Once the models are structures then minimal cut sets can be generated which can help to determine the software reliability for the specific condition for which it should be evaluated.

7. Operational Safety and Reliability Program; Operational Risk Management

All four industries have risk management program throughout the product life cycle starting from initial design through the end of life decommissioning. The risk management program during the operational phase generally follows the SMS framework. The operational risk management programs have three objectives; (1) Risk-informed management of changes (MOCs) in design or operation as it becomes necessary due to accident/incident investigation or other emergent issues, (2) continuous monitoring of safety and risk by tracking a set of measures of performance (MOPs) and (3) evaluating MOPs and trying to identify risk significant deviations which require intervention using a risk-informed process. Typical MOPs for probabilistic requirements might include the computed probability of loss of the system and the mean failure rates of major subsystems or components for specified conditions.

The risk management applications are remarkably like activities at nuclear industry. These include risk-informed changes in Technical Specifications (TS), system changes required during plant operation (as a result of failure monitoring, discovery of a design flaw, or unavailability of replacement due to obsolescence). This changes also could include the reclassification of SSCs, changes required through the results of maintenance rule or Reliability Assurance Program (RAP), etc.

All industries reviewed rely on both qualitative deterministic criteria as well as risk criteria to manage risk and require risk control measure if needed. Similar guidance could be found in RG 1.174 for USNRC.

8. Safety Goals/ Quantitative Risk Requirements (Criteria)

Most of NRC’s quantitative risk-informed regulatory framework relies on the common understanding of what is “sufficiently safe”. This is done by formal definition of safety goals and subsidiary goals. If there is no safety goal, PRA applications will be limited to PRA insights which could include relying on redundancy, diversity, safety margins, relative PRA risk results, and PRA importance measures. To extend the domain of risk-informed application, it is important that the analysis to have common understanding of what is safe enough.

We could not find formal safety goals in other industries like what is being used at USNRC. Almost all the four industries reviewed here use a safety goal based on the best reliability that can be practically achieved. Such a safety goal is dynamic in nature and can change with time and improvement in technology. For example, FAA uses a safety goal based on the estimates available for rate of accidents per flight hour. These are driven by past accidents. These rates are categorized based on phase of flight, failed systems, and the number of fatalities. Comparative analyses to these targets are generally made to address the cumulative risk effect. NASA also uses safety goals based on past performance for example for loss of crew transportation system missions to the International Space Station; it uses the mission success probability of space shuttle at the end of its operational life. Similar approaches are used by Chemical industry and DOT/FRA and are referred as the “tolerable risk”.

In summary, the safety goals are used in other industries, but they are not as formal as those used in USNRC. These safety goals also are dynamic; they will change as the systems become more mature, more reliable, and as the technology progresses or operation changes towards safer and more reliable regime.

A.7 REFERENCES

1. SAE ARP 4754A-2010; Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, "*Guidelines for Development of Civil Aircraft and Systems*, "December 21, 2010.

2. NASA/CR-2015-218982; "Application of SAE ARP 475A to Flight Critical Systems," Eric M. Peterson, November 2015.

3. ARP-4761, Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761, "Guidelines and methods for Conducting Safety Assessment Process on Civil Airborne System and Equipment," December 1996.

4. DO 254, RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000.

5. RTCA/DO 178 B, Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992.

6. DO 297, RTCA/DO297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations, dated November 8, 2005.

7. Advisory Circular (AC) 23.1309-1E, "System Safety Analysis and Assessment for Part 23 Airplanes," U.S. Department of Transportation, Federal Aviation Administration, 11/17/2011.

8. Advisory Circular (AC) 120-92B, "Safety Management Systems for Aviation Service Providers," U.S. Department of Transportation, Federal Aviation Administration, 1/8/2015.

9. FAA-H-8083-2, "Risk Management Handbook," U.S. Department of Transportation, Federal Aviation Administration, Change I, January 2016.

10. Advisory Circular (AC) 431.35-2A, "Reusable Launch and Reentry Vehicle System Safety Process," U.S. Department of Transportation, Federal Aviation Administration, July 20, 2005.

11. OSHA 3132, Process Safety Management, U.S. Department of Labor, Occupational Safety and Health Administration, reprinted 2000.

12. OSHA 3133, Process Safety Management Guidelines for Compliance, U.S. Department of Labor, Occupational Safety and Health Administration, 1994.

13. Code of Federal Regulations, 40 CFR Part 68, "Chemical Accident Prevention Provisions," Subparts A to H.

14. "Guidelines for Risk Based Process Safety," ISBN: 978-0-470-16569-0, John Wiley, March 2007.

15. "Guidelines for Safe Automation of Chemical Processes," 2nd Edition, CCPS, ISBN: 978-1-118-94949-8 December 2016.

16. NPR 8715.3D, “NASA General Safety Program Requirements (Updated w/Change 1),” effective August 01, 2017 through August 01, 2022.

17. MIL-STD-882E, “Department of Defense Standard Practice, System Safety,” 11 May 2012.

18. NPR 8705.5A, “Technical Probabilistic Risk Assessment (PRA) Procedure for Safety Mission Success for NASA programs and Projects,” (Rev. W/Change1), effective June 07, 2010 through June 07, 2022.

19. NASA/SP-2011-3421, “Probabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioner,” Second edition, December 2011.

20. NPR 8705.2C, “Human-Rating Requirements for Space Systems,” Office of Safety and Mission Assurance, effective July 10, 2017 through July 10, 2022.

21. NASA/SP-2010-580, “NASA System Safety Handbook, Volume 1: System Safety Framework and Concept for Implementation,” Version 1.0, November 2011.

22. NASA/SP-2010-576, “NASA Risk Informed Decision-Making Handbook,” Version 1.0, April 2010.

23. NASA/SP-2014-612, “NASA System Safety Handbook, Volume 2: System Safety Concepts, Guidelines, and Implementation Examples,” November 2014.

24. NASA/SP-2011-3422, “NASA Risk Management Handbook, “Version 1, November 2011.

25. 49 CFR Part 236.909, Title 49 of Code of Federal Regulations part 236.909, “Minimum Performance Standard.”

26. 49 CFR Part 236 h, Title 49 of Code of Federal Regulations part 236 h, “Standards for Processor-Based Signal and Train Control Systems.”

27. 49 CFR Part 236 i, Title 49 of Code of Federal Regulations part 236 i, “Positive Train Control Systems.”

28. 49 CFR Part 236-Appendix B, Title 49 of Code of Federal Regulations part 236 – Appendix B, “Risk Assessment Criteria.”

29. 49 CFR Part 236-Appendix C, Title 49 of Code of Federal Regulations part 236 – Appendix C, “Safety Assurance Criteria and Processes.”

30. DOT/FRA/ORD-09/15, “A Practical Risk Assessment Methodology for Safety-Critical Train Control Systems,” U.S. Department of Transportation-Federal Railroad Administration, Office of Research and Development, July 2009.

APPENDIX B. PRA INSIGHTS FROM I&C MODELING IN NUCLEAR POWER PLANTS

B.1 INTRODUCTION AND PURPOSE

The purpose of this appendix is to compile a summary of the current practices and lessons learned from existing probabilistic risk assessment (PRAs) with instrumentation and controls (I&C) systems modeled. A risk perspective gained from the existing analog instrumentation and controls (AI&C) systems can also provide risk insights for digital instrumentation and controls (DI&C) system since they perform similar functions and have many similar components, such as sensors and actuators. The summary of the past PRA works, methods, data, and results, including the challenges, are discussed as follows.

B.2 PAST STUDIES AND CURRENT PRACTICES FOR APPLYING PRA TO AI&C AND DI&C SYSTEM FOR OPERATING AND NEW REACTORS

In the early 1990s, PRA studies for AI&C systems were performed, in limited scope, to provide risk insight for decision making on specific emergent issues. These earlier studies [Ref. 1] included Rosemount pressure transmitters, Bromley relays, and alternate/diverse backup scram systems. The first major study evaluating the impact of I&C failure on plant performance and safety was discussed by Jackson and Brill [Ref. 2]. This study indicated that approximately 8% of licensee event reports (LERs), from 1994 to 1999, contain DI&C failures, and 9% of reactor trips are attributed to DI&C failures. The study also reported two major observations: (1) failure contribution of some I&C (AI&C or DI&C) components in non-safety systems could be risk-significant, and (2) a closer look at I&C components embedded in safety systems with the potential for causing risk-significant initiators (e.g., loss of service water system, loss of main feedwater) should also be considered in PRAs. For the non-risk significant initiators (e.g., turbine trip), I&C contribution to risk was found to be negligible and detailed modeling may not be required. The study also indicated that the fractions of failures caused by hardware and software in I&C systems, are almost equal (34.0% versus 31.8%).

B.2.1 Studies Performed by Electric Power Research Institute (EPRI)

An Electric Power Research Institute (EPRI) study, EPRI 1019183, “Effect of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants”[Ref. 3], a full-scope Level 1 internal events PRA for a typical pressurized-water reactor (PWR), was modified to include a plant-wide DI&C system. The focus of the study was to evaluate the effects of the DI&C system in the context of the overall integrated plant design. This is important since the study addressed issues similar to both AI&C and DI&C systems. The study considered three factors that can impact the risk through failures of critical functions due to the failure of I&C systems. These factors are, the combinations of digital division reliability (Factor A), the potential for common-cause failures (CCFs) (Factor B), and the level of system diversity (Factor C). It was concluded that these three factors in current PWRs would yield an acceptably small increase in risk due to the failure of I&C systems. For the CCF of DI&C, the study concluded that the introduction of diversity is of great value when the existing defense-in-depth and diversity are designed in the mechanical and electrical systems that the I&C controls and supports. EPRI claims that if this diversity does not exist in mechanical and electrical systems, introducing diversity into their I&C system for reducing CCF would be of little value. Safety I&C systems, such as the reactor protection system (RPS) and the engineered safety features actuation system (ESFAS), are generally redundant and diverse. In addition, there is built-in diversity in the design for accomplishing a safety function in the current generation of reactors. Each critical safety function, such as core cooling, can be achieved with a minimum of two diverse means; therefore, it is supported by two sets of diverse I&C systems. However, this level of redundancy and diversity is not available for I&C systems in which their failure can cause plant initiators.

Another EPRI report, EPRI 1025278, “Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments” [Ref. 4], provides guidance on the modeling of DI&C in the context of the systems they support within the PRA. This report concludes that the modeling of DI&C in a nuclear power plant PRA can be accomplished using many of the same methods used for PRA modeling of AI&C systems. This is due to the fact that many components making up DI&C systems perform the same functions as their analog counterparts (e.g., sensors, signal processors, voting and actuation devices), one difference is that a subset of these functions may be accomplished by different component types (e.g., processors as opposed to electrical/electronic components, such as relays or signal converters). The significant change between modeling of digital versus analog systems is the inclusion of software and its failure modes. In addition, the report identifies some PRA modeling and data challenges for DI&C systems, which could include advanced diagnostic methods, such as the use of watchdog timers, data validation routines, and fault detection and fault tolerance techniques. Reference 4 also emphasizes that the development of DI&C modeling in PRA is a joint effort between the PRA analysts and I&C specialists familiar with the I&C design. It recommends a nine-step process, as that shown in Figure B-1, for performing AI&C/DI&C PRAs. Step 4 in this process expects that the PRA analyst develop a simplified model using high-level events and “super-components” for the I&C failure effects. This crude model is used to screen down the number of I&C systems for which detailed models must be developed based on the assessment of the relative importance of the digital system failures in Step 5 through an importance and sensitivity analysis. It is also important to note that this guide requires that the I&C specialist use detailed digital system design information (e.g., failure mechanisms, defensive design measures) to develop reasonable parameter estimates for use in the PRA given the sensitivity of PRA results to the effects of the I&C and its failure. The PRA analyst should incorporate the aggregate data from the manufacturer and past operational experience into the analysis. The input of the I&C lead is necessary for grouping and characterizing the data from the manufacturer or the operational experience, but as support to the PRA lead.

A recent paper presented by Blanchard, et al. [Ref. 5], closely related to the previous EPRI guide, discusses PRA modeling of DI&C systems with a special focus on defensive measures and the varying conditions (context) under which a DI&C system must respond. Defensive measures are design processes and system features implemented by the I&C vendor to prevent, mitigate, or tolerate potential failures within the digital system, including those associated with both hardware and software. Defensive measures are important in the estimation of “failure rates” for the computing units that make up the digital system. This article identifies four tasks necessary for software failure evaluation, which also include the assessment of defensive measures. These tasks are as follows:

1. Development of a digital system reliability model.
2. Identification and classification of failure mechanisms.
3. Assessment of defensive measures.
4. Quantification of residual failure modes and mechanisms.

The study suggests a design review approach for estimating digital system failure rates. It requires breaking the system up into its major parts (i.e., voting logic, signal processing, communication units, etc.), and examining the internal design of these units in some detail with respect to defenses against important failure modes and potential failure mechanisms. The study concludes that sufficient operating experience is available from nuclear power plants outside the U.S. to provide an estimate of systematic failure rates (software) of plant protection systems when defensive measures are uniformly implemented.

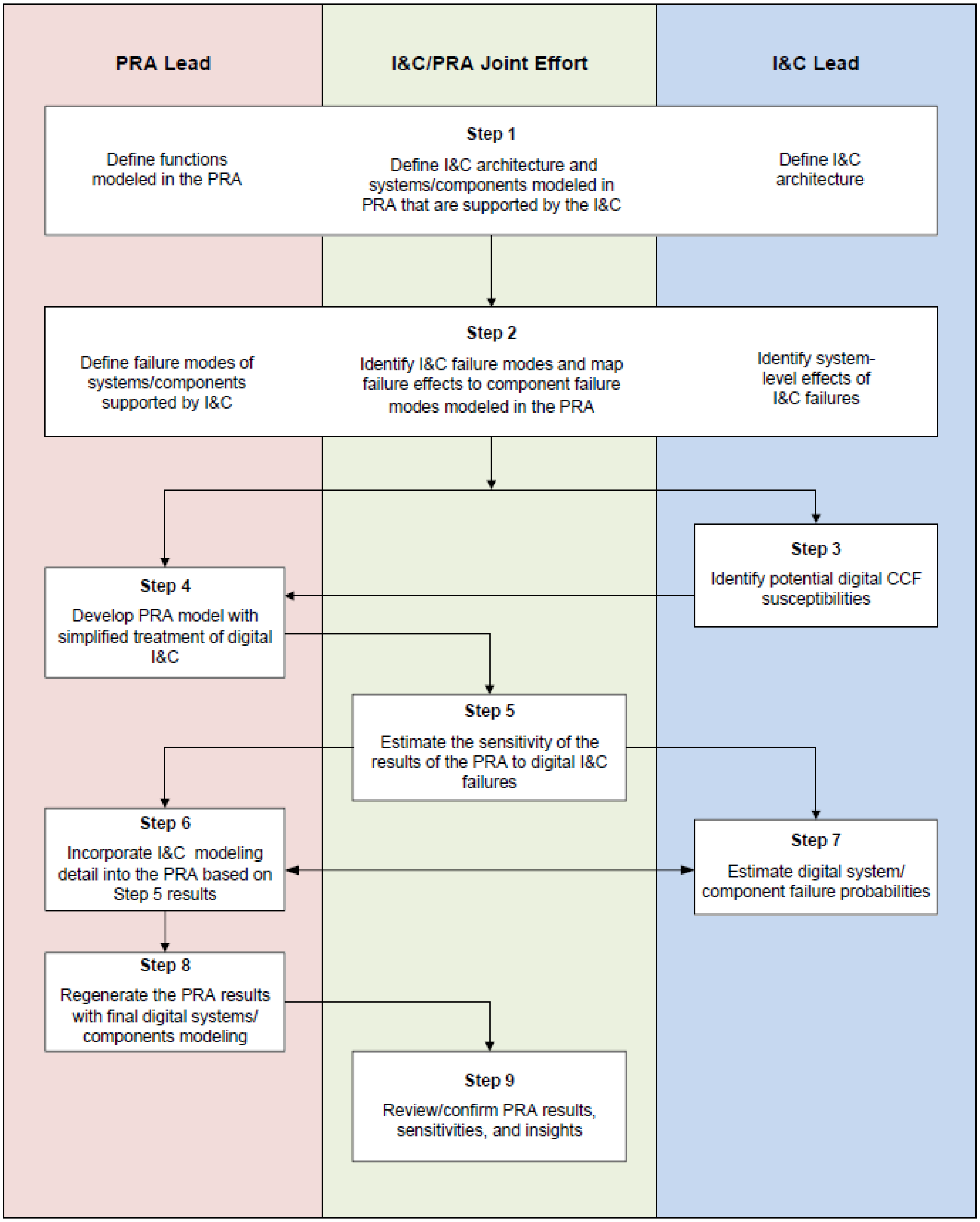
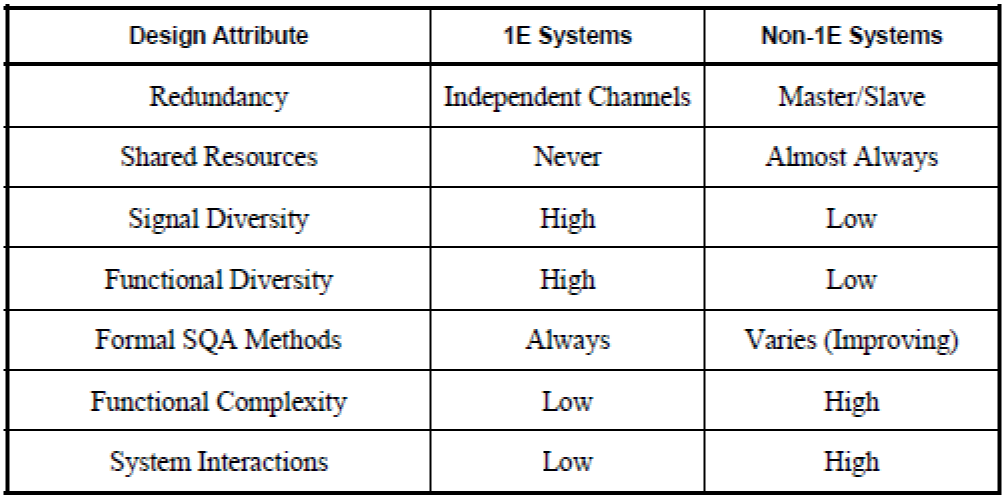

PRA Lead
I&C/PRA Joint Effort
I&C Lead
Step 1
Define functions modeled in the PRA
Define I&C architecture and systems/components modeled in PRA that are supported by the I&C
Define I&C architecture
Step 2
Define failure modes of systems/components supported by I&C
Identify I&C failure modes and map failure effects to component failure modes modeled in the PRA
Identify system-level effects of I&C failures
Step 3
Identify potential digital CCF susceptibilities
Step 4
Develop PRA model with simplified treatment of digital I&C
Step 5
Estimate the sensitivity of the results of the PRA to digital I&C failures
Step 6
Incorporate I&C modeling detail into the PRA based on Step 5 results
Step 7
Estimate digital system/ component failure probabilities
Step 8
Regenerate the PRA results with final digital systems/ components modeling
Step 9
Review/confirm PRA results, sensitivities, and insights

Figure B-1 Nine-Step Process duplicated from Figure 2-1 of EPRI 1925278

EPRI 1016731, “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems,” December 2009 [Ref.6], evaluated 322 events involving I&C systems [See Appendix A of Ref. 6]. It is important to note that the “events” captured in this investigation cover a broad range of occurrences that involved or affected digital systems; they are not limited to only failures of digital equipment, and it would be misleading to characterize the 322 events evaluated as “digital system failures.” Out of 322 events, 246 are related to Non-1E systems, such as plant computer, turbine electrohydraulic control, feedwater, etc.; 49 events are related to 1E systems, such as the RPS, ESFAS, diesel load sequencer, post-accident monitoring, etc.; and 27 events are identified in the systems which are not typical plant indicator or control systems, such as emergency sirens. These 27 events are grouped with non-1E for later classification. The study concluded that there were no actual CCF events in Class 1E systems. The authors believe that this is indebted to significant diversity and restrictive requirements exist for Class 1E systems compared to non-1E systems. Table B-1 is reproduced from this document for further illustration of the differences. For non-1E systems, the CCF events were dominated by hardware rather than software failures.

Two other EPRI studies, “Estimating Failure Rates in Highly Reliable Digital Systems,” December 15, 2010 [Ref. 7] and “Digital Operating Experience in the Republic of Korea,” 2011 [Ref. 8], have been referenced by a previous study. These documents appear to provide insightful information on DI&C PRA; however, these documents are not publicly available.

Table B-1 IE versus Non-IE Design Characteristics (Reproduced from Table 5-2 of Ref. 6]



Design Attribute	1E Systems	Non-1E Systems
Redundancy	Independent Channels	Master/Slave
Shared Resources	Never	Almost Always
Signal Diversity	High	Low
Functional Diversity	High	Low
Formal SQA Methods	Always	Varies (Improving)
Functional Complexity	Low	High
System Interactions	Low	High

The following is a summary of lessons learned and challenges concluded by the authors after the reviews of various EPRI studies:

1. The safety-related software development process for nuclear power plants is equivalent to or better than Safety Integrity Level (SIL)-4 of International Electrotechnical Commission (IEC) Standard 61508[32]; the use of SIL-4 bounds for failure rates could be applied.
2. The modeling of DI&C systems for normal plant control systems may not be necessary since their contribution is included in initiating event frequency and DI&C contributions are generally not dominant contributors. The contribution of DI&C systems for the balance of plant systems when credited as a mitigation system post trip may not have to be modeled, since the general practice is to take either manual control or the system has restricted control. For example, consider the control of a main feedwater pump following

[32] IEC 61508, “Functional safety of electrical/electronic/programmable electronic safety-related systems,” Seven (7) parts, Commercial Version (CMV), International Electrotechnical Commission, 2010.

a reactor trip. Some plants automatically bypass the normal three-element control of feedwater flow in preference to a predetermined flow setpoint or switch to single-element control.

3. A minimum amount of fault tree modeling of initiating events may be necessary to capture dependencies (e.g., shared components or support systems), and the purpose of these models is to ensure that credit is not given post-trip for a system or component that was involved in the initiating event.
4. The plant protection system, such as reactor trip (RTS) and ESFAS, should be a primary I&C focus for the PRA. These systems interact with many different mitigation capabilities and perform under many different contexts (initiator and accident sequences).
5. The mitigating systems that support critical functions can be a mix of safety-related and non-safety-related systems. Dependencies between these mitigating systems may include not only shared equipment but also common software between redundant systems where digital systems are used.
6. Non-safety-related mitigating systems should also be considered in the PRA, generally for accident sequences that go beyond design basis events. These may include diverse systems required by regulation (e.g., anticipated transient without scram [ATWS] systems) or other plant systems that can back up the functions provided by the safety systems (e.g., main feedwater, fire system, containment venting, etc.). Whether these systems are controlled by DI&C may vary from plant to plant. Where these systems share dependencies with initiating systems or other mitigating systems, these dependencies are generally developed in the PRA.
7. The support systems (component cooling water [CCW], emergency service water [ESW], chilled water, instrument air and electrical systems) may include system-specific controls and they are not integrated across other systems. Simplified PRA models at the module levels may be developed for these systems as a part of system failure probability estimation.
8. A large number of redundant and diverse indicators and displays are available in the control room, the impact of partial loss of indication and display on operator actions and control may not have to be modeled unless a significant number of them is lost in the scenario (e.g., such as fire). Non-safety-related controls and displays in the control room are designed so that a credible failure will not interfere with automatic protection system functions. Conversely, the manual control systems credited for diversity and defense-in-depth assessments are independent of the postulated protection system computer failure. Detailed PRA modeling may not be required for such cases.
9. Digital common cause can have both intra- and inter-system impacts on mitigation systems. CCF events could be initially modeled as super component and determine if further detail is necessary.
10. For a plant-wide digital system, the plant operating system or the digital platform[33] can be common to many plant systems, both mitigating systems as well as normal operating systems. The CCF due to fault of the operating system is generally negligible as long as they are designed to perform cyclically, with few interruptions and are not affected by plant conditions.

[33] Operating system: set of software that manages computer hardware resources and provides common services for computer programs. Platform: set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). Platform usually provides a number of standard functionalities (application functions library) that may be combined to generate specific application software.

Some of the challenges for traditional PRA modeling of DI&C that were interpreted from the various EPRI reports are summarized below:

1. Determination of appropriate level of detail in logic models.

2. Failure mode, failure probabilities and associated uncertainties for DI&C hardware accounting for specific technology, failure modes, fault tolerance and other defensive measures.

3. Failure probability of software since the faults are generally designed in, they can be eliminated when they occur and are detected, and the failure rates are greatly affected by software development and the verification and validation (V&V) processes, error checking techniques, and diagnostics (for hardware and software interactions).

4. Inter- and intra-system CCF for software and the operating systems when various methods of diversification are used.

As discussed in the main body of the report, this study considers an appropriate level of detail and scope for PRA shall be commensurate with the risk-informed application of the PRA models. All insights and challenges identified here shall be tempered with the specific risk-informed applications of interest.

B.2.2 NRC Studies Related to AI&C/DI&C PRAs

PRA modeling for DI&C systems is discussed in detail in NUREG-0800, Standard Review Plan (SRP), Chapter 19, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” [Ref. 9]. This document lists several areas the NRC staff considers important and must be subjected to review for DI&C systems. The SRP does not indicate how and at what level of detail these reviews should be performed.

The SRP identifies specific audit topics for reviewing DI&C. These topics are said to be based on the lessons learned from previously accepted new reactor DI&C system PRA reviews. The following lists major guidelines contained in the SRP to ensure that the risk contributions from DI&C, including software, are reflected in the PRA.

1. The level of review of the DI&C portion of the PRA may be limited due to limitations such as the lack of design details, lack of applicable data, and the lack of consensus in the technical community regarding acceptable modeling techniques for determining the risk significance of the DI&C system.
2. The modeling of DI&C systems should include the identification of how DI&C systems can fail and what these failures can affect. The failure modes of DI&C systems are often identified by the performance of failure modes and effects analyses (FMEA). It is difficult to define DI&C system failure modes especially for software because they occur in various ways depending on specific applications. Also, failure modes, causes, or effects often are intertwined or defined ambiguously, and sometimes overlap or are contradictory. Examine applicant documentation to ensure that the most significant failure modes of the DI&C are documented with a description of the sequence of events (context) that need to take place to fail the system. The sequence of events should realistically represent the system’s behavior at the level of detail of the model.
3. The DI&C system CCF events should be identified by the applicant and the bases for grouping of CCFs should be provided. Review the discussion of how the applicant

determined the probabilities associated with CCFs. The PRA reviewer should work closely with the I&C reviewer responsible for implementing SRP Section 7.1, “Fundamental Design Principles,” to evaluate the applicant’s justifications.

4. Uncertainties in DI&C modeling and data should be addressed in the DI&C risk assessment. It is expected that the DI&C risk assessment will address uncertainties by at least performing several sensitivity studies that vary modeling assumptions, reliability data, and parameter values both at the component and system level. The reviewer should evaluate the sensitivity studies performed by the applicant on the PRA models and data to assess the effect of uncertainty on CDF, risk, and PRA insights. Sensitivity studies may be particularly helpful in assessing the effectiveness of design attributes. Additional support for the review and treatment of uncertainties is provided by NUREG-1855, Volume 1, Main Report, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making,” dated March 2009 [Ref. 10].
5. The DI&C reviewer should confirm that DI&C system equipment can meet its safety function in environments associated with accident sequences modeled in the PRA. This is done in collaboration with the reviewer for the PRA and severe accident evaluation that provides input on the expected environments that need to be considered.
6. The PRA reviewer should confirm that the impact of external events (i.e., seismic, fire, high winds, flood, and others) on DI&C has been addressed in the PRA.
7. Coordinate the human reliability assessment (HRA) review with the staff evaluating areas such as main control room design and minimum alarms and controls inventory. If recovery actions are modeled, they should consider the loss of instrumentation and the time available to complete such action.
8. Verify that key assumptions from the DI&C PRA are captured under the applicant’s design reliability assurance program (D-RAP), which is described in SRP Chapter 17, Section 17.4, “Reliability Assurance Program (RAP).” The applicant should describe adequately where and how the D-RAP captures the DI&C system key assumptions, such as how future software and hardware modifications will be conducted to ensure that high reliability and availability are maintained over the life of the plant.
9. Common cause failures can occur in areas where there is sharing of design, application, or functional attributes, or where there is sharing of environmental challenges. Each of the areas found to share such attributes should be evaluated in the DI&C analysis to determine where CCF should be modeled and to estimate their contribution. The CCF probabilities and their bases should be evaluated and provided based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of defensive measures meant to protect against CCF (e.g., separation and independence, operational testing, maintenance, diagnostics, self-testing, fault tolerance, and software/hardware design/development techniques and processes). Dependencies between hardware and software should be identified.
10. Design features such as fault tolerance, diagnostics, and self-testing are intended to increase the safety of DI&C systems, and therefore are expected to have a positive effect on the system’s safety. However, these features may also have a negative impact on the safety of DI&C systems if they fail to operate appropriately. The potentially negative effects of these features should be included in the probabilistic model. An issue associated with including a design feature, such as fault tolerance in a DI&C system, modeled in a PRA is that its design may be such that it can only detect, and hence mitigate, certain types of failures. A feature may not detect all the failure modes of the associated component, but just the ones it was designed to detect. The PRA model should only give credit to the ability of these features to automatically mitigate these specific failure modes; it should consider that all remaining failure modes cannot be

automatically tolerated. A fault-tolerant feature of a DI&C system can be explicitly included either in the logic model or in the PRA data, but not both.

11. If a DI&C system shares a communication network with other DI&C systems, the effects on all systems due to failures of the network should be modeled jointly. The impact of communication faults on the related components or systems should be evaluated, and any failure considered relevant should be included in the probabilistic model.

It is clear from the discussion in SRP Chapter 19 that there are many challenges in performing and reviewing the PRA for the DI&C system. Additional challenges could be identified when a specific risk-informed application is considered (e.g., SSC classification for DI&C).

Another important challenge of performing the DI&C PRA is to determine failure modes and their relative contribution. An NRC study [Ref. 11] at Oak Ridge National Laboratory (ORNL) was conducted to investigate DI&C systems and module-level failure modes, using a number of databases[34] both in the nuclear and non-nuclear industries. The objectives of the study were to obtain relevant operational experience data to identify generic DI&C system failure modes and failure mechanisms, and generic insights to establish a unified framework for categorizing failure modes and mechanisms. This study identified a total of 2,263 reported events related to DI&C systems. The study evaluated a small sample of these events (226 out of 2,263 events). The study concluded that unified failure modes cannot be developed due to the lack of quality of a data source and the small sample evaluated.

The study however, reported fractions of evaluated events that reside in different groups based on their specific characteristics. Such information can be used to scale the overall DI&C failure probability to different groups with similar characteristics. Examples of such results/insights are summarized below:

a. About 11% of the 226 events were related to application-specific integrated circuits (ASIC) and/or field programmable gate arrays (FPGA). It appeared that the “loss of programmed memory” appears to be a significant failure mode of such devices. Failure modes of the ASIC cards included “failed passive components” (e.g., “shorted capacitor”), “failed output” (LO or HI), “shorted operational amplifier,” and “intermittent loss of power.”
b. The breakdown of the programmable logic controller (PLC) failure modes was also reported. About 35% of failures involved PLCs. Failure modes included, “loss of communication,” “incorrect firmware coding,” “loss of power,” and “processor lockup.”
c. The EPIX database was found to contain little information on software failure modes. Less than 10% of the records analyzed were attributed to software. In addition, event descriptions were often not comprehensive enough to identify the software failure mode and/or the cause of the software failure.

Re-evaluation of more events (larger sample size) could provide additional information regarding the contribution (fraction of total) of the failure of components contributing to the overall failure counts.

One of the early PRA applications to the reactor protection system (RPS) was reported in NUREG/CR-5500, “Reliability Study: Westinghouse Reactor Protection System, 1984-1995” [Ref. 12]. This multivolume report covers all types of existing reactors and utilizes the plant data

[34] The databases included EPIX, COMPSIS, SPIDR, FARADIP, GIDEP, OREDA, and civil aviation database.

from 1984 through 1995. Approximately 1500 events were evaluated, Volume 2 for Westinghouse plants covers the unavailability estimation for solid state protection system trains and Analog Series 7300 or Eagle-21 channels. The fault trees developed for these designs assumed a four-loop plant. The trip signal logic is developed in a stylized manner based on two of three logics of diverse signals twice (e.g., primary temperature and pressure).

The PRA for DI&C systems has been mainly at the research stage at the NRC with limited applications performed by nuclear industries in two areas: upgrades to analog I&C systems and DI&C for advanced reactors. The level of detail of most of these PRAs is generally at the module levels. These PRAs are generally supported by limited generic data on DI&C hardware and software. Most of the NRC applications of PRA for I&C systems and supporting data were performed for safety-related actuation systems. However, some NRC studies attempted to develop PRA methods for control systems. The dynamic nature of I&C control systems is highlighted in NUREG/CR-6901, “Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessment” [Ref. 13]. This study focuses on the dynamic nature of control systems and their impact on the rate of change of plant parameters causing the failure of the system supported by DI&C controller. It highlights the need for simulation in support of the dynamic reliability evaluation of DI&C responses.

A reliability study of the digital feedwater controller was reported in NUREG/CR-6997, “Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods” [Ref. 14]. This study utilized a simplified simulation tool that could propagate the failure modes of various devices through the control system. This tool can significantly assist in the development and verification of FMEA tool for DI&C controllers. The study identified some chronological events that should occur in certain order to cause DI&C failures. The study applied Markov models for quantification. The traditional PRA methods (e.g., FT and ET) can be used with minor modifications. The study was only applicable for full-power operation and, for example, did not address the single-element controller (rather than the three-element controller) when the power level is less than 15%.

There are other NRC studies that were not reviewed here in detail. They will be examined as needed in other phases of this program. However, two studies generated insights and introduced techniques that are mentioned in this report. The existence of fault tolerance, fault diagnostics, and voting systems in DI&C systems could eliminate the impact of some failures (e.g., put the channel in trip mode) and improve reliability. The software response to a fault generated by hardware and the role of fault tolerance techniques, generally referred to as hardware software interaction, should be evaluated. Fault injection techniques are designed to discover such interactions. NUREG/CR-7151, “Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems” [Ref. 15], addresses some of these issues regarding the effectiveness of fault tolerance using fault injection techniques. Another study regarding the factors affecting software reliability is reported in NUREG/GR-0019, “Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems” [Ref. 16]. This study started with a pool of 78 software engineering measures identified by Lawrence Livermore National Laboratory (LLNL) and attempted to identify a subset of these measures that are more important for predicting software failures. Additional missing measures were also identified, and expert elicitation was used for ranking.

B.2.3 Other Studies: Vendors and International

A paper published by Stacey Davis, et al. [Ref. 17]; focuses on the protection and safety monitoring system (PMS) and its interaction with plant control system (PLS). The DI&C system model in this study was developed consistent with the results generated from a detailed device level FMEA developed for an AP1000 plant PRA. PMS serves to perform the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip or engineered safety functions actuation, and component control functions. The PLS performs signal acquisition, calculations, setpoint comparisons, logic calculations, and component control to maintain the plant's systems during all modes of operation. Independence and elimination of any possible interaction between safety and non-safety systems are required and generally is met using complete segregation and separation. In cases when total separation cannot be achieved between DI&C systems (such as shared parameters and actuation signal between safety and non-safety), electrical and signal isolations will be necessary. This was the case for the PMS and PLS systems. The PRA study reported by Davis, et al. was intended to evaluate the effectiveness of such isolation strategies. The PRA had to be performed at a level of detail consistent with the engineering evaluation and FMEA studies. This study generated several insights and identified many challenges if the DI&C PRA models were to be developed at a level of detail at the component (device) level. Some of these challenges and insights are identified below.

1. The failure modes tabulated in the FMEA are to be reviewed and the effects of the failure modes assessed on the PRA success criteria, however the level of detail of modeling should also consider the available component failure data.
2. Generic data for current operating plant ESF and RPS systems was not a direct one-to-one comparison. The data used in the study was primarily developed using the "217Plus" software tool developed by the Reliability Information Analysis Center (RIAC), [Ref. 18]. The Department of Defense authorized and supported the effort to collect and analyze data for use in the reliability analyses.
3. Both unavailability and failure probabilities were modeled in the DI&C PRA for major components. Design features, such as the self-diagnostics capability, allow for rapid replacement and, therefore, were modeled to reduce the unavailability contribution.
4. Failure of the manual soft control action is modeled via manual CCF of operator workstations, failure of the power supplies to the cabinets supporting the operator workstations, operator action failure, and failure of the PLS logic from the controller cabinet(s) to the actuated component(s).
5. It is important to distinguish main control room (MCR) actions from local actions outside the control room. The I&C system models and human reliability analysis (HRA) should ensure that when credit is taken for manual actions from the MCR, the system model includes all components within the associated I&C cabinets that could fail the signal from manually actuating the equipment.
6. The ability to locally start equipment by bypassing the I&C cabinets should not be used as a justification for screening the I&C equipment from failing the actions. A control room action and a local action could be modeled with corresponding I&C failures for the same actuation, if risk important.
7. Detailed modeling of the non-safety-related I&C equipment would increase the magnitude of circular logic significantly and is a lot more complicated than what is seen in current-PWR PRAs. Similar findings were reported in NUREG/CR-6997, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods" [Ref. 14]. The findings relate to the ordering of the failures in a sequence. Section 4.3 of this NUREG indicates that the DI&C system (it can also be extrapolated to AI&C systems), in a few simulations, in some failure sequences did not cause system failure. However, the same set (or a subset) of component failures in a different order did result in system failure. The treatment of circular logic is well known. The ordering of sequences can be handled via priority gates (logics) and use dynamic models for

quantification. Neglecting the effect of ordered sequences will result in some degree of overestimation, which in most cases could be tolerable.

The study concluded that it could be more efficient and economically preferable to share plant parameters or actuations between safety-related functions and non-safety-related functions, but it can significantly affect the complexity of the PRA and may reduce defense-in-depth by introducing common failures that are evaluated by the PRA.

Fault monitoring and fault tolerance events were reported in two international PRA studies [Ref.19 and Ref. 20]. The faults in a DI&C system are monitored by a self-monitoring algorithm and recovered before a fault causes a system failure. Protecting a system from catastrophic damage is possible even for a fault that cannot be perfectly recovered. Multiple channel processing systems might have cross-channel monitoring functions. Independent heartbeat monitoring equipment can also be installed in these systems. Software-based intelligence and the flexibility of microprocessors accommodate these sophisticated reliability-enhancing mechanisms successfully. An insight from this study is to model fault tolerance features in an actual reliability model, it is necessary to classify faults as detectable and non-detectable and do the same in evaluating operational data.

Software-based intelligence and the flexibility of microprocessors to accommodate fault tolerance strategies using sophisticated, reliability-enhancing mechanisms is discussed in detail in a study by Pierre Rebours [Ref. 21]. This study also finds that the classification of failures into detectable and recoverable classes, detectable and not automatically recoverable, and not detectable is necessary for evaluating the DI&C system reliability.

There have been many other international studies regarding DI&C PRAs from which some lessons and challenges could be extracted. Reviews of all these documents were not considered within the scope of this study. Therefore, we concentrated on major activity related to the development and application of a consensus taxonomy for using traditional PRA methods for modeling DI&C systems.

NEA/CSNI/R(2014)16, “Failure modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA” [Ref. 22], reports on the activities by an international consensus task group, called DIGREL, regarding developing the failure modes taxonomy for reliability assessment of DI&C systems for PRAs. The purpose of the taxonomy is to support the PRA framework for including DI&C systems. It focuses on high-level functional aspects rather than low-level structural aspects. This focus allows the handling of the variability of failure modes and mechanisms of I&C components. It reduces the difficulties associated with the complex structural aspects of software in redundant distributed systems. A major part of their effort was devoted to developing a hierarchical definition of five basic levels of modeling. At the system~~s~~ level, between divisions and I&C units, no significant distinction is made between hardware or software aspects. At the module and basic component levels, however, the taxonomy differentiates between hardware- and software-related failure modes.

The PRA taxonomy was implemented to develop the guidelines for the reliability analysis of digital systems in a PRA context, NKS-330 [Ref. 23]. This study shows that the modelling of digital I&C is of high importance by using a simplified PRA model representing a four-redundant distributed protection system. This study also categorizes hardware and software failures as detected and undetected. Detected failures are those discovered continuously by online monitoring where undetected failures are discovered off-line. For undetected failures, this study does not differentiate between off-line detection during periodic testing and off-line detection that can only occur due to an actual demand. The study recommends that both detected and undetected failures be modeled, because they both contribute to system failure probability through unavailability and unreliability. The study suggests that to develop a realistic fault tree model for a digital I&C protection system, it is vital that the chosen fault tolerant design is fully understood and correctly described in the model. The study also attempted to evaluate the impact of the level of detail in PRA modeling on the results by comparing the approaches in four PRAs. A more detailed discussion of the models and results can be found in NKS-361 [Ref. 24].

B.2.4 Summary and Conclusion

Generally, the NRC and industry, both recognize that developing the PRA that includes DI&C systems explicitly should address a set of concerns as summarized below:

- Common Cause Failures: new digital instrumentation and controls are highly redundant and there is the potential for introducing CCFs and possibly undesirable failure modes. The CCFs and other undesirable failure modes of DI&C systems that did not exist in the AI&C systems primarily deal with the software and, to a lesser extent, DI&C-specific hardware. Common cause errors can be introduced to software at different phases through its life cycle. Different techniques exist to reduce software CCF contributions. There are also different contributors to DI&C hardware CCF, including external causes, such as high-frequency radio frequency interference (RFI)/electro-magnetic interference ((EMI). To address these issues, NRC guidance recommends a defense-in-depth and diversity evaluation [Ref. 25, 26] for all digital upgrades involving the RTS and ESFAS. These CCF contributors should also be accounted for and differentiated in the DI&C PRA model.
- Fault Coverage, Fault Monitoring and Fault Tolerance: The faults in a DI&C system are monitored by a self-monitoring algorithm and recovered before a fault causes a system failure. Protecting a system from catastrophic damage is possible even for a fault that cannot be perfectly recovered. Multiple channel processing systems might have cross-channel monitoring functions. Independent heartbeat monitoring equipment can also be installed in these systems. Software-based intelligence and the flexibility of microprocessors accommodate these sophisticated reliability-enhancing mechanisms successfully [Ref.19]. To model fault tolerance features in an actual reliability model, it is necessary to classify faults as detectable and non-detectable.
- Integration: Although the DI&C systems for most support systems and non-safety systems are dedicated to a specific task in a specific system, there are significant integrations on the safety-related side. Software provides the capability for integrating several different functions within a physical DI&C system. Software routinely integrates the control/actuations of many systems; each with a specific physical impact on plant risk. For example, the scram logic software integrates the scram functions for many different physical conditions (e.g., failure to scram due to steam generator tube rupture, and failure to scram due to loss of flow) and interacts with the ESFAS DI&C. As a result of such an integration, there could be many different failure modes of software each representing one of many functions performed by the software. In addition to automations tasks performed within software, they could also provide data, graphs, drawings, initiate alarms, and other information/displays to operators in the control room and receive soft or hard commands from the operator as input. DI&C PRA models, if developed at a detailed level, are expected to be complex. They may also require HRA re-evaluation if DI&C failure modes interact with the operator’s actions in the control room.

- Unavailability of a Single DI&C Module: DI&C systems have smart features that could facilitate online testing and repair by setting the system status in a safe mode. Although, there would be no unavailability contribution from these events, the reduced redundancy could increase the failure rates associated with spurious actuation. Other software failures, such as an operating system crash, would stop the entire computer system. Since many software problems are transient, a reboot often repairs the problem. This involves rebooting the operating system, running software that repairs the disk state[35] that might have become inconsistent due to the failure, recovering communication sessions with other systems in a distributed system, and restarting all the application programs [Ref.21]. Another contributor to the DI&C unavailability relates to software upgrades either as a preventive or corrective measure. PRA models should explicitly model the unavailability contribution.
- Failure of Single DI&C Module: For a DI&C module, the impact of individual hardware failures on module operation is more challenging than an AI&C train. The existence of fault tolerance, fault diagnostics, and voting systems could eliminate the impact of some failures (e.g., put the channel in trip mode). The interaction of software and hardware should also be considered. The latter statement specifically refers to memory failures and failure of microprocessors where hardware failure could interact with software and the resulting outcome may be difficult to predict. The fault injection techniques are designed to discover such interactions [Ref. 15]. This challenging task for DI&C PRAs may initially be addressed using a combination of empirical estimation and bounding analysis.

A complete review of all references on lessons and challenges of the DI&C PRA is not possible due to large number of citations. It is also the opinion of the authors that other lessons and challenges will be identified when the DI&C PRA is used for specific risk-informed applications due to their varying needs for level of detail and scope. The requirements of some risk-informed applications could be much easier than others. For example, SSC classification using importance measures is anticipated to be less demanding than design changes, which may require changes in CDF and LERF to be evaluated. A plant PRA with flexible modeling of the DI&C system could be helpful in testing different risk-informed applications and identifying application-specific lessons and challenges.

[35] Disk state generally refers to disk size, occupied sector information, etc. Some DI&C systems perform checks of disk spaces prior to complete reload to make sure they are consistent with the last recorded information.

B.3 REFERENCES

1. Azarm, M.A., et al., “An Evaluation of Surveillance and Technical Issues Regarding Rosemount Pressure Transmitter Loss of Fill-Oil Failures,” BNL Technical Report L-1311, December 20, 1991.
2. Jackson, T.W., and Brill, R., “A Study of Nuclear Power Plant Events That Involve Instrumentation and Control Systems,” Proceedings of ICONE 8, 8th International Conference on Nuclear Engineering, April 2-6, 2000, Baltimore, MD, USA.
3. EPRI 1019183, “Effect of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants,” December 2009.
4. EPRI 1025278, “Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments,” July 2012.
5. David Blanchard, Thuy Nguyen, and Ray Torok, “Modeling Digital I&C in PRA: Considering Context and Defensive Measures,” ANS PSA 2013, Columbia, SC, September 22 to 26, 2013.
6. EPRI 1016731, “Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems,” December 2009.
7. EPRI 1021077, “Estimating Failure Rates in Highly Reliable Digital Systems,” December 15, 2010.
8. EPRI 1022986, “Digital Operating Experience in the Republic of Korea,” 2011.
9. Standard Review Plan (SRP), Chapter 19.0, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” NUREG-0800, December 2015.
10. NUREG-1855, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making,” March 2009.
11. K. Korshah, et al., “An investigation of Digital Instrumentation and Control System Failure Modes,” ORNL/TM-2010/32, Technical Report March 2010.
12. NUREG/CR-5500, “Reliability Study: Westinghouse Reactor Protection System, 1984-1995,” Vol. 2, December 1998. NUREG/CR-5500 has several volumes and covers all reactor designs.
13. T. Aldemir, et al., “Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessment,” NUREG/CR-6901, Ohio State University, February 2006.
14. T.L. Chu, M. Yue, et al., “Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods,” NUREG/CR-6997, September 2009.
15. NUREG/CR-7151, “Development of a Fault Injection-Based Dependability Assessment Methodology for Digital I&C Systems.”
16. C. Smidts and M. LI, “Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems,” Univ. of Maryland, NUREG/CR-0019, October 2000.
17. Stacy A. Davis, Heather L. Detar and Yves Masset, “Lessons Learned from the Digital I&C System Modeling of the AP1000 Plant PRA,” ANS PSA 2013, September 22-26, 2013, Columbia SC.
18. 217Plus is a methodology and a software tool that was developed by the RIAC to aid in the assessment of system reliability. It represents the next generation of the PRISM software tool initially released in 1999.
19. Hyun Gook Kang, et al., “An Overview of Risk Quantification Issues for Digitalized Nuclear Power Plants Using A Static Fault For a DI&C module Tree,” Korean Atomic Energy Research Institute, March 10, 2009.
20. Man Cheol Kim, et al., “Evaluation of Effectiveness of Fault-Tolerant Techniques in a Digital Instrumentation and Control System with a Fault Injection Experiment,” Nuclear Engineering and Technology 51 (692-701), 2019.

21. Pierre Rebours, Taghi M. Khoshgoftaar, “Software Failure; An Overview,” Science Direct, Advances in Computers, 2006.
22. NEA/CSNI/R(2014)16, “Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA,” 2/15/2015.
23. NKS-330, “Guidelines for Reliability Analysis of Digital Systems in PSA Context,” Risk Pilot AB, Sweden, and VTT of Finland, February 2015.
24. NKS-361, “Modelling of Digital I&C, MODIG-Interim Report 2015,” Risk Pilot AB, Sweden, and VTT of Finland, March 2016.
25. Branch Technical Position (BTP) 7-19, Rev. 7-August 2016, NUREG-0800, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems.”
26. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994.

APPENDIX C. INSIGHTS FROM CURRENT RISK-INFORMED APPLICATIONS AT NRC

C.1 PERSPECTIVE OF RISK-INFORMED DECISION MAKING AT NRC

In August 1995, the NRC adopted the probabilistic risk assessment (PRA) policy statement [Ref.1] regarding the expanded use of PRA. It states the following:

> PRA results and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

This resulted in the use of risk insights and a risk-informed regulatory framework for addressing several NRC regulatory decisions for current reactors. The Risk-Informed Decision Making (RIDM) process has been used by NRC for the past three decades. During this period, risk information was used by the regulators to strengthen requirements, relax requirements, and provide efficiency in the regulatory process and compliance with the requirements. Some of the applications were found important enough to be included in Part 10 of the *Code of Federal Regulations* (10 CFR) (See Table C-1). Table C-1 provides a comprehensive listing of NRC's major risk-informed applications (RIDM).

The RIDM process is driven by two principles (1) deterministic regulatory compliance to assure adequate protection (such as defense-in-depth, safety margins and standards), and (2) risk insights. The decision making varies based on the maturity of the PRA, and the uncertainties associated with PRA results, including the characterization of the issue being regulated [Ref. 2].

Table C-0-1 NRC Use of Risk Insights

Risk Application Area	Summary Description
10 CFR 50.109 (Backfit Rule)	For adding or amending a provision in the regulations or regulatory position interpretation that is either new or different from previous ones. Formal risk and cost benefit methodologies are implemented.
10 CFR 50.44 (Combustion Gas Control)	For monitoring, control of hydrogen combustion inside containment and assuring containment integrity based on selected severe accident scenarios for both current and future reactors.
10 CFR 50.48 (NFPA 805)	Fire protection program, which approves the use of risk-informed decision making as discussed in NFPA 805.
10 CFR Part 54 (License Renewal)	Governs the issuance of renewed licenses for nuclear power plants. It is generally not risk-informed except for the section that requires the licensee perform Severe Accident Management Alternatives (SAMA) accounting for postulated

Risk Application Area	Summary Description
	accidents as well an environmental impact review.
10 CFR 50.61a (PTS Rule)	Allow the use of alternate fracture toughness requirement for pressurized thermal shock (PTS) events. Mostly deterministic document but allows the use of plant-specific risk analyses, which demonstrate acceptable risk with RTMAX–X values above the PTS screening criteria.
10 CFR 50.62 (ATWS Rule)	Requirement for reduction of risk from anticipated transient without scram (ATWS). Risk insights were used to recommend diverse scram system and auto auxiliary feedwater (AFW) actuation for pressurized-water reactors (PWRs) and alternate rod injection (ARI) for boiling-water reactors (BWRs).
10 CFR 50.63 (Station Blackout [SBO] Rule)	Required plant-specific SBO coping duration based on SBO risk; specifically, onsite power reliability and redundancy, loss of offsite power frequency, and time required for offsite power recovery. Also see RG 1.155. SBO rule when applied to new reactors resulted in additional plant features; coping via alternate AC (AAC) for 8 hours of coping, and for passive designs coping of 72 hours with batteries.
10 CFR 50.65 (Maintenance Rule)	Requirement for monitoring the effectiveness of maintenance at nuclear power plants. Risk insights were used to select safety systems to be monitored. Risk controls were also required to be implemented by license, “the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities.” The scope of the assessment may be limited to structures, systems, and components that a risk-informed evaluation process has determined are significant to public health and safety.
10 CFR 50.69 (Special Treatment)	This will be discussed within this report [RG 1.174 and RG 1.201].
10 CFR Part 52 (Licenses, Certifications, and Approval for Nuclear Power Plants)	10 CFR 52.47 requires design-specific probabilistic risk assessment and its results (generally documented in Chapter 19). Severe Accident Mitigation Design Alternative (SAMDA) and postulated accidents (generally included in environmental assessment). Scattered throughout 10 CFR Part 52 are all previous NRC risk-informed applications, such as ATWS rule, SBO rule, etc.)

Risk Application Area	**Summary Description**
Risk-Informed Technical Specification Initiative (TSTF-505/4b)	This will be discussed within this report [RG 1.174 and RG1.177].
Surveillance Frequency Initiative (TSTF-505/4b)	This will be discussed within this report [RG 1.174 and RG1.177].
Generic Issue Prioritization/Emergent Issues (LIC 504)	Integrated Risk-Informed Decision-Making Process for screening emergent issues. This guide uses both conditional and incremental risk criteria (different than RG 1.174), however uses the five principles as RG 1.174.
Reactor Oversight Program (ROP) Significance Determination Process (SDP)	ROP basis document, IMC 0308, defines risk criteria based on “GREEN” to “RED” findings. The risk is defined by ΔCDF and ΔLERF when findings are related to an increase in failure rate of a basic event or a class of basic events. When findings relate to an adverse condition that existed for some duration, the more appropriate risk metrics should be ΔCDP and ΔLERP. The criteria for RED findings correspond to RG 1.174, not differentiating between frequency or probability (e.g., ΔCDF/ΔLERF and ΔCDP/ΔLERP.
Incident Investigation (MD 8.3)	It discusses the process of responding to an event across all NRC-regulated facilities. The events may involve responses by an incident investigation team (IIT) or less formal responses by an augmented inspection team (AIT) or a special inspection team (SIT), depending on the level of response required. The type of response is defined by a set of criteria including risk criteria (for power reactor only). The risk criteria for power reactors are defined based on conditional core damage probability (CCDP).
Accident Sequence Precursor (ASP)	The ASP Program systematically evaluates U.S. nuclear power plant operating experience to identify, document, and rank operational events by calculating a CCDP for an event, or an increase in core damage probability (ΔCDP) for a condition.
Containment Sump Clogging (GSI-191)	NRC allowed licensee to adopt a risk-informed resolution to Generic Safety Issue-191 (SECY-10-113 and SECY-12-0093). RG 1.174 was implemented to select between alternative resolutions, including accepting low-risk sump blockage scenarios.
Integrated Leak Rate testing (ILRT)	This is similar to changing surveillance frequency for integrated leak rate tests (ILRT) using the guidance of RG 1.174.
10 CFR 50.54 (hh)(2): Extensive Damage Mitigating Guidelines	B5b was a prescriptive/deterministic rule and did not include any risk-informed guidance.

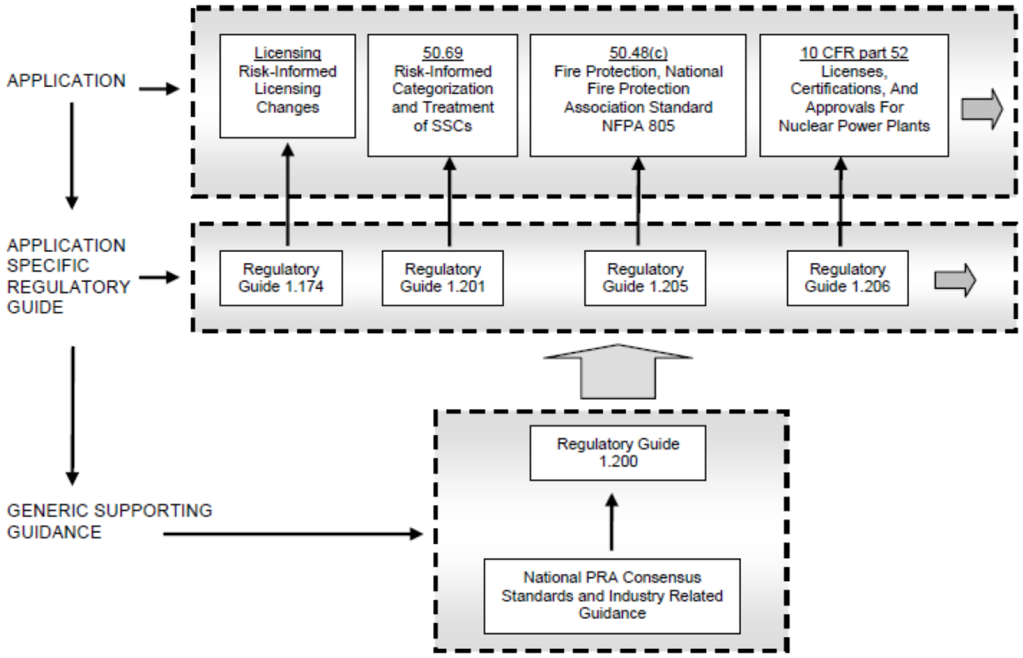
Risk Application Area	Summary Description
	However, it was found during evaluation of the identified strategies that use of PRA personnel and PRA insights was beneficial. PRA insights could identify the existing plant equipment and procedures that could help B5b strategies, and PRA personnel could identify the areas of plant risk from causes other than security threats that could benefit from the B5b equipment and strategies.
NTTF (Near Term Task Force Recommendation)	FLEX, seismic PRA (multi-facility issue), Severe Accident Management Guidelines (SAMG), containment venting, spent fuel pool accidents, flood hazard re-evaluation, etc.
Others: Shutdown Risk, decay heat removal (DHR) reliability, AFW reliability goals, reactor coolant pump seal loss-of-coolant accidents (LOCAs), Rosemont pressure transmitters, etc.	There have been many PRA applications and risk-informed decisions by NRC that are not discussed in the previous rows of this table. This row is devoted to disposition of many risk issues from Three Mile Island (TMI) action plans, generic issue prioritization, industry-wide emergent issues (e.g., those identified by Bulletins), etc.

C.2 RISK-INFORMED FRAMEWORK AT NRC

The current use of the NRC risk-informed regulatory framework is to support decisions to modify an individual plant’s licensing basis (LB). The LB consists of those licensee commitments (modifications, changes in process, or upgrades e.g., limiting conditions for operations (LCO) at the plant) that if modified, would require NRC approval. These modifications could include items such as exemption requests under 10 CFR 50.11, “Exceptions and exemptions from licensing requirements,” and license amendments under 10 CFR 50.90, “Application for amendment of license, construction permit, or early site permit,” for example, license amendment requests for technical specification changes.

The current set of regulatory guides and their relationships are shown in Figure C-1 (reproduced from Regulatory Guide (RG) 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis” [Ref. 3]. These regulatory guides (except RG 1.206, “Applications for Nuclear Power Plants,” for 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”) are generally intended for risk-informed regulatory changes after the design is complete, the plant is constructed, commissioned, and licensed for operation.

NRC will review applications for license amendments using traditional deterministic methods. However, NRC could request an analysis of the risk impact related to the requested change of the LB, to demonstrate that the level of protection necessary to avoid undue risk to public health and safety (i.e., “adequate protection”) is present. This could also occur under special cases in which new information reveals an unforeseen hazard or a substantially greater potential for a known hazard to occur. Licensees may also utilize the risk-informed regulatory framework to further support the acceptability of the requested changes in LB due to specific enhanced design and operational features in their plant beyond what is generally credited in a traditional deterministic evaluation.



APPLICATION
APPLICATION SPECIFIC REGULATORY GUIDE
GENERIC SUPPORTING GUIDANCE
Licensing
Risk-Informed Licensing Changes
50.69
Risk-Informed Categorization and Treatment of SSCs
50.48(c)
Fire Protection, National Fire Protection Association Standard NFPA 805
10 CFR part 52
Licenses, Certifications, And Approvals For Nuclear Power Plants
Regulatory Guide 1.174
Regulatory Guide 1.201
Regulatory Guide 1.205
Regulatory Guide 1.206
Regulatory Guide 1.200
National PRA Consensus Standards and Industry Related Guidance

Figure C-1 Regulatory Guides for the NRC Risk-Informed Regulatory Framework and Their Relationship

Risk insights have also been integrated into the NRC regulatory framework beyond those covered by the set of regulatory guides described above. Additional risk-informed regulatory activities have been implemented for the licensing of advanced reactors (10 CFR Part 52) and the next generation of nuclear power plants.

In the following sections, a discussion is provided on five regulatory guides (RG 1.174; RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities”; RG 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance”; RG 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants”; and RG 1.177, “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications”), which are considered relevant to this project.

C.2.1 <u>Summary of RG 1.174</u>

Regulatory Guide 1.174 [Ref. 3] describes an acceptable approach for assessing the impact of proposed LB changes by considering safety margins, defense-in-depth, and risk insights. This guide also addresses implementation strategies and performance monitoring plans associated with LB changes that will help ensure that assumptions and analyses supporting the change are verified.

In addition to maintaining sufficient defense-in-depth and sufficient margins, RG 1.174 establishes risk controls based on safety goals in the form of the predicted changes in risk results caused by LB change requests. The risk controls based on the safety goal and subsidiary objectives are used to ensure that nuclear power plants operate routinely at a prudent margin above adequate protection.

The risk controls are set at two levels, core damage frequency (CDF) and large early release frequency (LERF). CDF and LERF are estimated for various modes of reactor operations such as power, low power, shutdown, or refueling, and for all internal and external hazards[36]. All CDF contributors are summed and annualized. Core damage is considered a major accident that envelopes all possible consequences such as late fatality, environmental and property impact of major accidents. LERF is being used as a surrogate for the early fatality "Quantitative Health Objective." It is defined as the sum of the frequencies of those accidents leading to rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of offsite emergency response and protective actions such that there is the potential for early health effects. Such accidents generally include unscrubbed releases associated with early containment failure shortly after vessel breach, containment bypass events, and loss of containment isolation.

RG 1.174 requires that the following five principles are met and included in the applications:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption (i.e., a specific exemption under 10 CFR 50.12, "Specific Exemptions").
2. The proposed change is consistent with a defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.
5. The impact of the proposed change should be monitored using performance measurement strategies.

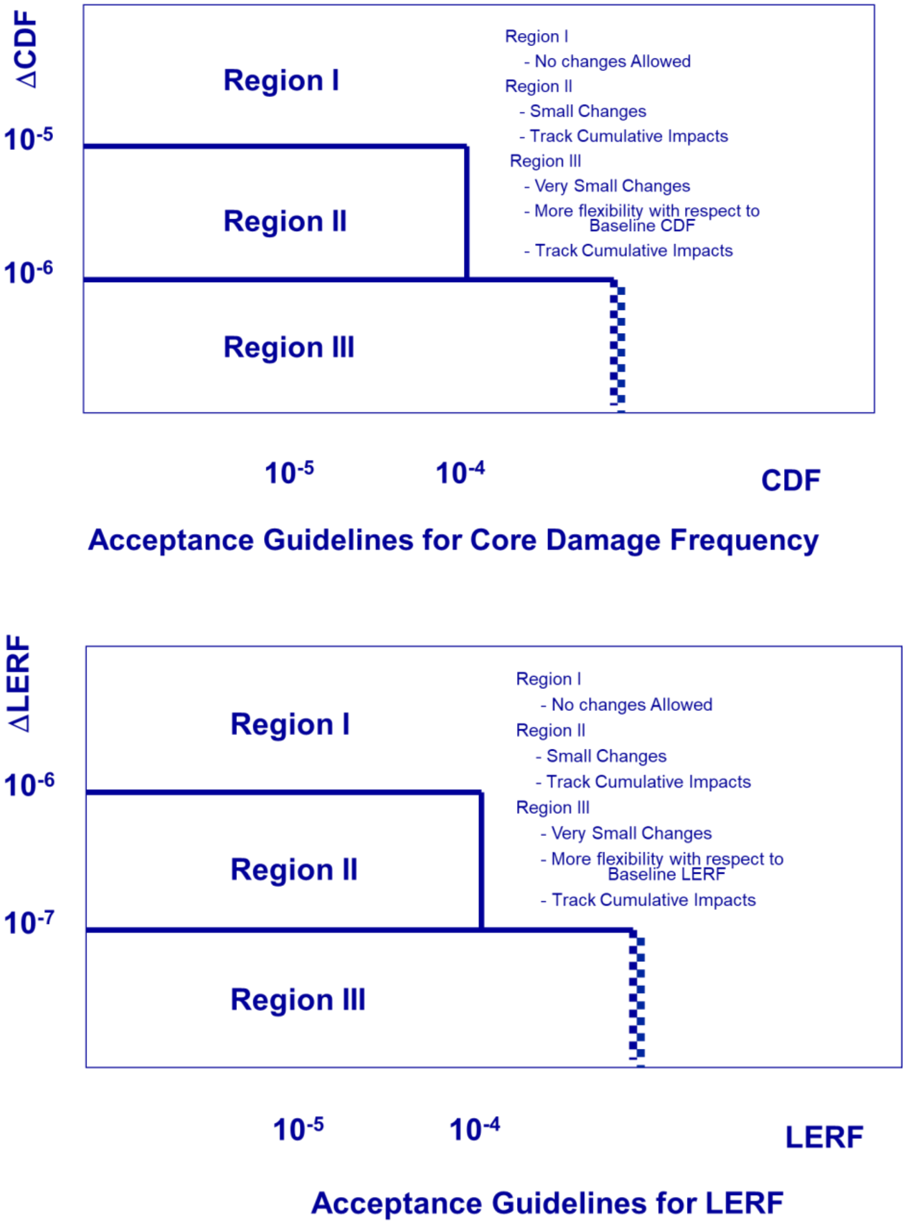
The first three principles are related to traditional deterministic analysis. The fourth principle is based on quantitative risk analysis. The fifth principle is a monitoring program limited to ensuring that the assertions and predictions made in Principle 4 are verified and not violated.

Risk controls for RG 1.174 are shown in Figure C-2 (reproduced from RG 1.174) for both CDF/ΔCDF and LERF/ΔLERF. The three regions are identified for the LERF and CDF metrics. The most limiting regions of LERF and CDF will apply.

When the increase in CDF and LERF are very small, less than 10^{-6} and 10^{-7} per reactor year, respectively, the change will always be accepted (Region III). If either annualized CDF or LERF significantly exceeds 10^{-4} and 10^{-5}, respectively, the change will not usually be considered since the focus should be on finding ways to decrease them (Region I).

[36] The necessary scope and sophistication of the evaluation depends on the perceived contribution of the risk. In most cases, as a minimum, a quality PRA for internal hazards at-power only is used for the base case analysis. For all other hazards and modes of operation, the applicant should show that the changes of LB have no impact or should show qualitatively that the impact is negligible. When the risk from other hazards or modes of operations must be quantitatively evaluated to show the risk impact of the LB change is not significant, a detailed PRA or bounding analysis (sometimes referred to scaling) would be necessary to evaluate the risk impact of the LB change.

These risk guidelines are applicable for at-power, low-power, and shutdown operations. However, during certain shutdown operations when the containment function is not maintained, licensees may use more stringent baseline CDF guidelines to ensure the LERF guideline is met (e.g., 10^{-5} for annualized CDF).



Acceptance Guidelines for Core Damage Frequency

Acceptance Guidelines for LERF

Figure C-2 Risk Controls from RG 1.174

RG 1.174 identifies three sources of uncertainties, (1) parametric, (2) model, and (3) completeness. The RG asserts that the analysis of parametric uncertainty is mature (i.e., it is addressed adequately through the use of mean values). The analysis of the model and completeness uncertainties cannot be handled in such a formal manner. It generally requires that the applicant shows the robustness of the results through sensitivity analysis. It will be incumbent on the licensee to demonstrate that the choice of reasonable alternative hypotheses, adjustment factors, or modeling approximations or methods to those adopted in the PRA model will not significantly change the assessment. NUREG-1855, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making” [Ref.4], shall be consulted in this regard.

C.2.1.1 Lessons from Applications of RG 1.174

RG 1.174 describes a process that can be used for any risk-informed application for LB changes. RG 1.174 could also be used for risk informing digital instrumentation and controls (DI&C) systems similar to previous applications for mechanical and electrical systems. Here the focus is on the generic nature of RG 1.174 when used to support LB changes to DI&C systems.

The risk-informed portion of RG 1.174 describes a fully quantitative process. The user should first evaluate and characterize the impact of requested changes in terms of quantities that could be used within PRA models and data structures. PRAs should also be detailed enough and be of sufficient scope to allow the impact of changes to be incorporated. The uncertainties associated with the changes on PRA input and the uncertainties associated with PRA models and data (without the impact of changes) as reflected on risk metrics (CDF/ΔCDF and LERF/ΔLERF) could also be evaluated.

The experience shows that, for some applications, the impact of changes on PRA input are quite uncertain, or the PRA models and data do not explicitly address the risk impact of the proposed changes in a comprehensive manner. In such cases, different approaches are implemented. These approaches may include the use of somewhat different risk matrices (conditional risk metrics) or the use of prioritization schemes, such as importance measures supplemented by other qualitative and engineering control measures. Specific cases will be discussed under the discussion for other risk-informed RGs (e.g., RG 1.177 and RG 1.201).

The first three steps of RG 1.174 are deterministic principles. They must all be met before a risk-informed approach can be applied to justify the proposed changes. Deterministic principles address single failure criteria, defense-in-depth, and safety margins (balance between mitigation and control of consequences). There could be several proposed changes that meet the deterministic principles. The fourth principle, acceptable risk metrics/insights, will help to select a suitable option out of the set of acceptable alternative~~s~~ (i.e., changes), which are acceptable to NRC and efficient for the licensee. The deterministic principles are prescriptive in nature. As an example, redundancy will be treated the same for single failure criteria regardless of the failure probability for the redundant trains (e.g., a redundant motor driven pump is treated the same as a redundant turbine driven pump).

The following lessons are generically identified for RG 1.174:

1. The principles and the integrated approach delineated in RG 1.174 have been successfully applied to many risk-informed applications, including those discussed in this appendix.
2. There have been some shortcomings in applying RG 1.174, but they were generally driven by large uncertainties for characterizing the impact of changes probabilistically or the lack of PRA scope and level of detail to evaluate the change in risk metrics [Ref. 1].

3. The rigidness of risk metrics and their associated criteria has limited the application of this RG to advanced and the next generation of power reactors where the risk metrics are much lower.
4. Generally, no formal risk insights are used to streamline the reviews and acceptability of the first three principles in RG 1.174. The use of risk insights could increase the regulatory efficiency and facilitate a graded review of the first three qualitative/engineering principles. Risk-informed prioritization methods can be used to support this objective. Other industries have used qualitative methods such as hazard and operational assessment (HAZOP) analysis and quantitative sensitivity analyses using the base PRA. Similar approaches could be implemented for NRC. Quantitative methods using the original PRA model without the I&C system combined with a sensitivity analysis can provide the initial prioritization of various systems. The process is similar to that of RG 1.201, which is discussed later for structures, systems, and component (SSC) classification.
5. Repeated use of RG 1.174 for several applications, one at a time, may increase overall risk and it could approach the risk goals.

C.2.1.2 AI&C/DI&C PRA Challenges to Support RG 1.174

Successful use of RG 1.174 to DI&C systems demands that the PRAs meet the following attributes, which also apply to analog instrumentation and controls (AI&C) systems:

(1) The ability to characterize the effect of the changes, probabilistically and systematically, at the level that they are applied and can be modeled in PRAs. This is important for any changes in AI&C/DI&C system designs. A change in AI&C/DI&C can introduce some failure modes that are not in PRA (e.g. spurious actuations) or a change may impact an accident sequence that is screened out of the PRA. In such cases, PRA models must be modified to accommodate the specific system failure modes.

(2) The ability of the PRA to allow the incorporation of change effect. PRAs must be detailed enough to explicitly incorporate the effect of change either through input modifications or changing the models. This could vary depending on the changes requested.

(3) The ability of the PRA to account for all hazards and contributors to risk. PRAs must have the appropriate scope to evaluate the impact of changes under all hazards, all relevant accident scenarios, and all possible environmental conditions. The required scope of the PRA also depends on the changes requested. Some changes may require external hazards and others may not. Some applications may be performed without full development of all Level 2 scenarios and some may not.

(4) The ability of the PRA to estimate the risk metrics and the associated changes in an acceptable manner. Acceptable manner is generally defined as meeting PRA standards [RG 1.200 [Ref. 5], peer-review [Refs. 6, 7], and PRA quality control. These documents must be examined to verify their adequacy of addressing AI&C/DI&C.

(5) The ability of the PRA to estimate the mean values of risk metrics by accounting for all sources of uncertainties [Ref. 4]. The issue of uncertainties is currently geared towards the overall results of PRAs and does not focus on the uncertainties associated with the effect of changes. For example, the effect of a set of changes may have a small impact on the mean value of CDF (i.e., ΔCDF) but could significantly affect the lower or upper bound of ΔCDF.

C.2.2 Summary of RG 1.177

Licensee-initiated technical specification (TS) change requests may be evaluated by the staff using traditional engineering analyses as well as the risk-informed approach set forth in RG 1.177 [Ref. 8]. Technical Specifications include: (1) safety limits, limiting safety system settings, and limiting control settings; (2) limiting conditions for operation (LCOs); (3) surveillance requirements (SRs); (4) design features; and (5) administrative controls. This RG, however, addresses two categories of TS, LCO and SRs. A duration in which a plant can reside in an LCO is limited by allowed outage time (AOT), which is also referred to as completion times (CTs). Limiting CTs reduces the chance that an accident occurs during the LCO. CTs are determined to ensure enough time is available for recovery and repair, and at the same time, avoiding unnecessary risk. The frequency of surveillance testing (surveillance frequency [SF]) is directly related to the reliability of a standby component. More frequent testing can reveal failures and degradation and reduces exposure time (the duration that a failure can be hidden without discovery and repair). Too frequent testing can increase the unavailability of the component, thus, the component may not be available to perform its function, may cause inadvertent transients[37], and could trigger unnecessary wear-out. Again, a balance must be achieved between the consideration of risk controls and sound engineering practice.

Although both LCOs and SRs are discussed in RG 1.177, here we will only focus on CTs associated with LCOs, i.e., risk-informed completion times (RICT). An interested reader can refer to RG 1.177 for risk-informed surveillance frequency.

Like RG 1.174, RG 1.177 follows five principles. These principles are listed below:

1. The proposed change meets the current regulations unless it is explicitly related to a requested exemption.
2. The proposed change is consistent with the defense-in-depth philosophy.
3. The proposed change maintains sufficient safety margins.
4. When proposed changes result in an increase in core damage frequency (CDF) or risk, the increases should be small and consistent with the intent of the Commission’s safety goal policy statement.
5. The impact of the proposed change should be monitored using performance measurement strategies.

TS conditions addressed by CTs are entered infrequently and are temporary by nature. However, TS do not typically restrict the frequency of entry into conditions addressed by CTs. Therefore, the following TS acceptance guidelines specific to CT[38] changes are provided for evaluating the risk associated with the revised CT:

1. The licensee has demonstrated that the CT change has only a small quantitative impact on plant risk. An incremental conditional core damage probability (ICCDP)[39] of less than

[37] For example, the calibration of relays in the reactor protection system could cause plant transients; the risk from the test-caused transients is then having to be estimated and accounted for.

[38] Permanent changes to CT are discussed in this section. There are similar guidelines for a one-time change that is not discussed here.

[39] ICCDP = ((conditional CDF with the subject equipment out of service and nominal expected equipment

1.0×10^{-6} and an incremental conditional large early release probability (ICLERP)[40] of less than 1.0×10^{-7} are considered small for a single TS condition entry (Tier 1).

2. The licensee has demonstrated that there are appropriate restrictions on dominant risk-significant configurations associated with the change (Tier 2).
3. The licensee has implemented a risk-informed plant configuration control program. The licensee has implemented procedures to utilize, maintain, and control such a program (Tier 3).

The above guidelines were developed since the impact of changes in CTs in terms of PRA input (component unavailability) cannot be fully characterized.

One way to verify that the increased risk from RICTs is consistent with RG 1.174 is by-the implementation of a third-tier element, the monitoring program, to ensure that the extension of CTs or the reduction of SFs do not degrade operational safety over time. One element of the third-tier approach is to monitor the cumulative risk (core damage probability [CDP] and large early release probability [LERP]) resulting from the cases when the extended CT as allowed by the RICT program have been relied on. This cumulative change in risk, accounting for its uncertainties, then could be used to show compliance with RG 1.174. Furthermore, the licensee should ensure, as part of its Maintenance Rule program (10 CFR 50.65), that when equipment does not meet its performance criteria, the evaluation required under the Maintenance Rule includes TS changes.

C.2.2.1 Lessons from Application of RG 1.177

The application of RG 1.177 to CT and SFs is perhaps one of the most widely used risk-informed application in the U.S. This is because it is a straightforward, quantitative, risk-informed application with minimum demand for PRA level of detail and scope.

There are some areas where RG 1.177 may need further clarification. These are discussed below.

Predicting the Impact of Change

RG 1.177 is a quantitative risk application similar to what was discussed for RG 1.174, however with different quantitative risk criteria. For a quantitative process, the user should first evaluate and characterize the impact of the requested changes in terms of quantities that could be used within the PRA model and data structure. To characterize the impact of a change in CTs, one should estimate how often the CT change will be triggered. This requires the estimates of the number of times that the plant enters a specific LCO, and the fraction of those with which the repair is not completed within the original CTs. As an example, an LCO could be entered for the repair of a failure or a degraded condition, and there is a probability that the repair duration could exceed the existing CTs. The frequency of entering in an LCO is generally a factor multiplied by the component failure rate (e.g., a factor of 3.5) to account for degraded conditions as well as failures. The risk impact of failures is different than that of degraded condition owing

unavailability for other equipment permitted to be out of service by the TS) − (baseline CDF with nominal expected equipment unavailability)) x (total duration of single CT under consideration).

[40] ICLERP = ((conditional LERF with the subject equipment out of service and nominal expected equipment unavailability for other equipment permitted to be out of service by the TS) − (baseline LERF with nominal expected equipment unavailability)) x (total duration of single CT under consideration).

to the possibility of CCFs. One could therefore estimate the impact of CT changes in terms of changes in maintenance unavailability and follow the guidelines in RG 1.174. RG 1.177 does not consider that the impact of changes in terms of PRA input and models can be characterized in full probabilistic terms. It states, "TS conditions addressed by CTs are entered infrequently and are temporary by their very nature. However, TS do not typically restrict the frequency of entry into conditions addressed by CTs."

To accommodate for this shortcoming, i.e., lack of probabilistically characterizing the change, the RG modifies the risk metrics. Although this step may not have been necessary, it can be justified since the risk associated with TS changes are expected to be small and infrequent.

Limited Application to I&C Systems

Past applications of Risk Informed Technical Specifications (RITS) for I&C systems were generally applied to the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS). A mapping of the number of ways a reactor trip or ESF actuation can occur for each of the postulated plant accidents are generally noted in Chapter 15 of the final safety analysis report (FSAR). This information could be used to determine the level of redundancy in RTS and ESFAS for each accident initiator. For example, for steam generator tube rupture (SGTR), the reactor trip and ESF actuation can occur due to low pressurizer pressure and over-temperature ΔT. FSAR Chapter 7 should then be consulted on a level of redundancy; for example, for over-temperature ΔT, coincident logic of 2 out of 3 would be required to actuate ESFAS. It should also be noted that manual actions (for reactor trip and ESFAS) can be credited in many of the initiators. The redundant signals are generally diverse with no intra connections between different signal channels.

RTS/ESF channels are designed with sufficient redundancy for individual channel calibration and tests to be made during power operation without degrading the reactor protection. In general, removal of the channel for calibration/surveillance is accomplished by placing the channel in a partial-trip mode. In such cases, a two-out-of-three channel becomes a one-out-of-two channel. When channel testing and calibration occurs during an LCO, the number of available redundancies would decrease. The ability of in-service testability without causing undue risk (maintaining sufficient redundancy) is also examined.

Most of the PRAs for the current generation of operating light-water reactors (LWRs) do not model RTS and ESFAS in detail. Individual RTS instrumentation channel input to the automatic RTS functions will be evaluated using a bounding method as permitted by NEI 06-09, "Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines," or use of a conservative surrogate model. Specific instructions are provided in NEI 06-09 [Ref. 9]. The rationale and instructions in NEI 06-09 are described below.

Two or more diverse RTS signals are generated for any initiating event. The failure probability of the automatic RTS function is typically dominated by failure of the common non-instrumentation components in the RTS system. The PRA logic addresses the failure of the automatic trip function when two of the two generic RTS signals fail to actuate using a model based on NUREG/CR-5500, "Reliability Study: Westinghouse Reactor. Protection System, 1984–1995." [Ref. 10]. This reference conservatively assumes any initiating event only results in two reactor trip signals.

For the RICT Program, (1) any inoperability of one channel of any RTS functional unit will conservatively be assumed to result in the unavailability of that signal as an input to the automatic RTS function; (2) the risk for one inoperable instrument channel for one RTS functional unit will be evaluated assuming that one of the two generic RTS signals is unavailable, and conservatively crediting only one remaining signal for automatic reactor trip for all initiating events; (3) if two or more RTS functional units have inoperable instrument channels, then no credit will be taken for the automatic RTS function by assuming unavailability of both generic RTS signal inputs.

It is conservative because (1) the inoperability of any single instrument channel for any RTS function is evaluated as causing the loss of that RTS function even if the remaining channels would actuate a reactor trip; (2) the inoperability of any RTS signal is assumed to impact the mitigation of transient and accident conditions, even though only a subset of initiating events would be impacted; and (3) no credit is taken for automatic RTS actuation for more than two RTS signal failures for any initiating event.

The risk-informed TS process impacts the plant risk in three different manners. These are as follows:

1. Controlling single RICT risk increase through controlling ICCDP of less than $1.0\text{x}10^{-6}$ and an ICLERP of less than $1.0\text{x}10^{-7}$ (Tier 1).
2. Reducing risk by imposing additional restrictions on dominant risk-significant configurations associated with the change (Tier 2). These are sometimes referred to as risk managed actions (RMA) and risk managed actions times (RMATs).
3. Reducing risk by implementing a risk-informed plant configuration control program. The licensee has implemented procedures to utilize, maintain, and control such a program (Tier 3). This is sometimes referred to the Configuration Risk Management Program (CRMP).

The overall risk from implementing a risk-informed TS process could be smaller than the risk evaluated in Tier 1 calculations due to the added non-quantifiable benefit from activities in Tiers 2 and 3.

The approach for RTS and ESFAS, as discussed above, could address the Tier 1 needs regarding the determination of RICT; however, it will not be able to explicitly address the Tier 2 and Tier 3 information needs due to the lack of a detailed PRA model. For example, it would be difficult to evaluate the impact on the RICT estimates if there is a simultaneous outage of one channel of low pressurizer pressure and one channel of over-temperature ΔT. Such estimates are generally provided by the CRMP, which requires a more detailed PRA model for these systems. Alternative approaches using conservative qualitive methods are generally used to supplement the lack of detailed PRA models, including any relevant RMAs that may apply. Finally, it may not be appropriate to treat all different types of trains within a channel as the same. A channel could include, a sensor (instrumentation), signal conditioning circuit, logic channel, and most probably a relay-based actuator (coil). It is not clear that RICT is typically dominated by the failure of the common non-instrumentation components. It is also possible that components, such as relays and associated coils, could have a much higher CCF contribution.

Treatment of External Events

The PRA modeling of internal events for TS application shall meet the requirements of RG 1.200 and Category 2 PRA quality as defined by the PRA standard. The contribution of external event risk, however, could be included using one of the following three options:

1. Screening the hazard based on a low frequency of occurrence,
2. Bounding the potential impact and including it in the decision-making, or
3. Developing a PRA model to be used in the RICT calculation.

For most common electrical and mechanical systems, Options 1 and 2 are mostly used since the risk associated with CT (an LCO condition) is small. This is mainly because the system unavailability from other causes is generally much larger. This may not be true for AI&C/DI&C systems. Any external event causing reduction of redundancy in I&C could also significantly increase the risk importance of the unaffected train. Also defining the RMAs and the associated RMATs will become more important for the I&C system when anticipating or during an external event.

Option 3, developing a PRA model, is the most desirable option due to the specific reliability characteristics of AI&C/DI&C. This requires evaluating the impact of external events, such as flood and fire on I&C systems, and the associated operator diagnostic aids. In addition, the use of PRA in Option 3 facilitates the use of tools and models that can support Tier 2 activities, which include CRMs and RMAs. This may increase the required scope of the PRA to include external events, especially fire and flood. The possibility that fire and flood could potentially damage I&C equipment and their support system is plausible. Failures and the unavailability of I&C systems can also impact operator actions, depending on the specific initiator and the associated scenarios.

In summary, RG 1.177 relies on multiple layers of risk controls ensuring robustness against possible uncertainties that may not have been accounted for. This is like defense-in-depth for the risk-informing process.

C.2.2.2 AI&C/DI&C PRA Challenges to Support RG 1.177

The following PRA challenges were identified for current and future use of RG 1.177 for AI&C/DI&C systems.

Scope of I&C Systems to be Modeled in PRA

The RICT for I&C systems associated with the RTS and ESFAS are generally considered by the licensees for RG 1.177 applications. There is currently no application for other systems. Furthermore, risk-informed applications have not been used for changes in the safety limit setting or other design issues that can affect the principle design criteria and design basis of RTS and ESFAS.

Impact of I&C System Failures on Human Reliability Analysis (HRA)

The equivalent RPS and ESFAS, as well as other DI&C systems for new reactors and next generation reactors, appear to perform additional functions, such as providing information for operator diagnostic aids. The changes of operator error rate as a result of missing information or erroneous information should be accounted for in PRAs.

Developing I&C PRA Meeting CRMP Needs

The AI&C/DI&C systems can operate in several modes as selected by the operator for specific conditions. CRMP models for AI&C/DI&C systems not only should account for the status of equipment but should use proper fault tree models for the I&C mode of operation. This could require the modification in current CRMP tools.

Level of Detail in PRA

The level of detail in a PRA to support an application should be consistent with the level at which the risk-informed changes are applied. The RICT is usually applied at the level of testable module or a major component. This would correspond to a modular level of detail for the AI&C/DI&C system in a PRA. The RICT would impact the unavailability of components and systems due to maintenance downtime. The PRA should model the unavailability contributions in addition to the failure per demand for the AI&C/DI&C systems. There are many challenges in modeling the unavailability contributions of AI&C/DI&C systems due to online diagnostics, fault tolerances, and periodic testing that must be addressed. It also should be noted that some faults are transient and are generally resolved when the system restarts. The duration of downtime for such cases is short and may not challenge the RICT. Generally, the faults that are detectable using defensive measures and early diagnostics could be resolved in a short period of time and do not challenge CT extension through RICT. The RICT, therefore, would be needed for system upgrades or replacement, either preplanned or forced (unexpected).

PRA Scope/External Events

As discussed earlier, the implementation of RG 1.177 for I&C systems requires evaluating the impact of external events such as flood and fire on I&C systems and the associated operator diagnostic aids. In addition, the PRA requires the tools and models that can support Tier 2 activities, which include CRMs and RMAs. In summary, the PRA scope for the current application in operating reactors is considered limited but it may not hold (should be examined) for new reactors.

Functional versus Physical System

The use of software in DI&C facilitates integrating many functions into one system. However, these functions need to be decomposed in the PRA model to support a risk-informed application. The issue of our interest is related to functional versus physical system modeling of AI&C/DI&C in PRAs. In some cases, a single I&C system with a physical boundary definition integrates the controls and actuations of many other systems in response to a specific accident condition. Failure to actuate or spuriously actuate a system could impact the accident scenario and carry different importance to risk. For example, the scram logic software integrates the scram functions for many different physical conditions (e.g., the failure to scram due to steam generator tube rupture, and the failure to scram due to loss of flow). The physical boundaries of I&C systems, including its software, should be decomposed into individual systems for PRA-modeling purposes. I&C systems should be modeled in the PRA like electrical systems supporting several other systems[41]. Detailed modeling of I&C systems with multiple basic

[41] The use of term, “PRA support system,” should not be misconstrued as the regulatory terms and its use of the term, “support system.”

events can help the integration of PRA insights in line with the defense-in-depth concept and provides context to software failure and the associated data and models.

C.2.3 Summary of RG 1.201

RG 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance” [Ref.11], allows licensees to use a risk-informed process for categorizing SSCs according to their safety significance. SSCs of low safety significance can be removed from the scope of certain identified special treatment requirements.

This RG describes a method that the NRC staff considers acceptable for use in complying with the Commission’s requirements in 10 CFR 50.69, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors,” with respect to the categorization of SSCs that are considered in risk-informing special treatment requirements. This categorization method uses the process that the Nuclear Energy Institute (NEI) described in Revision 0 of its guidance document NEI 00-04 [Ref.12][42]. This process determines the safety significance of SSCs and categorizes them into one of four risk-informed safety class (RISC) categories. The provisions of 10 CFR 50.69 allow adjustment of the scope of SSCs subject to special treatment requirements (e.g., quality assurance, testing, inspection, condition monitoring, assessment, reporting requirements, and evaluation) based on an integrated and systematic risk-informed process that is discussed within RG 1.201.

The safety significance of SSCs is determined using an integrated decision-making process, which incorporates both risk and traditional engineering insights. The safety functions of SSCs include both the design-basis functions (derived from the safety-related definition) and functions credited for preventing and/or mitigating severe accidents. This results in SSCs being grouped into one of four categories, as represented by the four boxes in Figure C-3.

Generally, there are two types of functions performed by categorized SSCs; the design basis (DB) function, such as that considered in Chapter 15 of the FSAR for accident analysis, and the PRA functions, such as all mitigation capabilities accounted for in PRAs. Category 1 SSCs perform functions in DB space and are risk significant for the PRA-based (PB) functions. Category 2 by design should not play any role in the DB function but they should be important (risk significant) for the PRA function.

[42] NEI 00-04 (Rev 0), “10 CFR 50.69 SSC Categorization Guideline,” July 2005.

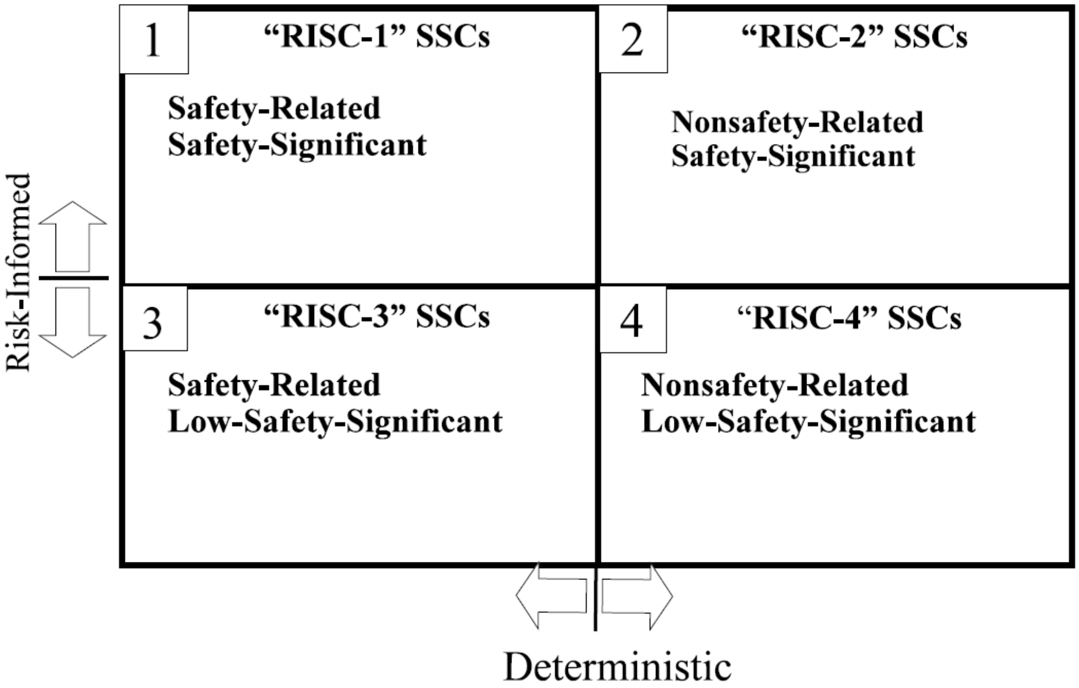


Figure C-3 Risk-Informed Safety Class (RISC) Categorization (duplicated from RG 1.201)

Category 3 is important for DB but not risk significant for the PB function. Finally, Category 4 SSCs are neither important for DB nor risk significant for the PB function. It is obvious that the requirements for SSCs in Category RISC-1 cannot be relaxed. Low risk significance of Category RISC-4 equipment may indicate that they are not significantly relied on during severe accidents[43]. There is no alternative or special treatment required for RISC-4 category equipment. They are generally treated the same as non-safety SSCs.

Alternative requirements for Category 3 SSCs as stated in 10 CFR 50.69 shall ensure, with reasonable confidence, that the SSCs remain capable of performing their safety-related functions under DB conditions, including seismic conditions and environmental conditions and effects throughout their service life.

Alternative requirements for Category 2 SSCs, as stated in 10 CFR 50.69, shall ensure that the SSCs perform their functions consistent with the categorization process assumptions by evaluating the treatment being applied to these SSCs to ensure that it supports the key assumptions in the categorization process relating to their assumed performance.

The categorization process involves several steps. The easiest way to describe these steps is first to assume the plant PRA is of such a scope and level of detail that all SSCs in the plant identified by system engineering assessment for categorization can be categorized. We do understand current PRAs do not have sufficient scope and level of detail to support

[43] Low risk significance generally occurs during PB events when there are many ways to mitigate an accident, including a success path, which involves the equipment of interest (mitigation redundancy and diversity is greater than 2) or it could be because the equipment of interest is rarely needed (low frequency of demand, low likelihood of initiator followed by failure of a low-probability event, such as a passive component failure).

categorization of all SSCs; however, this issue will become more clear later in our discussion. Under this assumption, there are only three steps involved.

The first step in the process is the initial engineering evaluation of a selected system to support the categorization process. This includes the definition of the system boundary to be used and the components to be evaluated, the identification of system functions, and a coarse mapping of components to functions. The system's functions are identified from a variety of sources including design/licensing basis analyses, Maintenance Rule assessments, and PRA analyses. The mapping of components is performed to allow the correlation of PB events to system functions.

The second step in the process is to use the PRA to differentiate between the high safety significance versus low safety significance (HSS and LSS) SSCs. This is currently done using importance measures such as Fussell Vesely (FV) and Risk Achievement Worth (RAW). The PRA-designated HSS components will be categorized to RISC-1 or RISC-2, depending on whether they play any role in DB events.

In the third step, the PRA-designated LSS components will be assigned to RISC-3 and RISC-4 depending on their function during DB.

Finally, in the fourth step, the qualitative deterministic considerations are used to ensure that the PRA assignment of LSS does not contradict the deterministic regulatory criteria. This is done through three different means: (1) examination of defense-in-depth (DID), (2) risk sensitivity studies (RSS), and (3) Integrated Decision-making Panel (IDP). These three steps taken by the applicants for a case of a full scope and detailed PRA can only be used to change the PRA designated LSS SSCs to HSS (not identifying new HSS components)

Defense-in-depth addresses the role of components in preserving defense-in-depth related to core damage, large early release, and long-term containment integrity. RSS is performed to investigate the aggregate impact of the potentially changing treatment of those low safety-significant SSCs (mainly RISC-3). The IDP is a multi-disciplined team that reviews the information developed by the categorization team. The IDP uses the information and insights developed in the preliminary categorization process and combines that with other information from design bases and defense-in-depth assessment to finalizing the categorization of functions.

However, the current state of practice for PRAs will only explicitly[44] cover a subset of SSCs and a subset of the functions they perform. This is done using the three qualitative reviews (DID, RSS, and IDP) identified earlier but usually without the added benefit of the PRA results and reasoning. These steps for this case will identify and categorize SSCs that are not explicitly modeled in PRA. This process will classify additional SSCs to supplement the PRA limitations. These qualitative reviews are intended to identify new HSS components or changing the PRA designated LSS SSCs to HSS (not the reverse).

The importance measures and the associated criteria used in RG 1.201 were used previously for other applications (e.g., Maintenance Rule) dealing with conventional electrical and

[44] "Explicit" refers to an element in PRA such as a basic event or an initiator for which risk importance measures can be automatically calculated without any PRA manipulation. There are many additional implicit considerations in PRAs for which determination of risk importance measures may require PRA manipulation.

mechanical components. The FV measure is related to the nominal contribution of the SSC failure to the top-level risk metrics. The higher the contribution, i.e., FV measure, the more important the SSC would be. The RAW importance measure, however, relates to the change in risk if the SSC is unavailable. It generally applies to standby components where the unavailability contributions are from two sources: fault exposure time (FET)[45] and maintenance downtime (MDT). The use of RAW values for operating and self-monitoring components or for components when the failure is self-revealing should be avoided (i.e., FET is very small due to the rapid detection of failure, and MDT is less than 72 hours but occurring with a very low occurrence rate). The limits on the risk contribution of component unavailability can then be estimated using the following equations.

$$\Delta CDF > F_{DT} \times (RAW - 1) \times (FET + MDT) \times CDF \qquad (1)$$
$$\Delta CDF < F_{DT} \times (RAW) \times (FET + MDT) \times CDF$$

Where ΔCDF is the expected change in CDF and F_{DT} is the annual frequency of component downtimes. Some example cases are shown below.

In the above equation, unavailability (Q) is defined by:

$$Q = F_{DT} \times (FET + MDT) \qquad (2)$$

All PRA minimal cutsets can be divided into two groups; those that contain the unavailability of component X, and those that do not. Let us call the contribution of the first group to core damage frequency (CDF) as CDFX and the other group as CDFX^. The overall CDF is therefore expressed as:

$$CDF = CDFX + CDFX^{\wedge} \qquad (3)$$

The change in CDF due to changing the unavailability of X from its baseline Q to a new value Q* only affects CDFX and it can be expressed by (note CDFX^ is not a function of Q and Q* and it will be subtracted out:

$$\Delta CDF = \left(\frac{CDFX * Q^*}{Q}\right) - CDFX \qquad (4)$$

Formulating the RAW value in terms of CDF, Q, Q*, and CDFX^, would yield Equation 5.

$$RAW = \frac{\left[\left(\frac{CDFX}{Q}\right) + CDFX^{\wedge}\right]}{CDF} \qquad (5)$$

Since CDFX^ is always less than CDF and greater than zero, we can establish some bounds from Equation 5 as shown in Equation 6.

[45] Fault exposure time is the duration that the component is in a failed state before the failure is detected. In short, it is a failure detection time. For most operating components and for all failures that are self-revealing, the fault exposure time is set to zero.

$$(RAW - 1) * CDF < \frac{CDFX}{Q} < RAW * CDF \qquad (6)$$

Inserting the bounds into Equation 4 from Equation 6 yields the following relationship [Equation 7].

$$(RAW - 1) * (Q^{*} - Q) * CDF < \Delta CDF < RAW * \ (Q^{*} - Q) * CDF \qquad (7)$$

Assuming the base line Q value is zero, one can estimate the risk contribution of component unavailability Q*.

If we assume criteria for tolerable ΔCDF and a base value of CDF; we can generate the range of RAW values that can achieve our ΔCDF criteria. This is shown In Table C-2.

Differentiations are made for various DI&C components, depending on the detection capabilities of online diagnosis and periodic testing. Depending on the design of diagnosis and other defensive measures, large fractions of failures can be monitored and be detectable almost immediately. These failures are named here as Type A failures. Type B failures, on the other hand, are not detectable by online monitoring and require more comprehensive periodic testing.

Table C-2 Examples of RAW Thresholds

Possible Cases	**F_{DT}**	**ΔCDF**	**FET**	**MDT**	**CDF**	**RAW Limit**
Typical standby component	0.1[1]	5.0E-07[2]	~0.05[3]	~8E-3[4]	1.0E-4	>1 <1.86[5]
CCF of two standby components	0.01	5.0E-07	~0.05	~8E-3	1.0E-4	>9.62 <8.62
Typical operating component	0.5	5.0E-07	0	~8E-3	1.0E-4	>2.25 <1.25
CCF of operating components	0.05	5.0E-07	0	~8E-3	1.0E-4	>13.5 <12.5
Typical DI&C channel (Type A failure modes[6])	8.0E-03	5.0E-07	0.0	~8E-3	1.0E-4	>78.1 <77.1
Typical DI&C channel (Type B failure modes[7])	1.5E-3	5.0E-07	~0.05	~8E-3	1.0E-4	>63.2 <62.20
CCF of DI&C Type A	8.0E-04	5.0E-07	0.0	~8E-3	1.0E-4	>781 <780
CCF of DI&C Type B	1.5E-3	5.0E-07	~0.05	~8E-3	1.0E-4	>632 <631

[1] Expected one failure every 10 years (failure rate of ~1.0E-5 per hour).

[2] The value 5.0E-7 corresponds to FV 0.005.

[3] Monthly periodic testing, i.e. 15 days of exposure time ~0.05 expressed in unit of a year.

[4] About 72 hours of repair time expressed in unit of a year.

[5] Limit 2 is generally used for RAW for SSC classification.

[6] Failure modes that are (monitored) and are detectable by diagnosis defenses and checks.

[7] Failure modes that are not detectable by monitoring but are detectable by periodic testing.

Finally, there are Type C failures that could not be detected either by monitoring or by periodic testing. Type C failures occur under specific conditions (context) and are discovered during actual demand. These failures are modeled under failure-per-demand and are not a contributor to unavailability, therefore, the RAW measure does not apply to Type C failures (the FV measure is more appropriate). For developing Table C-2, the fractions of Type A, B, and C failures considered are 80%, 15%, and 5%. Type A failures include all failures discovered by input checking error, watchdog time, output error checking (voting logics), transient memory faults, failures detectable by heartbeat monitoring, and self-revealing failures (e.g., power supply failure). Type B failures may include other failure modes that are not monitored or self-revealing unless a periodic check is performed (e.g., failure of a protective Zener diode for high-voltage protection, which does not impact normal operation of DI&C).

As shown in Table C-2, the use of RAW threshold could vary depending on the SSC to which it is applied. We will revisit the use of RAW values for DI&C for the current generation and advanced reactors. It currently appears that the RAW threshold for DI&C system failure (CCF failure of software or hardware) is about 1000 (conservatively shown in Table C-2 between 600 and 700) for the current generation of LWRs.

C.2.3.1 Lessons from Application of RG 1.201

RG 1.201 is a quantitative risk application; however, it utilizes risk importance measures in lieu of the risk metrics in RG 1.174. This is mainly due to the difficulty and uncertainties associated with characterizing the impact of requested changes in terms of quantities that could be used within the PRA model and data structure. It is possible to conservatively characterize the changes such that an upper bound of the risk impact could be estimated to show compliance with RG 1.174 criteria. However, this may require changes in PRA models and data to account for possible effects such as component aging and reduction in safety margins. RG 1.201 relies on the explicit calculation of importance measures from PRAs rather than other quantitative risk insights that could be obtained from the manipulation of PRA models. The use of automated importance measures for equipment that are modeled explicitly limits the number of equipment that could be evaluated. As a result, RG 1.201 heavily relies on qualitative engineering analysis performed by IDP and some risk-sensitivity studies.

The following lessons are gleaned from the review of RG 1.201 and several of its sample applications.

1. Explicit modeling of safety and non-safety systems in PRA for RG 1.201

   Modeling all plant systems needed for RG 1.201 will result in a large and unmanageable PRA model. Not explicitly modeling all systems, safety and non-safety, significantly limits the number of equipment classified by the PRA. This is because RG 1.201 relies on the explicit calculation of importance measures from PRAs rather than other quantitative risk insights that could be obtained from the manipulation of PRA models. The use of automated importance measures for equipment that are modeled explicitly limits the number of equipment that could be evaluated. As a result, RG 1.201 ends up being heavily dependent on qualitative engineering analysis performed by IDP and some risk-sensitivity studies. To manage the size of PRA when all systems are modeled for RG 1.201, a careful graded approach is proposed.

2. Enhanced importance measures with modified thresholds

   The importance measures and the associated criteria used in RG 1.201 were used previously for other applications (e.g., maintenance rule) dealing with conventional electrical and mechanical components. There is little or no experience of the use of importance measures for highly redundant equipment, such as AI&C/DI&C systems with significant CCF contribution, and passive components, such as pipes and tanks. Alternate importance measures and modified thresholds may be necessary for extending the use of the approach described in RG 1.201. Examples of a modified threshold for RAW and the potential use of RAW importance measures were discussed earlier.

3. IDP qualitative ranking and the role of PRA

   IDP decisions and the qualitative criteria in SSC categorization play an important role in SSC classification. IDP generally identified a large fraction of HSS components[46] for some applications. The exact reason is not yet examined, but it appears some PRAs may not have enough scope and level of detail to automatically generate the importance measures and classify the components. As a result, many components cannot be classified by automatic generation of importance measures. As an example, the loss of main feedwater is a basic event (no fault tree is developed) representing an initiator in most current PRAs. It would be impossible to identify the importance of various contributors to the loss of the main feedwater initiator in such a PRA. IDP is then responsible for the breakdown of a super component into sub-components (including the associated I&C) for the purpose of SSC classification. This same issue will also be discussed as part of the PRA level of detail suitable for RG 1.201 application.

   Another important area for IDP review is the classification of passive components. The failure of passive components not only degrades the system, but if not isolated, can be a source of flooding. The possible use of flooding PRA, the use of risk insights from risk-informed inservice testing/inservice inspection (IST/ISI), and focused PRA sensitivity analyses could be beneficial for this purpose. In addition, I&C systems can provide early warning, such as alarms and indicators that help the operators detect external events (e.g., fire, flood). Taking advantage of external event PRAs for passive components and modeling of I&C systems for indicator and alarms (as will be discussed in the next subsection) is advisable.

4. PRA scope for RG 1.201

   The scope of a PRA to fully support RG 1.201 should include all systems, safety and non-safety, should address both internal and external events, and explicitly account for dependence of HRAs on the failed components (not just HRA dependencies on each other). The graded approach to developing PRA models should be implemented to ensure all risk potential risk-significant contributors are modeled in enough level of detail.

5. PRA level of detail

   The PRAs that lack the necessary level of detail would increase the burden on IDP to classify the components that are not modeled. The level at which the PB events are

[46] NEI presentation from an industry and NEI/NRC meeting on, “NEI Lessons-Learned Workshop,” Washington DC, Jan 30-31, 2019.

currently established is based on the available generic data. The available PRA generic data were developed over several decades without systematically accounting for what PRA will be used for and what generic data would be needed. The current generic data is developed to support an overall risk estimation rather than insights for risk applications. For estimating an overall risk estimation, a basic event could be a super component (e.g., main feed water). Balancing the PRA level of detail with the needs of SSC classification in a practical manner is a challenging task for all systems including I&C systems.

C.2.3.2 AI&C/DI&C PRA Challenges for Support RG 1.201

The following PRA challenges were identified for current and future use of RG 1.201 for AI&C/DI&C systems.

Scope of I&C Systems to be Modeled in PRA

Scope and coverage of SSCs: A PRA to support RG 1.201 should include many front-line, support and backup systems. A PRA of such a large scope should be managed properly by appropriate screening criteria and detailed documentation. For example, for I&C systems, the PRA should include a large number of I&C modules (not only RTS and ESFAS). The PRA modeling detail should be commensurate with the importance of the modules and inclusion into the PRA based on well-defined screening criteria.

Scope and coverage of hazards: I&C systems can provide early warning such as alarms and indicators that help the operators detect external events (e.g., fire, flood). This is in addition to standard modeling of I&C systems to support major plant safety functions. External events, such as fire, can be considered a CCF mechanism for I&C systems and should be addressed. This will be discussed next. The availability of an external-event PRA and the inclusion of I&C systems in external event PRAs is advisable for performing risk-informed applications.

Impact of I&C System Failures on Human Reliability Analysis (HRA)

The DI&C systems for new reactors and next generation reactors, and AI&C systems for the current generation of operating reactors, appear to perform additional functions, such as providing information for operator diagnostic aids. The dependency of operator error probabilities on missing or erroneous indication due to failures in I&C systems must be explicitly modeled, at least for risk important I&C degraded states during internal and external events. The changes of operator error rate as result of missing information or erroneous information should be estimated and modeled in PRAs.

PRA Level of Detail

The level of detail in PRA to support an application should be consistent with the level at which the risk-informed changes are applied. RG 1.201 generally applies to a module level for the AI&C/DI&C system. The PRAs that lack the necessary level of detail would increase the burden on IDP to classify the modules that are not modeled explicitly in the PRA and are embedded within a super basic event. The generic data for I&C systems should be developed at a level that can support not only the overall risk estimation but also be capable of providing quantitative risk insights for individual SSC classification.

Functional versus Physical System

This is a generic issue regarding PRA modeling, which was discussed in Section 4.2.2 in the main body of the report under the subject, “physical versus functional” modeling.

PRA Data Needs

Since operational data in the nuclear industry for DI&C is quite limited, generic data is needed for hardware and software from other non-nuclear industries. This is a generic issue that is discussed throughout the report.

CCF of Software and Hardware

CCF of I&C software and hardware events can render AI&C/DI&C systems inoperable. It is important to note that breaking down CCF to each function performed by the system can reduce the risk significance of each CCF and the associated importance measure (for example RAW). Furthermore, modeling the contributors to CCF probabilities for both software and hardware, accounting for partial diversity, can result in smaller and more realistic importance measures. The modeling and estimation of CCF is a generic PRA issue, which is discussed throughout the report.

Improved Importance Measures and Thresholds

The current importance measures and their thresholds must be revisited in light of much higher reliability of DI&C systems and their increased redundancy and diversity. This was discussed for the application of RAW values to RG 1.201. The improvement of the importance measures and the associated thresholds shall be addressed with pilot applications through comparative studies.

Sensitivity and Uncertainty Analyses

Robustness of the risk-informed decisions depends on identifying the major sources of variations and uncertainties. Not all uncertainties have the same importance and impact of the PRA results. Uncertainties can be addressed by parametric uncertainty propagations, sensitivity analysis and establishing practical bounds. The identification and the evaluation of the impact of these uncertainty sources should be piloted on a DI&C PRA model. This, of course, requires developing a PRA test bed for DI&C.

C.2.4 Summary for RG 1.205

RG 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants” [Ref. 20], provides guidance for risk-informed, performance-based fire protection programs that meets the requirements of Title 10, Section 50.48(c), of the *Code of Federal Regulations* (10 CFR 50.48(c)).

For licensees choosing to adopt NFPA 805, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” under 10 CFR 50.48(c), a set of risk criteria is defined as the basis for making changes to the approved NFPA 805 FPP without prior NRC approval. The criteria (deterministic and risk-informed) duplicated from RG 1.205 are shown below:

a. Prior NRC review and approval is not required for a change that results in a net decrease in risk for both CDF and LERF. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. The change may be implemented following completion of the change evaluation.
b. Prior NRC review and approval is not required if the change results in a net calculated risk increase less than <1E-7/yr for CDF and less than <1E-8/yr for LERF. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. The change may be implemented following completion of the change evaluation. Change reports need not be submitted to the NRC for these changes.
c. Where the calculated plant change risk increase is <1E-6/yr, but >1E-7/yr for CDF or <1E-7/yr, but >1E-8/yr for LERF, the licensee must submit a summary description of the change to the NRC following completion of the change evaluation. The proposed change must also be consistent with the defense-in-depth philosophy and must maintain sufficient safety margins. If the NRC does not object to the change within 90 days, the licensee may proceed with implementation of the proposed change.

The Nuclear Energy Institute (NEI) has developed NEI 04-02, “Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)” [Ref. 13], to assist licensees in adopting 10 CFR 50.48(c) and making the transition from their current fire protection program (FPP) to one based on NFPA 805 [Ref. 14].

The steps for performing a fire PRA to satisfy NFPA 805 criteria are provided in NUREG/CR-6850, “EPRI/NC-RES Fire PRA Methodology for Nuclear Power Facilities” [Ref. 15]. In the appendices to NUREG/CR-6850, there is an extensive evaluation of the experimental database existing at that time underlying the various steps of the PRA procedure. Since that time, additional fire research has been performed by the NRC and the Electric Power Research Institute (EPRI) to enhance the methodology and data in NUREG/CR-6850. Major areas of enhancement were in cable fire heat release rates, target damage criteria, and circuit failure analysis. An extensive study was performed under the sponsorship of NRC and EPRI of the status of “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications” [Ref. 16], in which a set of fire scenarios are established and comparisons made among the NRC’s Fire Dynamics Tool (FDT), EPRI’s FIVE model, NIST’s CFAST zonal model, EdFs MAGIC code and NIST’s Fire Dynamics Simulator (FDS). The information generated from multi-volume NUREG-1824, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications” [Ref. 17] was summarized in NUREG-1934, “Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG)” [Ref. 18]. This document also includes eight example fire scenarios and evaluated them using the five different codes (FDT, FIVE, CFAST, Magic and FDS) addressed by NUREG-1824. Additional enhancement in estimates of fire ignition frequencies to reduce fire PRA conservatism is currently being studied by the industry.

RG 1.205 provides a risk-informed justification for licensee amendment of proposed changes to the fire protection program. The specific area of the fire protection requirements that could benefit from risk-informed approaches are Section IIIG, on safe shutdown capability, IIIF, on automatic detection, and IIID, on manual suppression. Fire events affect instrumentation in many ways and some indications may not be accurate during a fire event. As discussed in NUREG/CR-6850, there are generally a limited set of instrumentation and diagnostic equipment such as indicators, lights, alarms, and similar devices considered necessary to support successful operator actions (e.g., such as carrying out the Emergency Operating Procedures (EOPs), following specific Fire Emergency Procedures (FEPs), or to credit certain recovery actions). NUREG/CR-6850 also considers the failures of those I&C, which could cause inappropriate operator actions. The limited I&C systems then should be included in a component list for cable tracing. Examples could be remote shutdown panel (or areas) equipment and controls, pump room high-temperature alarms, certain plant parameter indicators with no or little redundancy, among others.

The fire-induced damage to instrumentation and alarms would be specific to each fire area. The available instrumentation and equipment must be adequate to support correct operator actions. Spurious alarms requiring direct operator response should also be considered separately to ensure that no inadvertent operator actions could occur due to spurious alarms. NUREG-1921, “EPRI/NRC-RES Fire Human Reliability Analysis Guidelines” [Ref. 19], provides guidance on human reliability analysis during fire, which indirectly addresses some of the issues related to modeling I&C equipment during a fire event. All these considerations are included in human failure probability calculations, but not explicitly a part of PRA development and quantification of scenarios.

C.2.4.1 Lessons Learned from RG 1.205/NFPA 805

NRC and the industry have spent significant resources in supporting fire PRAs. As a result, guidance documents for the various PRA elements to support RG 1.205 [Ref. 20] and NFPA 805 are the most comprehensive. In addition, some level of conservatism has been permeated throughout the fire PRA guide to ensure its regulatory applicability. NFPA 805 fire PRAs are also resource intensive, indebted to not using the risk screening. A good example is the circuit analysis tasks that look for all spurious actuations rather than those that are shown to be risk significant. This could require a lot of resources and it may not be an efficient approach. There are also some issues that need to be explored in detail, such as high initial heat release rate from ignition source for the assumed ignition frequency. Sophisticated uncertainty analysis is performed as a part of the NFPA 805 PRA. However, uncertainty analysis estimates contaminated with bias may not be as informative unless the degree of bias (conservatism) is explicitly shown on all resulting estimates (as it is for some of the estimates generated from fire codes such as FDS).

Enhanced methods and data are being developed to address many of these challenges and issues, specifically in reducing the conservatisms, by both NRC and industry. The next section will focus on those challenges that the implementation of RG 1.205 would create for PRA modeling and data specific to AI&C/DI&C.

C.2.4.2 AI&C/DI&C PRA Challenges to Support RG 1.205/NFPA 805

Like the internal events PRA, the NFPA 805 fire PRA models also have not modeled I&C systems in detail. NFPA 805 requires that the available instrumentation, indicators, and alarms that operators rely on to maintain critical safety functions during each major fire scenario, be documented. It is generally assumed that the contribution of I&C failures to CDF and LERF during a fire scenario is small when considering the availabilities of one train of I&C, unaffected by fire, for auto actuation with a diverse manual actuation. Spurious alarms requiring direct operator response are also considered qualitatively in fire PRA and indirectly for human reliability estimation. Current practices generally assume that the failure of I&C is not a significant contributor to fire-induced CDF/LERF for dominant accident sequences. This is because the conditional core damage probabilities in fire scenarios are generally around 1.0E-2, compared to the 1.0E-3 failure probability of I&C systems consisting of one train plus diverse manual initiation.

Additional PRA challenges for modeling I&C systems are as follows:

1. Effect of the I&C system on non-dominant accident scenarios: There is a concern that non-dominant fire accident scenarios could become dominant if a fire affects the I&C systems such that higher human error rates and response to spurious actuations could significantly increase the risk contribution. PRA-based screening criteria should be devised to identify those scenarios where detail modeling may be needed to account-for the risk increase from the non-dominant fire sequences caused by fire-induced degraded I&C systems.
2. Spurious actuation and partial CCF: AI&C/DI&C are highly redundant and segregated systems. The potential of CCF of all modules of I&C systems due to a harsh fire environment, including smoke, is not very likely. However, the occurrence of fire when a portion of the system is unavailable due to test and maintenance as governed by TS can significantly increase the probability of various I&C failure modes, including spurious actuation.
3. Human Error Probability: Fire scenarios could result in failure of sensors, instrumentation channels, and communication links. These effects could reduce the information available for major operator actions, which depend on the accident scenario. Missing, confusing information, spurious alarms, and wrong indicators could significantly increase the human cognition of the accident condition. More formal treatment of human failure probabilities could become necessary in some cases.

All other PRA issues related to scope and level of detail described for RG 1.201 are also applicable to this RG. Fire PRA modeling of DI&C may introduce additional challenges due to the response of DI&C to possible fire scenarios.

C.2.5 Summary of RG 1.200

RG 1.200 [Ref. 21] describes a peer review process utilizing the ASME/ANS PRA standard, “Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” (currently the ASME/ANS RA-Sa-2009 PRA standard) to determine whether the technical adequacy of the PRA, in total or the parts that are used to support an application, is sufficient to provide confidence in the results. The primary result of a peer review are the findings and observations (F&Os) recorded by the peer review and the subsequent resolution of these F&Os. Peer reviews are also needed each time a major PRA upgrade has been performed, which could include (1) use of new methodology, (2) change in scope that impacts the significant accident sequences or the significant accident progression sequences, and (3) change in capability that impacts the significant accident sequences or the significant accident progression sequences. The NRC staff will review the PRA and the status of F&O closures as a part of the review of the application-specific, risk-informed submittal. Several of these reviews and the associated request for additional information (RAI) were examined to better understand the relation of RG 1.200 with the ASME/ANS PRA standard and the peer review process.

The summary of technical attributes for Level 1 PRA for internal events is listed in Table 2 of RG 1.200. There is no specific mention of the I&C system in Table 2, although it could be argued that it is implicitly accounted for by other attributes and general principles covered in this guide. The first place that instrumentation is explicitly mentioned is as a part of equipment selection for performing fire PRA.

Tables A-1 through A-10 in Appendix A of RG 1.200 provide the staff's position on each requirement in Parts 1 through 10 of the ASME/ANS RA-Sa-2009 PRA standard, respectively. The ASME/ANS PRA standard has some discussion on the PRA modeling of spurious actuation and/or spurious alarms during fire PRA and their effect on operator actions of commission, which are not generally modeled in PRAs. For example, if a high-temperature alarm is spuriously induced by fire for a running pump, the operator is expected to shut down the pump. PRA fire models should not credit the pump and any recovery of pump should account for verification that the alarm is false (remote or local actions). Response time and the human error probability should be addressed as a part of estimating the recovery probability. It is assumed that RG 1.200 supports those limited instructions in the ASME/ANS PRA standard.

PRA modeling for the DI&C system is discussed in detail as a part of Standard Review Plan (SRP) Chapter 19 [Ref. 22]. This document lists several areas that the NRC staff considers important for the review of DI&C systems. The SRP does not indicate how and at what level of detail these reviews should be performed.

C.2.5.1 Lessons Learned from RG 1.200

RG 1.200 establishes the scope and attributes of PRAs needed to address the risk-informed applications. It focuses on CDF and LERF consistent with the current risk-informed regulatory framework. RG 1.200 is supported by the ASME/ANS PRA standard, which provides specific high-level requirements (HLR) and supporting requirements (SRs) for various elements of PRAs. Its scope includes internal and external events, although most emphasis so far has been on internal events. Both RG 1.200 and ASME/ANS standards are supported by a series of technical documents that provide detailed instructions (low-level documents) of how the PRA for each application should be performed.

A combination of RG 1.200, the ASME/ANS standard, and a peer review process [Ref. 23] is an effective and efficient approach for identifying weaknesses in PRAs. Additionally, the F&Os generated through peer reviews identify specific aspects of the PRA that may need revision, provide the primary basis for PRA conformance with the state-of-the-practice, and identify areas for focus review and PRA updates. As noted in RG 1.200, the guide and process of review is based on the PRA state-of-the-practice. It cannot be used for new methods, i.e., PRA practices, which are state-of-the-art and beyond. These guides should be updated as PRA methods are enhanced, and the state-of-the-practice is improved. For example, there is a limited discussion within RG 1.200 about the PRA modeling of I&C systems. RG 1.200 mainly relies on the ASME/ANS PRA standard for this PRA area. The consideration of I&C systems in the ASME/ANS PRA standard is generally discussed as a support to HRA estimates, recovery actions or the availability of support systems in an implicit manner. Explicit requirements for PRA modeling of I&C systems as a standalone subject is not currently included in the ASME/ANS PRA standard.

The authors examined what would be needed to update the ASME/ANS PRA standard to make it more responsive to the needs of PRA modeling of I&C systems. Parts 1 through 10 are written in the form of HLRs and SRs, along with examples for specific consideration. One example set of the requirements (HLR, SR, and Example) is shown in Table C-3 below.

Table C-3 Illustration of HLR, SR, and Example from ANS/ASME PRA Standard

HLR-AS-B	Dependencies that can impact the ability of the mitigating systems to operate and function shall be addressed.
SR: AS-B; AS-B2:	IDENTIFY the dependence of modeled mitigating systems on the success or failure of preceding systems, functions, and human actions. INCLUDE the impact on accident progression, either in the accident sequence models or in the system models.
Example	*(a)* turbine-driven system dependency on stuck-open relief valve (SORV), depressurization, and containment heat removal (suppression pool cooling) *(b)* low-pressure system injection success dependent on need for RPV depressurization.

The authors have concluded, based on a preliminary examination and review of the ANS/ASME PRA standard, that:

1. HLRs appear to be applicable to all systems and perhaps to all plant designs.

2. Some changes are envisioned for supporting requirements to address the DI&C PRA more specifically. The SR for some PRA elements, especially Element 3 of the success criteria and Element 4 of system analysis, may be needed. For example, SR-SY-A9 requires that super components be decomposed down to a level of detail when the specific failure mode and recovery action can be determined. Decomposing software to specific functions can be explicitly covered under this requirement. Please note that this was discussed as a PRA requirement for decomposing software earlier in Section C.2.2.2.

3. New example to highlight major considerations for DI&C PRA should be added to the ANS/ASME PRA standard.

Performing additional DI&C PRAs and PRA applications including pilot studies can help with updating both RG 1.200 and the ASME/ANS PRA standard.

C.2.5.2 AI&C/DI&C PRA Challenges to Support RG 1.200 Updates

As noted in the previous section, RG 1.200 and associated documents have no explicit requirements for modeling I&C systems in PRAs. Requirements for PRA modeling for DI&C systems, however, can be found in SRP Chapter 19 for new reactors. This document lists areas the NRC may review as a part of the design certification document (DCD) or final safety analysis report (FSAR). Neither the SRP nor RG 1.200 indicates how and at what level of detail these reviews should be performed.

The SRP requirements for reviewing DI&C are generally based on the lessons learned from previously accepted new reactor DI&C system PRA reviews. Meeting these requirements is judged to be challenging for DI&C and are highlighted as follows:

1. The modeling of DI&C systems should include the identification of how DI&C systems can fail and what these failures can affect. The failure modes of DI&C systems are often identified by the performance of failure modes and effects analyses (FMEA). It is difficult to define DI&C system failure modes especially for software because they occur in various ways depending on specific applications. Also, failure modes, causes, or effects often are intertwined or defined ambiguously, and sometimes overlap or are contradictory. Examine applicant documentation to ensure that the most significant failure modes of the DI&C are documented with a description of the sequence of events (context) that need to take place to fail the system. The sequence of events should realistically represent the system's behavior at the level of detail of the model.

2. The DI&C reviewer should confirm that DI&C system equipment can meet its safety function in environments associated with accident sequences modeled in the PRA. This is done in collaboration with the reviewer for the PRA and severe accident evaluation that provides input on the expected environments that need to be considered.

3. The PRA reviewer should confirm that the impact of external events (i.e., seismic, fire, high winds, flood, and others) on DI&C has been addressed in the PRA.

4. Coordinate the review of human reliability assessment (HRA) with staff evaluating areas such as main control room design, and minimum alarms and controls inventory. If recovery actions are modeled, they should consider loss of instrumentation and the time available to complete such action.

5. The applicant should describe adequately where and how the design reliability assurance program (D-RAP) captures the DI&C system key assumptions, such as how future software and hardware modifications will be conducted to ensure that high reliability and availability are maintained over the life of the plant. Verify that key assumptions from the DI&C PRA are captured under the applicant's D-RAP, which is described in SRP Chapter 17, Section 17.4.

6. Common cause failures can occur in areas where there is sharing of design, application, or functional attributes, or sharing of environmental challenges. Each of the areas found to share such attributes should be evaluated in the DI&C analysis to determine where CCF should be modeled and to estimate their contribution. The CCF probabilities and their bases should be evaluated and provided based on an evaluation of coupling mechanisms (e.g., similarity, design defects, external events, and environmental effects) combined with an evaluation of defensive measures meant to protect against CCF (e.g., separation and independence, operational testing, maintenance, diagnostics, self-testing, fault tolerance, and software/hardware design/development techniques and processes). Dependencies between hardware and software should be identified.

7. Design features, such as fault tolerance, diagnostics, and self-testing are intended to increase the safety of DI&C systems, and therefore are expected to have a positive effect on the system's safety. However, these features may also have a negative impact on the safety of DI&C systems if they fail to operate appropriately. The potentially negative effects of these features should be included in the probabilistic model. For example, a design feature; fault tolerance in a DI&C system is designed such that it can only detect and hence mitigate certain types of failures. A feature may not detect all the failure modes of the associated component, but just the ones it was designed to detect. The PRA model should only give credit to the ability of these features to automatically mitigate these specific failure modes; it should consider that all remaining failure modes cannot be automatically tolerated. A fault-tolerant feature of a DI&C system can be explicitly included either in the logic model or in the PRA data, but not both.

8. If a DI&C system shares a communication network with other DI&C systems, the effects on all systems due to failures of the network should be modeled jointly. The impact of communication faults on the related components or systems should be evaluated, and any failure considered relevant should be included in the probabilistic model.

It is clear from the discussion in SRP Chapter 19 that there are many challenges in performing and reviewing the PRA for DI&C system for new reactors. The reviews are currently being performed as best as possible without detailed guidance and a working PRA for pilot applications and testing. Additional challenges could be identified when a specific risk-informed application is considered (e.g., SSC classification for DI&C).

C.3 REFRENCES

1. 60 FR 42622, “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement.”
2. NUREG/CR-6813, “Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making,” April 2003.
3. RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.”
4. NUREG-1855, “Guidance on the Treatment of Uncertainties associated with PRAs in Risk-Informed Decision Making,” March 2009.
5. RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.”
6. “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, Addendum A,” ASME/ANS RA-Sa-2009, American Society of Mechanical Engineers, March 2009.
7. NEI 17-07 [Rev A], “Performance of PRA Peer Reviews Using the ASME/ANS PRA Standard,” December 2017.
8. RG 1.177, “An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications.”
9. NEI 06-09, “Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines,” Industry Guidance Document, November 2006.
10. NUREG/CR-5500, Vol. 2, “Reliability Study: Westinghouse Reactor. Protection System, 1984–1995.” INEEL/EXT-97-00740. S. A. Eide. S. T. Beck. M. B. Calley.
11. RG 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance.”
12. NEI 00-04 (Rev 0), “10 CFR 50.69 SSC Categorization Guideline,” July 2005.
13. NEI 04-02, “Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c),” Revision 1, September 2005.
14. NFPA, “Performance Based Standard for Light Water Reactor Electric Generating Plants,” NFPA-805, 2001.
15. “EPRI/NC-RES Fire PRA Methodology for Nuclear Power Facilities,” NUREG/CR-6850 2005.
16. NRC/EPRI, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” NUREG-1824, EPRI-1011999, 2007.
17. NUREG-1824, EPRI 1011999. Final Report. “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” Volume 1: Main Report.
18. “Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG),” NUREG-1934, EPRI 1023259, November 2012.
19. “EPRI/NRC-RES Fire Human Reliability Analysis Guidelines,” NUREG-1921/EPRI 1023001, July 2012.
20. RG 1.205, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants.”
21. ASME/ANS PRA Standard, “Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” currently ASME/ANS-RA-Sa-2009.
22. Standard Review Plan (SRP), Chapter 19.0, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” NUREG-0800, December 2015.
23. NEI 17-07, “Performance of PRA Peer Reviews Using the ASME/ANS PRA Standard,” December 2017.