INL/RPT-23-74703

Investigation and Demonstration of Reliability Target Allocation to Support Reliability and Integrity Management Program

September 2023

Final Report

Diego Mandelli[1], Todd Anselmi[1], Courtney Otani[1], Emerald Ryan[1], Kevin O'Rear[1], Svetlana Lawrence[1], Ralph Hill[2]

[1]Idaho National Laboratory, [2]Hill Eng Solutions, LLC

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/RPT-23-74703

Investigation and Demonstration of Reliability Target Allocation to Support Reliability and Integrity Management Program

Final Report

Diego Mandelli[1], Todd Anselmi[1], Courtney Otani[1], Emerald Ryan[1], Kevin O'Rear[1],
Svetlana Lawrence[1], Ralph Hill[2]
[1]Idaho National Laboratory, [2]Hill Eng Solutions, LLC

September 2023

Idaho National Laboratory
Advanced Reactor Technologies
Idaho Falls, Idaho 83415

http://www.art.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

ABSTRACT

Nuclear energy is the most reliable and environmentally sustainable energy source available today. In the United States (U.S.), nuclear-generated power accounts for approximately 20% of total electricity and over 55% of clean energy. New advanced reactors have enormous potential to help further decarbonize the energy market, enhance grid resiliency, create new jobs, and build a stronger economy. More than 50 new reactors are being developed in the U.S., and the federal government realizes an urgent need to deploy nuclear technologies to meet the country's energy, environmental, and national security goals. As such, the U.S. Department of Energy (DOE) launched multiple programs to support advanced reactor deployment. The research described in this report explores implementation strategies for the Reliability and Integrity Management Program that directly supports the DOE goal to enable the near-term deployment of the advanced reactor technologies. The project is conducted under the Regulatory Development Program for advanced reactors sponsored by the DOE.

Page intentionally left blank

INL ART Program

Investigation and Demonstration of Reliability Target Allocation to Support Reliability and Integrity Management Program

INL/RPT-23-74703

September 2023

Technical Reviewer: (Confirmation of mathematical accuracy, and correctness of data and appropriateness of assumptions.)

James Kinsey 9/14/23

James Kinsey
Regulatory Development Technical Area Lead

Date

Approved by:

9/14/2023

Michael E. Davenport
ART Project Manager

Date

MT Sharp 9/14/2023

Michelle T. Sharp
INL Quality Assurance

Date

ACKNOWLEDGEMENTS

The authors would like to acknowledge support of this project provided by Kyle Metzroth from X-Energy and by EPRI researchers Chris Wax, Mark Albert, Eric Thornsbury, and Greg Shelby.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

AC	Alternating current
ACC	Accumulator
AOO	Anticipated Operational Occurrence
AR	Advanced reactors
ASME	American Society of Mechanical Engineers
BDBE	Beyond Design Basis Event
BE	Basic Event
BEI	Basic Event Information
CAFTA	Computer Assisted Fault Tree Analysis
CLR	Component-Level Requirement
ConOps	Concepts of Operation
DBA	Design Basis Accident
DBE	Design Basis Event
DC	Direct current
DID	Defense-in-depth
DMA	Damage mechanism assessment
DOE	Department of Energy
ETL	Event Tree Logic
F-C	Frequency-Consequence
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FT	Fault Tree
FTL	Fault Tree Logic
FY	Fiscal year
HE	Human Error
IE	Initiating Event
INL	Idaho National Laboratory
ISI	In-service
LBE	Licensing Basis Event
LLOCA	Large loss of coolant accident
LMP	License Modernization Project
LOCA	Loss of coolant accident

LPI	Low-pressure injection
LPR	Low-pressure recirculation
LWR	Light Water Reactor
MANDE	Monitoring and Non-destructive Examination
MANDEEP	Monitoring and Non-Destructive Examination Expert Panel
MCS	Minimal cut sets
MBSE	Model-Based Systems Engineering
NDE	Non-destructive examination
NEI	Nuclear Energy Institute
NPP	Nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	Operations and maintenance
OE	Operating Experience
PM	Preventive Maintenance
PRA	Probabilistic Risk Assessment
PRE	Plant Risk Evaluation
PSD	Plant Systems Design
PWR	Pressurized-Water Reactor
RAM	Reliability, Availability, and Maintainability
RAMI	Reliability, Availability, Maintainability, and Inspectability
RBD	Reliability Block Diagram
RCCS	Reactor cavity cooling system
RG	Regulatory Guide
RIM	Reliability and Integrity Management
RIMEP	Reliability and Integrity Management Expert Panel
SAPHIRE	Systems Analysis Program for Hands-on Integrated Reliability Evaluation
SEDI	Systems Engineering Design Integration
SSC	Structures, systems, and components
U.S.	United States
V&V	Verification and Validation

TERMS AND DEFINITIONS

This section defines terms used in this report. Definitions are consistent with terms and definitions presented in 2019 edition of ASME Boiler and Pressure Vessel Code Section XI Division 2 code "Requirements for Reliability and Integrity Management (RIM) Programs for Nuclear Power Plants" [1] herein after referred to as ASME Section XI Div. 2 and with Nuclear Energy Institute (NEI) Technical Report 18-04, Revision 1 "Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development" [2] herein after refereed as NEI 18-04.

Accident Sequence

A representation in terms of an initiating event followed by a sequence of failures or successes of events (i.e., system, function, or operator performance) that can lead to undesired consequences with a specified end state.

Alternate Requirements

Monitoring or augmented non-destructive examination (NDE) methodologies used to assess and evaluate component degradation other than the prescribed NDE methods contained in [1] Mandatory Appendix V and any augmented provisions contained in the applicable reactor design supplement of Mandatory Appendix VII.

Anticipated Operational Occurrence (AOO)

Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant (NPP), which may include one or more reactor modules. Event sequences with mean frequencies of 1×10^{-2}/plant-year and greater are classified as AOOs. AOOs take into account the expected response of all structures, systems, and components (SSC) within the plant, regardless of safety classification.

Availability

The probability that a system or component is capable of supporting its function.

Beyond Design Basis Event (BDBE)

Rare event sequences that are not expected to occur in the life of a NPP, which may include one or more reactor modules, but are less likely than a Design Basis Event (DBE). Event sequences with frequencies of 5×10^{-7}/plant-year to 1×10^{-4}/plant -year are classified as BDBEs. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.

Capability Target

Definition of what a system (or a component) shall do and how well in order to achieve plant-level and system-level performance goals. Capability is described and prescribed via functional and performance requirements for a system or a component.

Component Exposure Population

The set of equipment included in the scope of the Reliability and Integrity Management (RIM) Program for which a particular RIM strategy is applied to influence reliability.

Component-Level Requirement (CLR)

CLRs are the allowable degradation limits of an individual component from a safety point of view. CLRs are described in accordance with the plant safety evaluation, using quantities such as the break size postulated in an accident scenario.

Condition Monitoring

The process of systematic data collection and evaluation to identify and quantify usage factors or changes in performance or condition of an SSC, such that remedial action may be planned to maintain SSC reliability targets.

Containment Failure Frequency (CFF)

CFF is the sum of frequencies of various containment failure modes ranging from small leaks to a large and early break of the containment.

Defense-in-Depth (DID)

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

Degradation Mechanism

A phenomenon or process that attacks (e.g., wears, erodes, corrodes, cracks) the material under consideration.

Design Basis Accident (DBA)

Postulated accidents that are used to set design criteria and performance objectives for the design of safety-related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of safety-related SSCs needed to mitigate and prevent accidents, respectively. DBAs are derived from the DBEs by prescriptively assuming that only safety-related SSCs classified are available to mitigate postulated accident consequences to within the 10 CFR 50.34 dose limits.

Design Basis Event (DBE)

Infrequent event sequences that are not expected to occur in the life of an NPP, which may include one or more reactor modules, but are less likely than AOOs. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification. The objective and scope of DBEs form the safety design basis of the plant.

Design Basis External Hazard Level (DBEHL)

A design specification of the level of severity or intensity of an external hazard for which the safety-related SSCs are designed to withstand with no adverse impact on their capability to perform their required safety function (RSF).

End State

The set of conditions at the end of an Event Sequence that characterizes the impact of the sequence on the plant or the environment. In most probabilistic risk assessments (PRA), end states typically include success states (i.e., those states with negligible impact) and release categories.

Event Sequence

A representation of a scenario in terms of an Initiating Event defined for a set of initial plant conditions (characterized by a specified plant operating state) followed by a sequence of system, safety function, and operator failures or successes, and sequence termination with a specified end state (e.g., prevention of release of radioactive material or release in one of the reactor-specific release categories). An event sequence may contain many unique variations of events (minimal cut sets) that are similar in terms of how they impact the performance of safety functions along the event sequence.

Failure

Events involving conditions that would disable a component's ability to perform its intended safety function.

Failure Mechanism

Any of the processes that results in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error.

Frequency-Consequence Target (F-C Target)

A target line on a frequency-consequence chart that is used to evaluate the risk significance of licensing basis events (LBEs) and to evaluate risk margins that contribute to evidence of adequate defense-in-depth.

Fundamental Safety Function (FSF)
Safety functions common to all reactor technologies and designs; includes control heat generation, control heat removal, and confinement of radioactive material.

Health
A quantitative or qualitative assessment of a system's (or component's) ability to satisfy required capability described via functional and performance requirements.

Human Error (HE)
Any human action that exceeds some limit of acceptability, including inaction where required and excluding malevolent behavior.

Indication of Degradation (ID)
A signal or response that degradation exists that could lead to the exceedance of a CLR.

Initiating Event
Any event that perturbs the steady state operation of the plant, if operating, or the steady state operation of the decay heat removal systems during shutdown operations such that a transient is initiated in the plant that leads to the need for reactor subcriticality and decay heat removal.

Level of Rigor
The level of confidence to which a given examination system must be demonstrated based upon factors such as user needs, degradation mechanisms, and required reliability targets.

Licensing Basis Event (LBE)
The entire collection of event sequences considered in the design and licensing basis of the plant, which may include one or more reactor modules. LBEs include AOOs, DBEs, BDBEs, and DBAs.

Mechanistic Source Term
A source term that is calculated using models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and the time-dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.

Mitigation Function
An SSC function that, if fulfilled, will eliminate or reduce the consequences of an event in which the SSC function is challenged. The capability of the SSC in the performance of such functions serves to eliminate or reduce any adverse consequences that would occur if the function were not fulfilled.

Monitoring
The systematic process of observing, tracking, and recording activities or data for the purpose of evaluating plant SSC conditions.

Monitoring and Non-destructive Examination (MANDE)
A term used in ASME Section XI, Div. 2 that includes the activities of monitoring, non-destructive examination (NDE), and use of surveillance specimens.

Non-Safety-Related with No Special Treatment SSCs (NST SSCs)
All SSCs within a plant that are neither safety-related SSCs nor non-safety-related SSCs with no special treatment SSCs.

Non-Safety-Related with Special Treatment SSCs (NSRST SSCs)
Non-safety-related SSCs that perform risk-significant functions or perform functions that are necessary for defense-in-depth adequacy (require special treatment).

Performance-Based

An approach to decision-making that focuses on desired objective, calculable or measurable, observable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based decisions lead to defined results without specific direction regarding how those results are to be obtained. At the Nuclear Regulatory Commission (NRC), performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives and flexibility for licensees to improve safety without formal regulatory intervention by the agency.

Probabilistic Risk Assessment (PRA)

A quantitative assessment of the event sequences that involve the release of radioactive material, an estimate of accident frequencies, consequences, and uncertainties.

PRA Safety Function

Reactor design-specific SSC functions modeled in a PRA that serve to prevent or mitigate a release of radioactive material, or to protect one or more barriers to release.

Prevention Function

An SSC function that, if fulfilled, will preclude the occurrence of an adverse state. The reliability of the SSC in the performance of such functions serves to reduce the probability of the adverse state.

Probability of Detection (POD)

The percentage resulting from dividing the number of detections by the number of flawed specimens or flawed grading units examined. POD indicates the probability that an examination system will detect a given flaw.

Reliability

The probability that a system or component will perform its specified function under given conditions upon demand and for a prescribed mission time.

Reliability and Integrity Management (RIM)

Those aspects of the plant design process that are applied to provide an appropriate level of reliability of SSCs and a continuing assurance over the life of the plant that such reliability is maintained. These include design features important to reliability performance such as design margins, selection of materials, testing and monitoring, provisions for maintenance, repair and replacement, leak testing, and NDE.

Reliability Target

A performance goal established for the probability that an SSC will complete its specified function in order to achieve plant-level risk and reliability goals.

Required Functional Design Criteria (RFDC)

Reactor design-specific functional criteria that are necessary and sufficient to meet the required safety functions.

Required Safety Function (RSF)

A PRA Safety Function that is required to be fulfilled to maintain the consequence of one or more DBEs or the frequency of one or more high-consequence BDBEs inside the F-C Target.

Risk-Informed

An approach to decision-making in which insights from probabilistic risk assessments are considered with other sources of insights.

Risk-Significant LBE

An LBE whose frequency and consequence meet a specified risk significance criterion. In the licensing modernization project framework, an AOO, DBE, or BDBE is regarded as risk-significant if the combination of the upper bound (95%tile) estimates of the frequency and consequence of the LBE are within 1% of the F-C Target and the upper bound 30-day total effective dose equivalent at the exclusion area boundary exceeds 2.5 mrem.

Risk-Significant SSC

An SSC that meets defined risk significance criteria. In the licensing modernization project (LMP) framework, an SSC is regarded as risk-significant if its PRA Safety Function is: (a) required to keep one or more LBEs inside the F-C Target based on mean frequencies and consequences; or (b) if the total frequency LBEs that involve failure of the SSC PRA Safety Function contributes at least 1% to any of the LMP cumulative risk targets. The LMP cumulative risk targets include: (i) maintaining the frequency of exceeding 100 mrem to less than 1/plant-year; (ii) meeting the U.S. Nuclear Regulatory Commission (NRC) safety goal quantitative health objective for individual risk of early fatality; and (iii) meeting the NRC safety goal quantitative health objective for individual risk of latent cancer fatality.

Safety Design Approach

The strategies that are implemented in the design of an NPP that are intended to support safe operation of the plant and control the risks associated with unplanned releases of radioactive material and protection of the public and plant workers. These strategies normally include the use of robust barriers, multiple layers of defense, redundancy, and diversity and the use of inherent and passive design features to perform safety functions.

Safety-Related Design Criteria

Design criteria for safety-related (SR) SSCs that are necessary and sufficient to fulfill the required functional design criteria for those SSCs selected to perform the required safety functions.

Safety-Related SSCs (SR SSCs)

SSCs that are credited in the fulfillment of RSFs and are capable to perform their RSFs in response to any DBEHL.

Safety-Significant SSC

An SSC that performs a function whose performance is necessary to achieve adequate defense-in-depth or is classified as Risk-Significant SSC.

Sizing Accuracy

The difference between the actual length, depth, flaw separation, and remaining ligaments and the values measured using a non-destructive sizing technique as determined during the performance demonstration process.

Surveillance Samples

Specimens of SSC representative materials for monitoring the material performance, relevant to meeting the RIM target reliabilities, of in-service SSCs subjected to environmental stressors. Surveillance samples are located in the same or higher levels of environmental stressors as the in-service SSCs. They are unique for each reactor design, SSC design and degradation mechanisms of concern.

Uncertainty (as used in MANDE)

A quantification representing the variability associated with monitoring and non-destructive examination (MANDE) data and includes many technique and application specific parameters such as the minimum detection capability, sizing accuracy, resolution tolerance, repeatability, consistency, etc.

Uncertainty (as used in PRA)

A representation of the confidence in the state of knowledge about the parameter values and models used in constructing the PRA.

Page intentionally left blank

Investigation and Demonstration of Reliability Target Allocation to Support Reliability and Integrity Management Program

SUMMARY

Every nuclear power plant (NPP) in the United States (U.S.) and around the world is obligated to maintain high levels of safety with measures that ensure plant reliability and integrity. These programs have become increasingly risk-informed in recent years. New reactor designs are very focused on risk-informed approaches to support all stages of development—from initial design and licensing to plant operation and retirement. The License Modernization Project (LMP) initiative by the U.S. Nuclear Regulatory Commission (NRC) is just one example of a risk-informed approach being encouraged for implementation.

The LMP initiative resulted in the issuance of Regulatory Guide (RG) 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors” [3]. RG 1.233 endorses Nuclear Energy Institute (NEI) 18-04, Revision 1, “Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development” [2] as one acceptable method for non-light water reactor (LWR) designers to use for selection of licensing basis events (LBEs); classification and special treatments of structures, systems, and components (SSCs); and assessment of defense-in-depth (DID). All of these activities are fundamental to the safe design of non-LWRs.

The NEI 18-04 document provides guidance for the following technology-inclusive, risk-informed, and performance-based (TI-RIPB) processes that must be completed to satisfy the requirements of RG 1.233:

- Systematic definition categorization and evaluation of event sequences for selection of LBEs, which include anticipated operational occurrences (AOOs), design basis events (DBEs), design basis accidents (DBAs), and beyond design basis events (BDBEs)
- Systematic safety classification of SSCs, development of performance requirements, and application of special treatments
- Systematic adherence to guidelines for evaluation of DID adequacy.

Some of the above processes are well-known since they were and still are used for licensing of LWRs, such as systematic definition and evaluation of event sequences and evaluation of DID. However, the systematic safety classification of SSCs, development of performance requirements, and application of special treatments are somewhat unfamiliar to LWRs. More specifically, development and monitoring of performance requirements are a completely new problem that does not exist in the LWR domain. The reason is that development and monitoring of performance requirements is the essence of a performance-based approach, a methodology not yet fully embraced and employed by LWRs. While a performance-based approach for risk management is very beneficial, LWRs have historically leaned toward deterministic methods, and only recently started shifting toward risk-informed approaches and, in lesser degree, to performance-based approaches.

Given the novelty of the process, the advanced reactor industry has an understandable difficulty in its interpretation and proper implementation. Fortunately, another industry initiative led by the American Society of Mechanical Engineers (ASME) has been in development for a few years—requirements for a reliability and integrity management (RIM) program for NPPs [1]. The objective of the RIM program is to define, evaluate, and implement strategies to ensure that performance requirements for SSCs are defined, achieved, and maintained throughout the plant lifetime. As such, the ASME RIM program fits extremely well with the objectives of the TI-RIPB approach described in RG 1.233 and, given its

acceptance by the NRC, can serve as an acceptable and satisfactory approach to addressing the process of systematic safety classification of SSCs, development of performance requirements, and application of special treatments.

NRC’s acceptance of the ASME RIM program was provided through the issuance RG 1.246, “Acceptability of ASME Code, Section XI, Division 2, Requirements for RIM Programs for NPPs, for non-LWRs” [4].

RG 1.246 “describes an approach that is acceptable to the staff of the NRC for the development and implementation of a preservice (PSI) and in-service (ISI) program for non-light water reactors” [4]. ASME Section XI, Division 2 also provides the requirements for the creation of the RIM program for any type of non-LWR NPP. The RIM program can be beneficial to the industry by reducing implementation costs and providing consistency in implementation for users. However, because ASME Section XI, Division 2 complies with ISI requirements through application of processes that are common to current LWR designs, there is limited experience for advanced reactor designs to draw from and limited guidance on meeting the requirements for the development of the risk-informed RIM program.

Therefore, Regulatory Framework Modernization Program within Regulatory Development supporting the Department of Energy’s (DOE) Office of Nuclear Energy initiated a project to develop guidance based on the ASME Section XI, Division 2 requirements for non-LWR developers through the establishment of the risk-informed RIM program.

1. PROJECT DESCRIPTION

1.1 Scope and Objectives

The scope of this project is to develop a framework supporting RIM development and implementation strategies for advanced reactors. This work supports the establishment of a defined and predictable regulatory framework by providing guidance for the development of a RIM program which directly supports the LMP approach for licensing of advanced reactors endorsed in RG 1.233.

The objective of this project is to support the design and continuous performance assessment of advanced nuclear power reactors with a framework and a guidance document that provides directions on the use of reliability targets, associated reliability allocation, and RIM strategies. The results obtained from this effort directly address the goal of enabling the deployment of advanced nuclear reactors by reducing the regulatory risks and uncertainties associated with their commercial deployment.

The research conducted in fiscal year (FY) 2022 [5] exposed the extreme complexity of the topic of reliability target allocation performed either as part of the LMP process (per RG 1.233) or as part of the RIM program development (per RG 1.246). To further support the advanced reactor community, the research continued into FY-23 to explore in greater detail the reliability targets allocation process. The goal of this research is to support advanced reactor developers with an approach for reliability target allocation that is:

- Aligned with methodology and guidance provided in both RG 1.233 and RG 1.246
- Based on proven and sound technical theories that are repeatable and demonstratable
- Technology-inclusive (i.e., any reactor design should be able to follow developed methods)
- Capable of addressing uncertainty considerations
- Simple and clear in order to minimize industry efforts and reliance on subject-matter experts.

In FY-23, the project continued the research started in FY-22 by expanding methodology for systematic, risk-informed allocation of reliability targets, starting from the plant-level reliability targets decomposed to system- and component-level reliability targets. The research in FY-23 also covered using systems engineering and digital engineering methods and tools, specifically Model-Based Systems Engineering (MBSE) to make RIM program development more effective and efficient while ensuring that all regulatory requirements are met.

To support the discussions in the following sections, we first need to describe reliability target, capability target, and health terms as well as relationships between them.

A capability target of a system or component is the definition of what a system (or a component) shall do in order to achieve plant-level and system-level performance goals. A capability target is both described and prescribed via functional and performance requirements for a system or component. Capability can also be described as a set of success criteria used in the PRA to describe what constitutes successful performance to preclude unwanted consequences. Example: a system shall deliver water flow with the rate of at least 100 gallons per minute with at least 35 psi pressure.

A reliability target is a performance goal established for the probability that the plant, system, or component will complete its specified function in order to achieve plant-level risk and reliability goals. Reliability and capability are related: reliability is the quantified measure of confidence that a required capability will be achieved. Example: system reliability to achieve required performance (described above as the capability example) is 99.5% or probability of system to fail to achieve required performance is 0.05%.

Health is a quantitative or qualitative measure of a system's (or component's) fitness, or ability, to satisfy functional and performance requirements (i.e., prescribed capability). While reliability and health both describe the ability to achieve required performance, reliability describes the confidence of performance expectation while health describes physical conditions and how close the current physical conditions are to the perfect condition (e.g., brand new). Example: the system rated performance is water flow with the rate of 150 gallons per minute at 50 psi pressure; the measured performance (i.e., health condition) is 120 gallons per minute at 40 psi pressure. The current system condition is degraded compared to the rated performance expected from a brand new system, but this performance is still above the minimum required performance of the previously cited 100 gallons per minute. Thus, the system successfully accomplishes prescribed performance requirements.

The outcome for this project is a framework that the nuclear power industry can use when developing ways to establish and meet reliability targets to comply with the requirements of RG 1.233 as well as requirements of RG 1.246. Another outcome is an efficient and effective approach for the RIM program development and implementation that uses MBSE methods and tools.

1.2 Description of RIM Program Development

1.2.1 Integrated Risk-informed Approach to Plant Operations

Figure 1 presents the conceptual framework for a RIM program. The development of a RIM program requires determination of:

- WHAT to monitor/examine to meet the end-goal plant operational requirements (i.e., safety, investment protection, and licensing)
- HOW to monitor/examine the “selected what”

As the result of RIM program implementation, a RIM strategy is developed to monitor the performance of the system at each level, at either the complete system or multiple subsystems, and for each SSC.

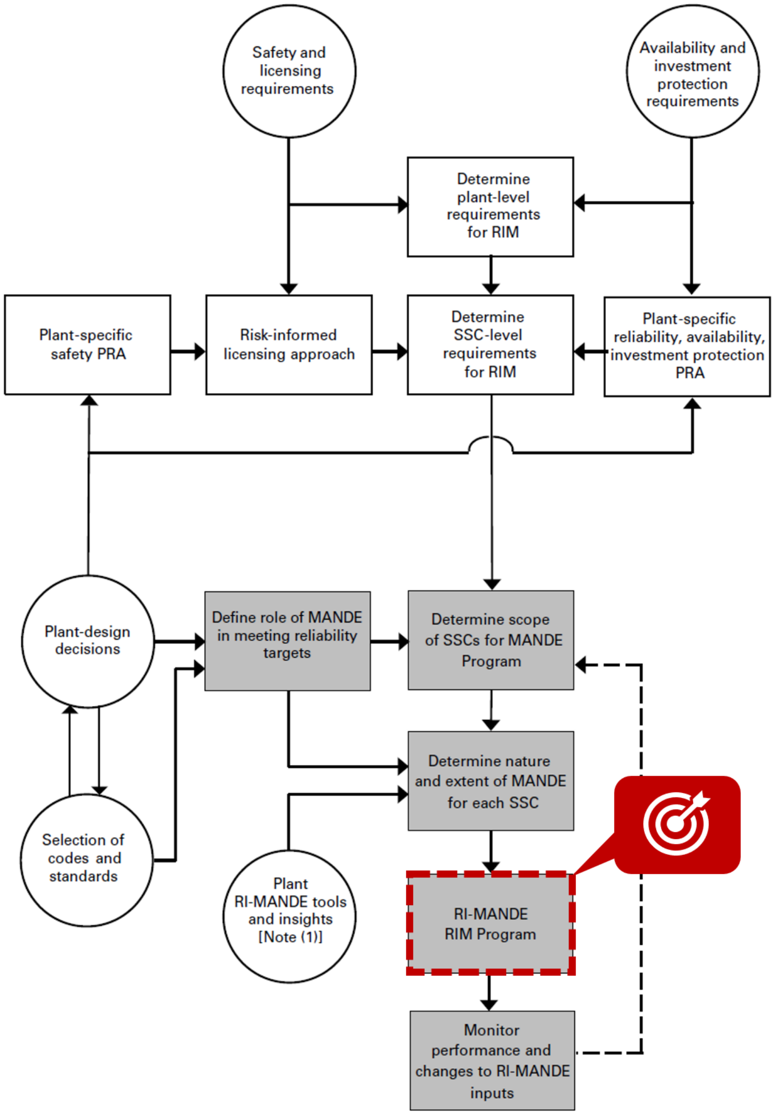

Safety and licensing requirements
Availability and investment protection requirements
Determine plant-level requirements for RIM
Plant-specific safety PRA
Risk-informed licensing approach
Determine SSC-level requirements for RIM
Plant-specific reliability, availability, investment protection PRA
Plant-design decisions
Define role of MANDE in meeting reliability targets
Determine scope of SSCs for MANDE Program
Determine nature and extent of MANDE for each SSC
Selection of codes and standards
Plant RI-MANDE tools and insights [Note (1)]
RI-MANDE RIM Program
Monitor performance and changes to RI-MANDE inputs

Figure 1. RIM program conceptual framework [1].

1.2.2 Plant and Structures, Systems, and Components Reliability Target Allocation

The reliability target allocation is a complex process because it involves considering multiple aspects largely grouped into two categories:

- Regulatory limits on the risks, frequencies, and radiological consequences of LBEs determined based on multiple considerations including deterministic analyses and evaluations, insights obtained from the plant probabilistic risk assessment (PRA), and defense-in-depths aspects.
- Requirements for plant availability and investment protection defined by the limits on the risks related to the loss of production and loss of assets determined by the plant reliability, availability, investment protection PRA.

The objective of selecting reliability targets is to establish a benchmark that will be used for evaluating system performance. As such, reliability targets are developed during the initial phase of the RIM program, and later, the actual plant performance is measured against the reliability targets to identify deviations from the expected performance. Therefore, reactor developers should be extremely cautious about setting reliability targets that are overly conservative (i.e., reliability values are unnecessarily high) because these targets will dictate potentially unrealistic expectations for the plant systems and components performance, resulting in an increase of operational costs.

The difficulty with reliability target allocation is due to an uncertainty as to how much of a risk increase (or reliability decrease) each SSC can afford before regulatory limits are compromised. This is a tricky question because an incremental risk increase for one SSC may not change anything at the plant level, whereas the same small risk increase in multiple SSCs can have a detrimental effect. Figure 2 presents a schematic of the reliability target allocation process, which also demonstrates the previously mentioned difficulty where multiple options for reliability targets are available at each level.

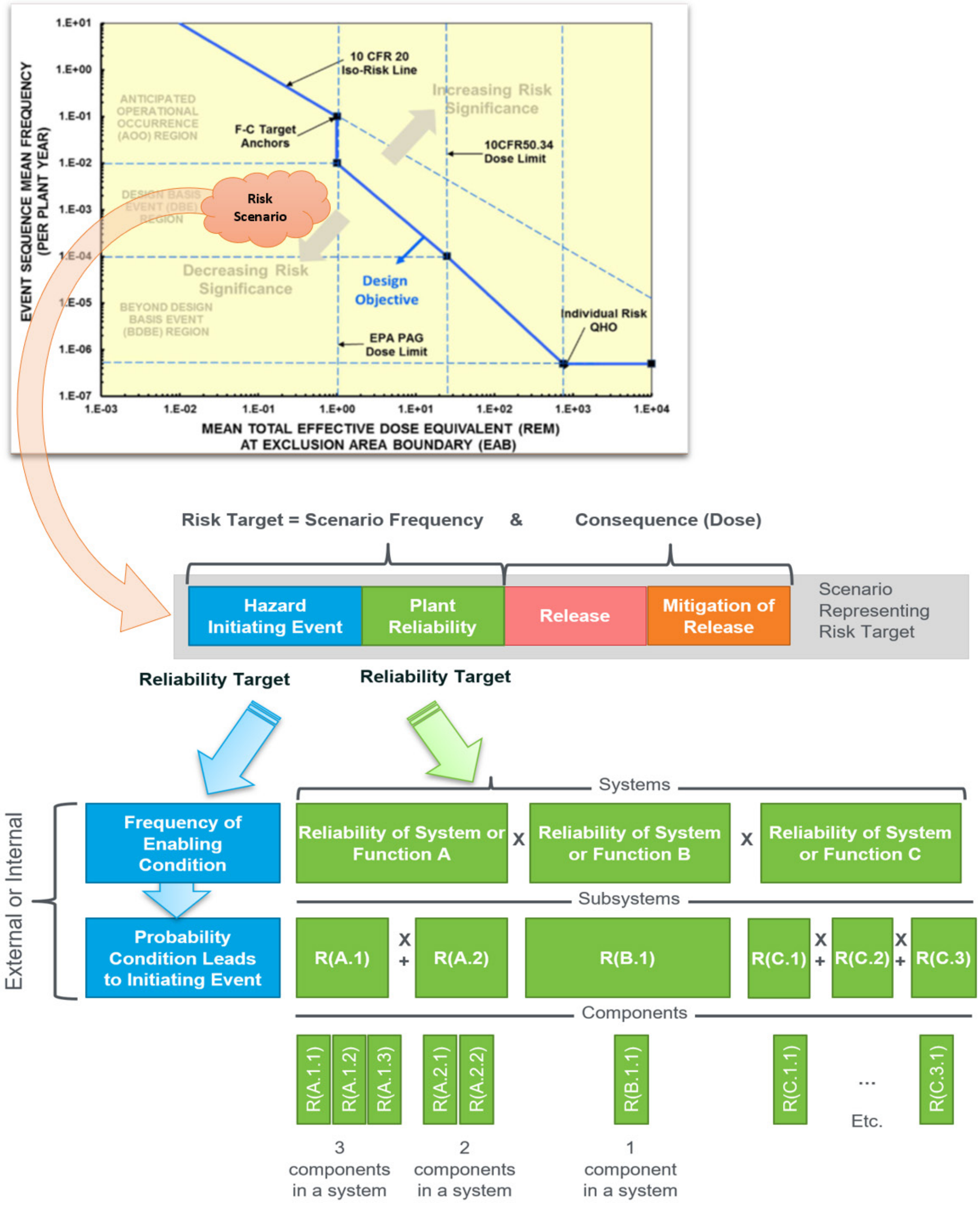


Figure 2. Schematic of reliability target allocation process.

2. RELIABILITY TARGET ALLOCATION CASE STUDY

Reliability target allocation is the key task in the risk-informed, performance-based licensing bases development following RG 1.233 [3] and in the RIM program development [1]. Figure 2 in Section 1 presents a schematic of the reliability target allocation process and demonstrates the difficulty of this process since multiple options for reliability targets are available. As part of this project, we performed a reliability target allocation for a simplified case study as discussed below.

The guidance in RG 1.233 or RG 1.246 does not specify process or provide directions as to how to establish reliability and capability targets that would meet the requirements. The high-level requirement identified in NEI 18-04 is that "the reliability targets are set to ensure that the underlying LBE frequencies and consequences meet the LBE evaluation criteria with sufficient margin" and that "information from the PRA is used as input to the selection of reliability targets. [2]"

Guidance for reliability targets allocation in ASME Section XI, Division 2 is also very narrow: "Plant-level reliability shall be derived from regulatory limits on the risks, frequencies, and radiological consequences of licensing basis events that are defined in the [PRA]," and, "The PRA model shall be used to allocate SSC reliability targets from and consistent with the plant-level reliability goals." As such, one of the top requests from the industry is to develop methodologies and guidance to support the reliability target allocation process in a consistent, repeatable, defensible, and verifiable manner that could be followed regardless of reactor technology. This project addressed this undertaking with results and findings discussed in the following sections.

Both NEI 18-04 and ASME Section XI, Division 2 indicate that reliability target allocation should be done at the plant-level first with the final goal of having reliability targets assigned to every SSC. The problem of reliability target allocation may be extremely large due to the presence of hundreds of SSCs, many SSCs contributing to multiple sequences, and each SSC Reliability Target having a range of acceptable values.

For example, let's consider a plant with only 100 SSCs and only two options for a reliability target assignment (e.g., one option uses a realistic reliability value, and a second option uses a more conservative value). This scenario would result in a total of 1.27E+30 possible combinations (2 options ^ 100 components = 1.27E+30 possibilities) of a reliability target allocation for plant SSCs. The goal of reliability target allocation is to find the appropriate reliability target values that would (1) satisfy all regulatory requirements; (2) be feasible to achieve (i.e., SSC actual performance can meet the assigned reliability target); and (3) be acceptable from economic perspective. Given these goals and the extremely large number of possible combinations, the reliability target allocation process is certainly a great challenge.

2.1 Framework for Reliability Target Allocation

This project has developed a systematic framework for the reliability target allocation as discussed in the following sections.

2.1.1 Problem Formulation

Without loss of generalization, let's consider an advanced reactor (AR) design consisting of a set of SSCs, the goal of a reliability target allocation process, from a RIM point of view, is to determine the reliability value for the subset of SSCs that are under the RIM program. In our view, such a process is designed in a way that regulatory (or safety) driven constraints are satisfied and operations and maintenance (O&M) costs are minimized (see Figure 3). In addition, it is relevant to highlight that an asset reliability target comprises several factors such as its design and its lifecycle strategy (i.e., planned replacement time along with type and frequency of surveillance, testing, maintenance, and inspection activities). Both factors affect the final reliability value associated with the SSC basic event(s) (BE) in the AR PRA model.

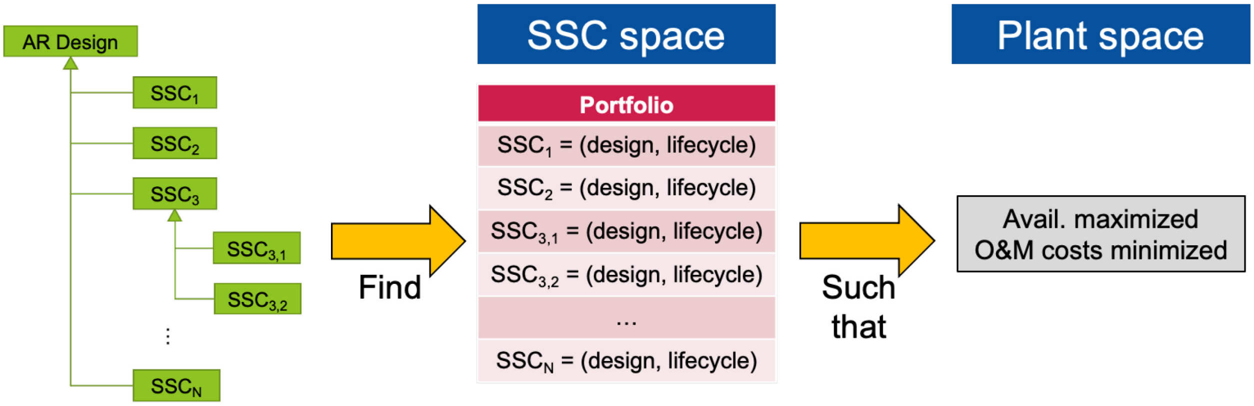

AR Design
SSC$_1$
SSC$_2$
SSC$_3$
SSC$_{3,1}$
SSC$_{3,2}$
⋮
SSC$_N$
Find
SSC space
Portfolio
SSC$_1$ = (design, lifecycle)
SSC$_2$ = (design, lifecycle)
SSC$_{3,1}$ = (design, lifecycle)
SSC$_{3,2}$ = (design, lifecycle)
…
SSC$_N$ = (design, lifecycle)
Such that
Plant space
Avail. maximized
O&M costs minimized

Figure 3. Graphical representation of the reliability target allocation process.

Note that the formulation of the RIM program indicated above and shown in Figure 3 can be framed as an optimization problem where the design space is the design and lifecycle choices of each SSC, the objective is cost driven, and the constraints are regulatory driven. The optimization formulation is in a single-objective form:

$$\begin{array}{cc} \min\limits_{\boldsymbol{opt}} & cost(\boldsymbol{opt}) \\ such\ that & f_m^{RR}(\boldsymbol{opt}) \leq f_{reg}^{RR} \end{array}$$

where:

- $\boldsymbol{opt} = [opt_1, \ldots, opt_S]$ represents the "decision space" and consists of the set of options of the considered S SSCs.
- $cost(\boldsymbol{opt})$ represents the cost of a generic option $\boldsymbol{opt}$, and in its most simple form (as in this work), is the sum of the costs associated with each asset option: $cost(\boldsymbol{opt}) \ = \sum_{s=1}^{S} cost(opt_s)$.
- $f_m^{RR}(\boldsymbol{opt})$ represents the frequency of radioactive release for the considered initiating event (IE) m, which is upper bounded as dictated by the regulatory limit.
- f_{reg}^{RR} represents the regulatory limit on the frequency of radioactive release

Here, a generic AR is characterized by the following constituent elements:

- The plant consists of S SSCs (e.g., heat exchanger, pipes, centrifugal pumps, motor-operated valves) designed to support system functions. Each SSC is modeled from a reliability standpoint by one or more BEs, where R represents the number of the complete set of BEs.
- The set of options for each of the S SSCs is well defined.
- A set of M IEs are considered, IE_m $(m = 1, \ldots, M)$, where the frequency f_m of occurrence of each IE_m is known. A PRA model $\mathbb{R}_m$ is available for each IE. $\mathbb{R}_m$ determines for IE_m the frequency f_m of an undesired event called an event sequence (e.g., frequency f_m^{CD} of core damage or frequency f_m^{RR} of radioactive release). The $\mathbb{R}_m$ consists of a set of fault trees and event trees. For each IE_m it is possible to calculate $f_m = \mathbb{R}_m(f_m, P_1, \ldots, P_r, \ldots, P_R)$ where P_r indicates the probability of each BE BE_r $(r = 1, \ldots, R)$.

2.1.2 System-Centric Reliability Target Allocation

The system-centric approach has been designed to solve the RIM target allocation problem in such a way that it can be solved using off the shelf computing machines. This approach follows a divide-and-conquer strategy, and is structured in two steps, each involving an optimization process as indicated in Figure 4.

- Step 1. In the first step, our approach decomposes the set of fault trees (FTs) that are an integral part of the plant PRA model into a minimal set of groups. Each group is composed of a set of FTs that are logically connected (i.e., represents a physical system) and are present in only one single group (more details on how this grouping can be performed are provided below). Each group is solved separately (i.e., the set of minimal cut sets [MCSs] is obtained). Then, a Pareto frontier (i.e., multi-objective) optimization that balances group reliability and group cost is performed; the outcome of this process is the optimal option for each of the SSCs that are part of the same group. The obtained Pareto frontiers are used primarily to filter out non-optimal system configurations and keep the problem tractable by making the problem complexity smaller (dimensionality wise).

- Step 2. In the second step, a single-objective optimization is performed; here the full plant PRA model is used but the decision space is no longer the full set of SSCs that are part of the RIM program but, instead, the set of groups (i.e., plant systems) that were identified in Step 1 (and, hence, greatly reduced in number). The goal is to minimize O&M costs by choosing for each group the optimal Pareto frontier point from the set obtained in Step 1.

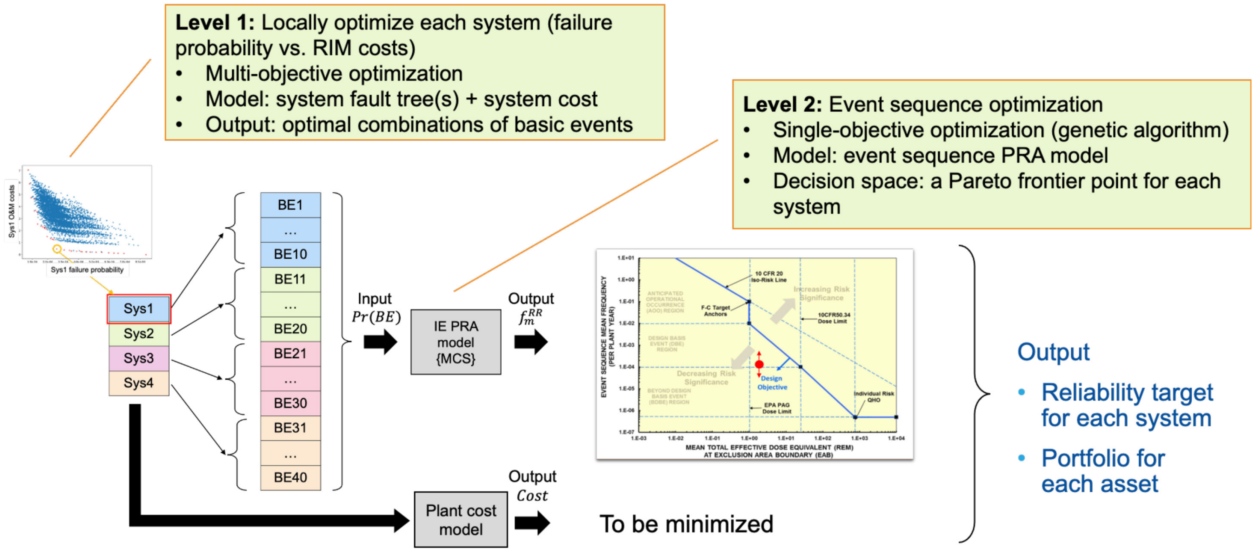

Level 1: Locally optimize each system (failure probability vs. RIM costs)
• Multi-objective optimization
• Model: system fault tree(s) + system cost
• Output: optimal combinations of basic events
Level 2: Event sequence optimization
• Single-objective optimization (genetic algorithm)
• Model: event sequence PRA model
• Decision space: a Pareto frontier point for each system
Sys1 O&M costs
Sys1 failure probability
Sys1
Sys2
Sys3
Sys4
BE1
...
BE10
BE11
...
BE20
BE21
...
BE30
BE31
...
BE40
Input
$Pr(BE)$
IE PRA model {MCS}
Output
f_m^{RR}
Plant cost model
Output
$Cost$
EVENT SEQUENCE MEAN FREQUENCY (PER PLANT YEAR)
MEAN TOTAL EFFECTIVE DOSE EQUIVALENT (REM) AT EXCLUSION AREA BOUNDARY (EAB)
1.E+01
1.E+00
1.E-01
1.E-02
1.E-03
1.E-04
1.E-05
1.E-06
1.E-07
1.E-03
1.E-02
1.E-01
1.E+00
1.E+01
1.E+02
1.E+03
1.E+04
10 CFR 20 Iso-Risk Line
ANTICIPATED OPERATIONAL OCCURRENCE (AOO) REGION
F-C Target Anchors
Increasing Risk Significance
10CFR50.34 Dose Limit
DESIGN BASIS EVENT (DBE) REGION
Decreasing Risk Significance
Design Objective
BEYOND DESIGN BASIS EVENT (BDBE) REGION
EPA PAG Dose Limit
Individual Risk QHO
To be minimized
Output
• Reliability target for each system
• Portfolio for each asset

Figure 4. Graphic representation of system-centric optimization approach for a system of four subsystems and 40 BEs.

2.1.3 Case Study Description

To show how reliability target allocation can be performed using the proposed optimization-based approach, we have selected the large loss of coolant accident (LLOCA) IE which is part of a publicly available pressurized-water reactor (PWR) PRA model. Note that from a conceptual point of view, the fact that the considered PRA model represents an LWR instead of an AR is irrelevant. The LLOCA PRA model is composed of a single event tree and multiple fault trees. The systems shown in Table 1 are credited for the mitigation of a LLOCA event.

Table 1. Systems identified in the LLOCA PRA model.

System ID	Description
ACC	Accumulator tanks
ACP-480	480V AC power system
ACP-4160	4160V AC power system
CCW	Component cooling water

System ID	Description
DCP-125	125V DC power
EPS-SWS	Emergency power system service water system
LPI	Low-pressure injection system
LPR	Low-pressure recirculation system
RWST	Refueling water storage tank
SWS-TRNA	Service water system train A

This document expands the work started in FY-22, where 92 assets subject to a RIM program were identified (from 10 systems). They represent the decision space of the reliability target allocation example problem, and, hence, it is required to determine the optimal configuration of reliability targets for these 92 SSCs. For argument's sake, we allowed two reliability options for each SSC represented by a BE in the PRA model with a corresponding reliability and cost values: a high reliable and expensive option, and a low reliable and a cheaper option. The goal is to identify the optimal option (out of the two considered) for each asset.

2.2 Fault Tree Grouping for Reduction of Problem Size

To efficiently carry out the multi-objective optimization, fault trees must be grouped to minimize the number of variables to optimize. Each fault tree group is where multi-objective optimization will be performed. These groups make up the network of fault trees in each event tree branching condition. To perform the overall optimization efficiently, each group must be consistent and unique among the event tree branching conditions, so the variables are independent (i.e., BEs are not shared between the groups). The following criteria are defined to ensure the groups are consistent and unique.

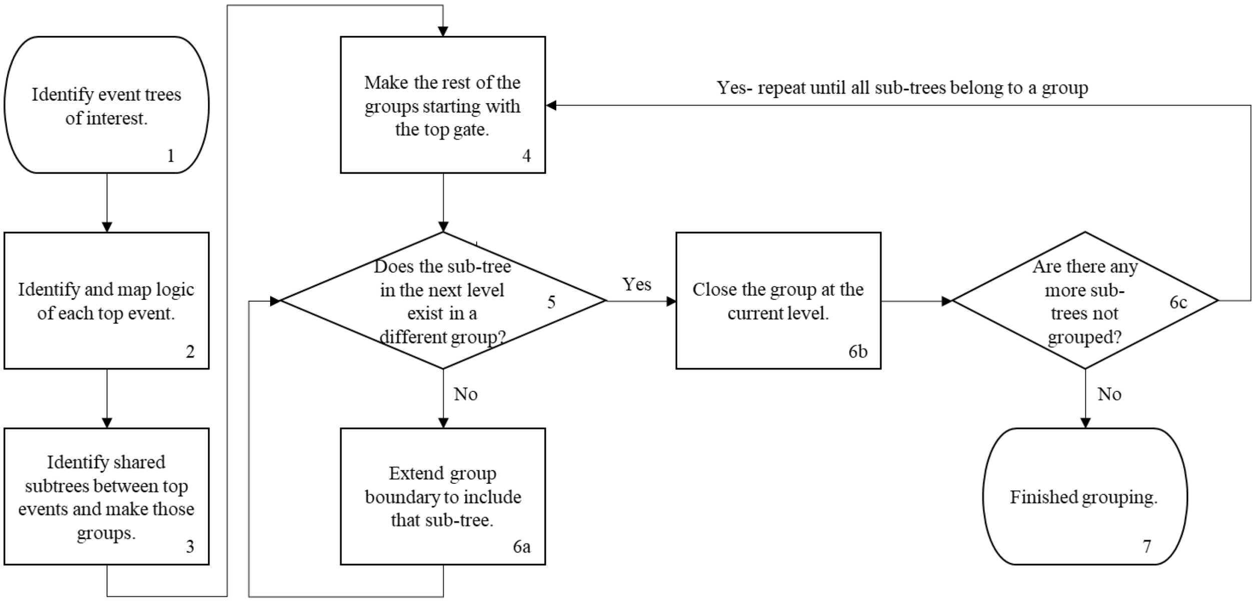
1. Each group should be of the same structure among the different fault trees it belongs to.
2. A fault tree in a group can be found only as part of the same group.
3. Basic events should only be queried within a single group.
4. Fault tree groups that represent a single train of a system that has multiple identical trains for redundancy will be considered under a single group that represent one arbitrary train.

Once the groups are determined, the MCSs can be solved for each group. The MCSs and their probability of occurrence are then used in the multi-objective optimization.

Initially, the grouping and preparation for solving MCSs was performed manually. The process became incredibly time intensive to properly meet the criteria. This led to the development of a more reliable and robust automated grouping script. These grouping methods are explained further in the following sections.

2.2.1 Manual Grouping

The process for manually grouping and solving the fault trees begins with the event tree logic of interest and ends with the MCSs of each group determined. To start the grouping process, shown in Figure 5, the top events of the event tree are identified. The logic of those top events is manually mapped to focus on which sub-fault trees share sub-trees. The map shows the top event and all of the lower levels of sub-trees. These sub-trees are compared with each other to see which ones exist in different top events or multiple higher level sub-trees. Those which are called in multiple places are defined as their own group which ensures the first three criteria listed in Section 2.2 are met. Then, for each top event starting from the very top gate, a group is expanded to as low a level as possible before encountering the groups that were already made or until a sub-tree is identified in multiple places within that same top event. The steps mentioned so far take into consideration criteria 1 and 2. Criteria 3 and 4 were thought about more passively throughout the process. If it was obvious that these criteria were not met, then an adjustment would be made.



Identify event trees of interest.
1
Identify and map logic of each top event.
2
Identify shared subtrees between top events and make those groups.
3
Make the rest of the groups starting with the top gate.
4
Does the sub-tree in the next level exist in a different group?
5
Yes
No
Extend group boundary to include that sub-tree.
6a
Close the group at the current level.
6b
Are there any more sub-trees not grouped?
6c
Yes- repeat until all sub-trees belong to a group
No
Finished grouping.
7

Figure 5. Flow chart of manual grouping which does not explicitly include consideration of criteria 3 or 4.

For an example, this grouping process was used for the LLOCA event tree using the step numbers in Figure 5. Step 1 selected the LLOCA event tree. Step 2 included identifying the top events of the accumulator system (ACC), low-pressure injection system (LPI), and low-pressure recirculation (LPR) system and manually creating the maps of those top events. Step 3 included identifying the shared trees such as electrical dependencies of direct current (DC) and alternating current (AC) power systems. Step 4 is where the more judgment-based process begins. Determining the answer to Step 5, when starting to expand a new group, was not trivial. Cross-referencing the LPI and LPR fault trees required close attention.

Once the first iteration of the grouping was complete, shown in Figure 6, three errors and an intricacy were noticed in the groups of the LPI fault tree. The errors were related to criteria 2 (a fault tree in a group can be found only as part of the same groups). The LPI heat exchanger trains, residual heat removal motor driven pump trains, and the 480 V AC power system were also in the LPR fault tree but were not initially noticed and therefore were included in other groups. This required breaking out what was initially group 1 into group 1i and group 1ii, as well as breaking out what was initially group 3 into 3i and 3ii. The intricacy was related to criteria 4 (fault tree groups that represent a single train of a system that has multiple identical trains for redundancy will be considered the same group). This case was not a train but nearly identical power systems with different functions. The emergency power system 125 V DC power system is nearly identical in logic structure to the regular 125 V DC power system. See the groups in Figure 6 highlighted in yellow. Gray outlines show initial groups, black outlines show final groups. The groups outlined in red are all treated as one group due to high similarities.

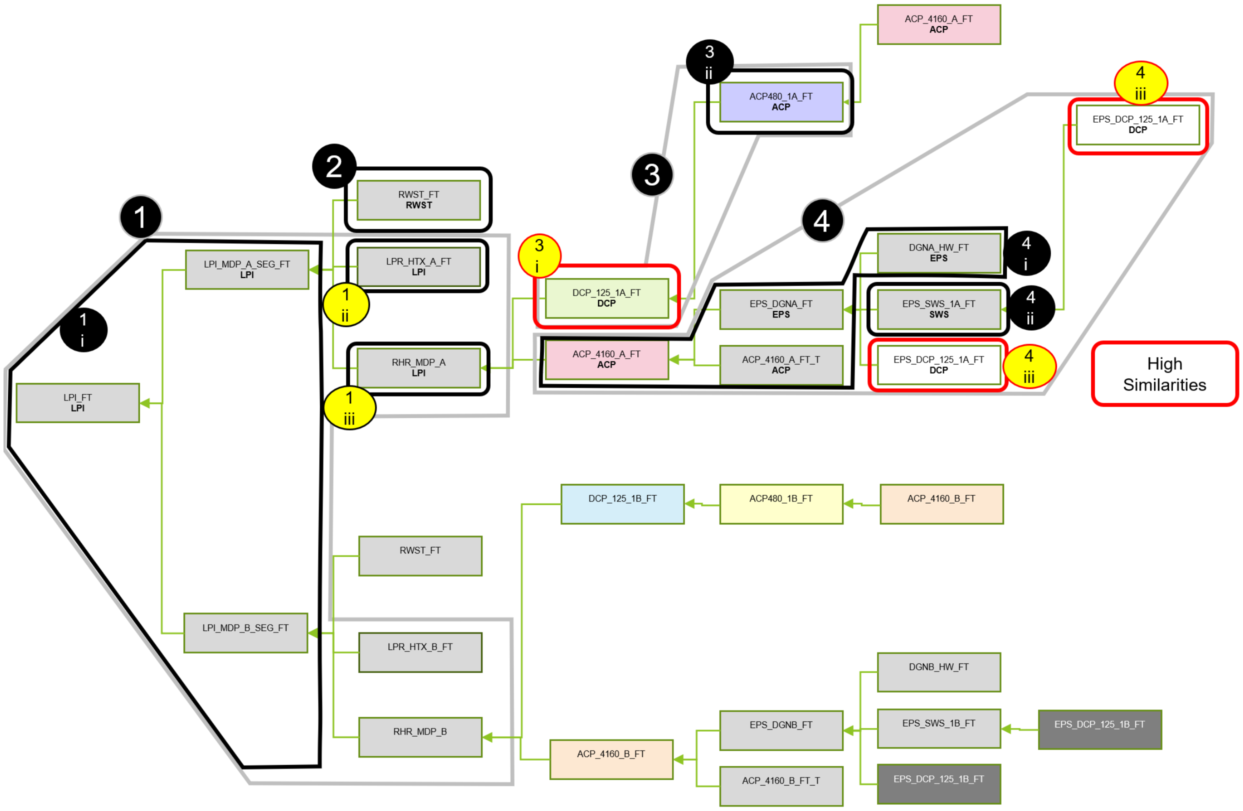


Figure 6. LPI fault tree highlighting changes made after initial inspection.

The second half of the overall process is manipulating the original fault tree logic to match the groupings made so the minimal cut sets of the groups could be solved for. Using the fault tree groups and mapping as a guide, the surrogate fault trees are made top-down similarly to how the groups were created. From the original top-event fault tree, all the sub-trees outside the group are removed. This is saved as a new surrogate top-event fault tree. After that, the original top-event fault tree file is opened again, and all sub-trees of the next group are selected and saved as their own group. In the case of a group like the one that starts with the 125 V DC power system, where the cut off is two sub-tree levels below to not include the 4160 V AC power system, the sub-tree in the middle must be edited so that the 4160 V AC power system is removed and this newly edited tree is the one called in the 125 V DC power system, not the original one. Looking at Figure 6, this kind of layered edit needed to be made twice for the groups starting with the DC and 4160 V AC power system and the 125 V DC power system. Then regular edits to sub-trees needed to be made three other times to create groups 1i, 1ii, and 1iii. Performing all these edits was time consuming and required close attention to detail to ensure the correct surrogate trees were being created and replaced as needed. This also made it tedious to then solve for minimal cut sets for each of the eight groups.

When the problem space was expanded from one event tree to six, it quickly became apparent that the manual grouping and fault tree solving would be an excessive task. Between the six event trees, there are 18 major subsystem top-event fault trees each with electrical dependencies, multiple trains, and other sub-trees. It would be unreasonable to cross reference them all manually to optimize the grouping size while meeting all the criteria. If done, it would likely include errors, as errors were made in the one event tree space. Another method was required.

The process of separating the PRA model into independent fault trees could be significantly simplified or avoided altogether by developing the PRA model where fault trees for plant main systems (e.g., heat removal from the reactor) and supporting systems (e.g., electrical power, cooling water) are independent for the purpose of the PRA model. However, if the PRA model is developed in a more traditional way (i.e., replicating the approach used for LWR PRA models), the automated process described in the following section offers an efficient approach to separating fault trees and BEs into independent groups.

2.2.2 Automatic Grouping

Based on the previous section, the process of manually grouping fault trees is shown to be difficult and time consuming. Therefore, automation of the process provides the benefit of reducing the time required as well as the potential for human errors. To automate the grouping process, a Python script was developed. The first task of the script is to read the required information from the Systems Analysis Program for Hands-on Integrated Reliability Evaluation (SAPHIRE) model. The SAPHIRE model can be exported to multiple text files based on the type of information. For the fault tree grouping, the script needs access to three files: the fault tree logic (FTL) file, the basic event information (BEI) file, and the event tree logic (ETL) file.

The FTL file has all fault tree logic information for the entire SAPHIRE model. This includes the gate types in a fault tree, the BEs in a fault tree, and transfers to other fault trees. The BEI file provides information regarding the BEs. For this purpose, the reason for reading the BEI file is to get a listing of all the BEs so that those can be identified in the fault trees. The ETL file has all the event tree logic information for the entire SAPHIRE model. This includes what the top events (fault trees) are in each event tree. The ETL file is needed to determine what fault trees are used as top events so that connections can be made starting with those fault trees. The names of these three files are required via an input file that the script reads.

Once the script was able to read the required files, verification was needed that the script was storing the structure of the fault trees appropriately. To perform the verification, the script was modified to print a graph structure of the fault trees based on the stored information from reading the files. This allowed the graph structure from the script to be compared to the fault tree in SAPHIRE. As an example of the verification, Figure 7 shows the fault tree logic for the accumulator in SAPHIRE and Figure 8 shows the graph structure for the accumulator produced from the script. In Figure 8, the orange circles denote “or” gates, the purple circles denote “N out of M” gates, the pink circles denote “transfer” gates, the green circles denote “and” gates, and the blue circles denote BEs. After comparison of the SAPHIRE fault tree logic to the script fault tree logic, the script was found to read and store the information correctly and confirmed that the fault tree logics match.

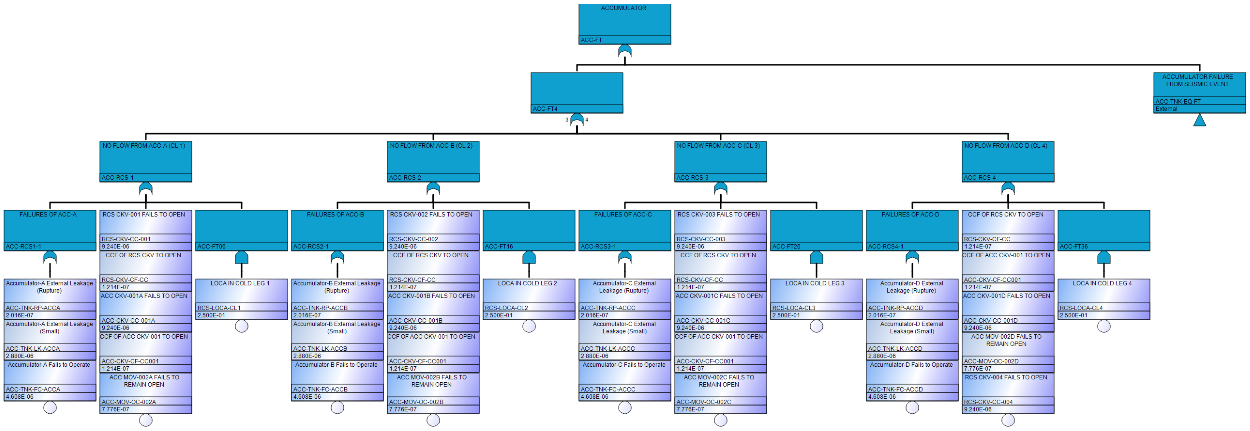


Figure 7. SAPHIRE accumulator fault tree logic.

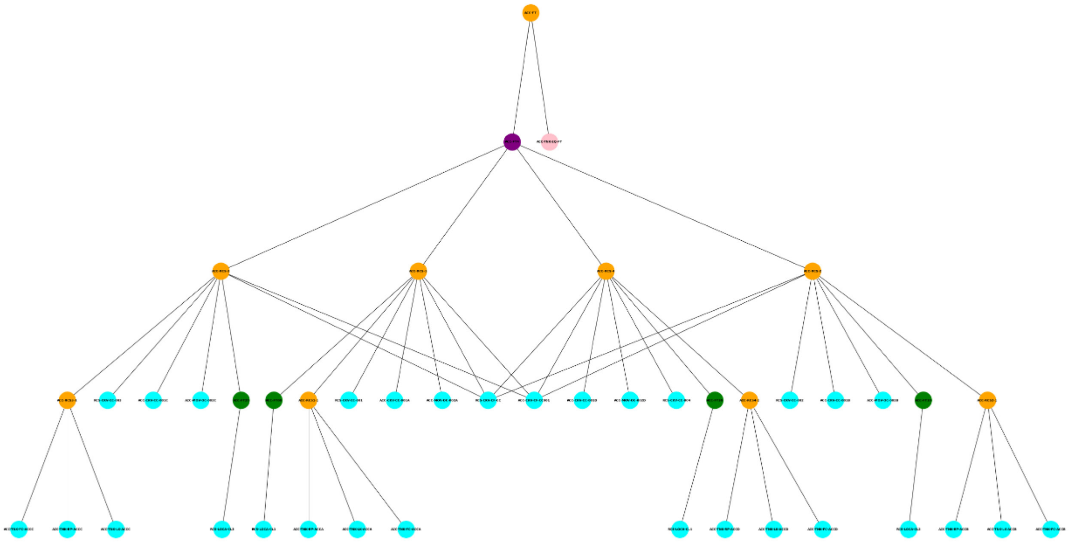


Figure 8. Python script accumulator fault tree logic.

The next task to incorporate into the script is determination of the fault-tree-to-fault-tree transfers. This is required because it will be used in the grouping of the fault trees. Therefore, the script reviews the fault tree logic looking specifically for transfers to other fault trees. At this point, BEs in the fault trees are ignored. During this step, the event tree logic top events are used. These top events (fault trees) are then used as the starting point to determine the fault tree transfers cascading down. Again, the script structure needed to be verified to determine that fault-tree-to-fault-tree transfers were performed correctly. This verification occurred by comparing the fault tree transfers for the LPI system. Figure 9 shows the manual fault-tree-to-fault-tree transfer for the LPI system and Figure 10 shows the scripts fault-tree-to-fault-tree transfer for the LPI system.

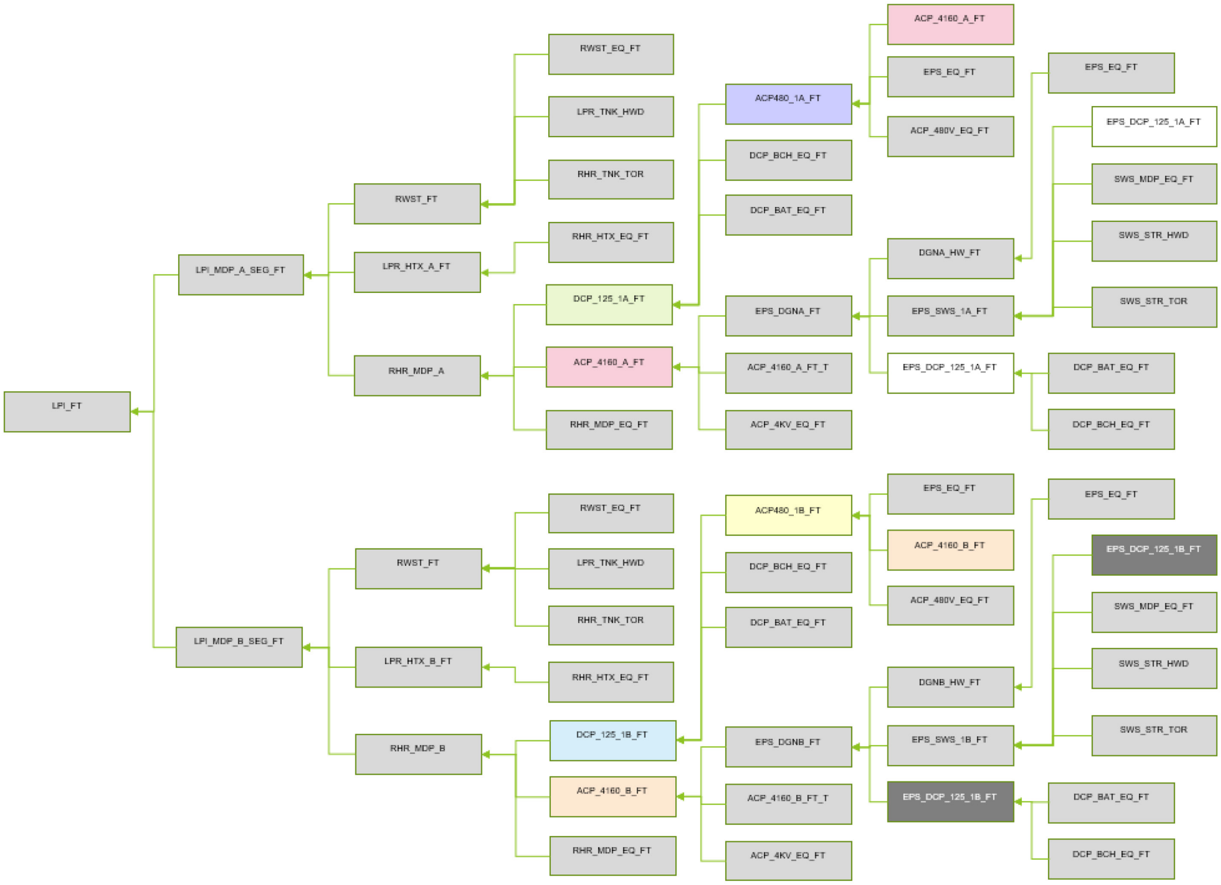


Figure 9. LPI system manual fault-tree-to-fault-tree structure.

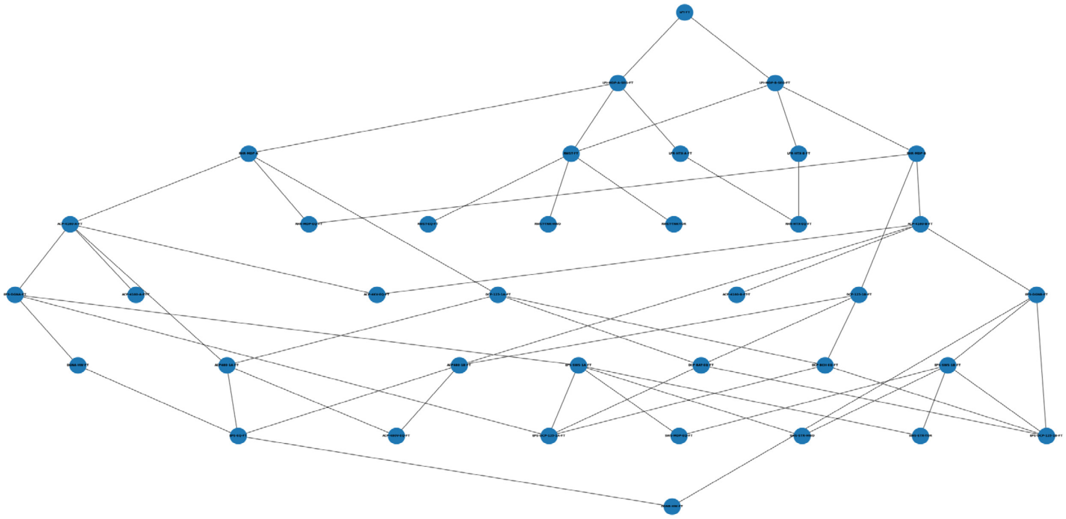


Figure 10. Python script LPI system fault-tree-to-fault-tree structure.

Reviewing the two figures, it is obvious that Figure 10 has a different structure than Figure 9. The reason being is that the script does not duplicate fault trees in the graph structure. Instead, it just adds another connection to that fault tree node. After comparing the two structures, one difference was identified between the two structures. The difference between the two structures was a difference in the names of two fault trees, shown in Figure 11 in the red boxes. Otherwise, the fault-tree-to-fault-tree transfer structure was the same.

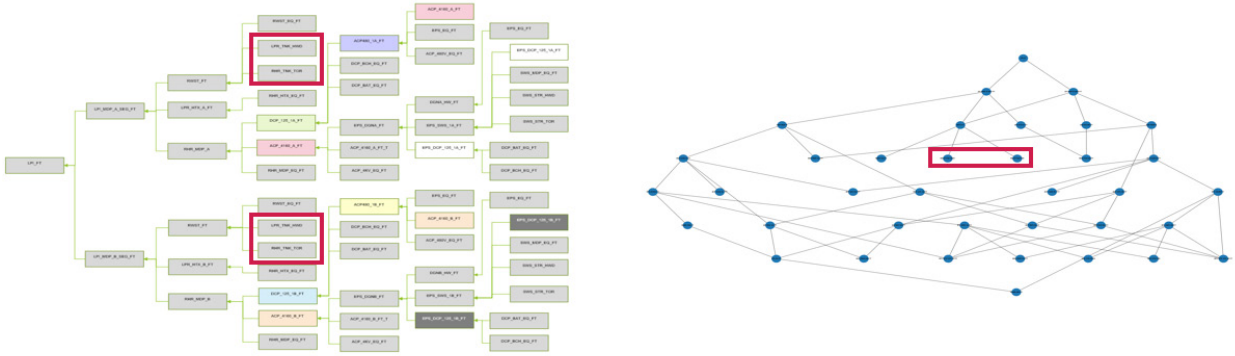


Figure 11. Difference between the manual and script fault-tree-to-fault-tree structures.

Since the Python script provided the same structure, the fault trees could now be grouped using the script. To group the fault trees, the Python script analyzes each fault tree to determine which other fault trees transfer to that fault tree. If the specific fault tree is called by only one other fault tree, then those fault trees can be grouped together. If the specific fault tree is called by multiple fault trees or no other fault tree, then the specific fault tree will be its own group. Again, once this grouping was initialized, it was compared to the manual grouping for the LPI system for the LLOCA IE. Figure 12 shows the manual grouping for the LPI system and Figure 13 shows the Python script grouping for the LPI system.

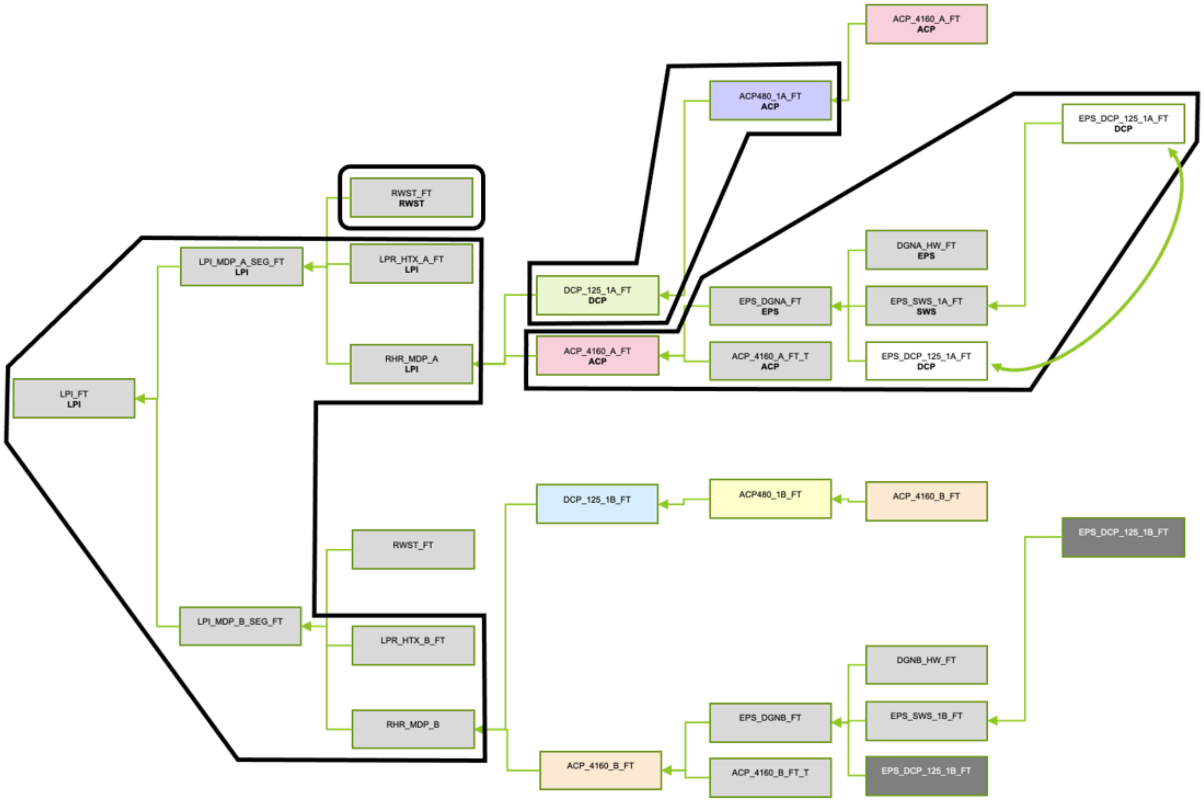


Figure 12. Manual grouping of the LPI system.

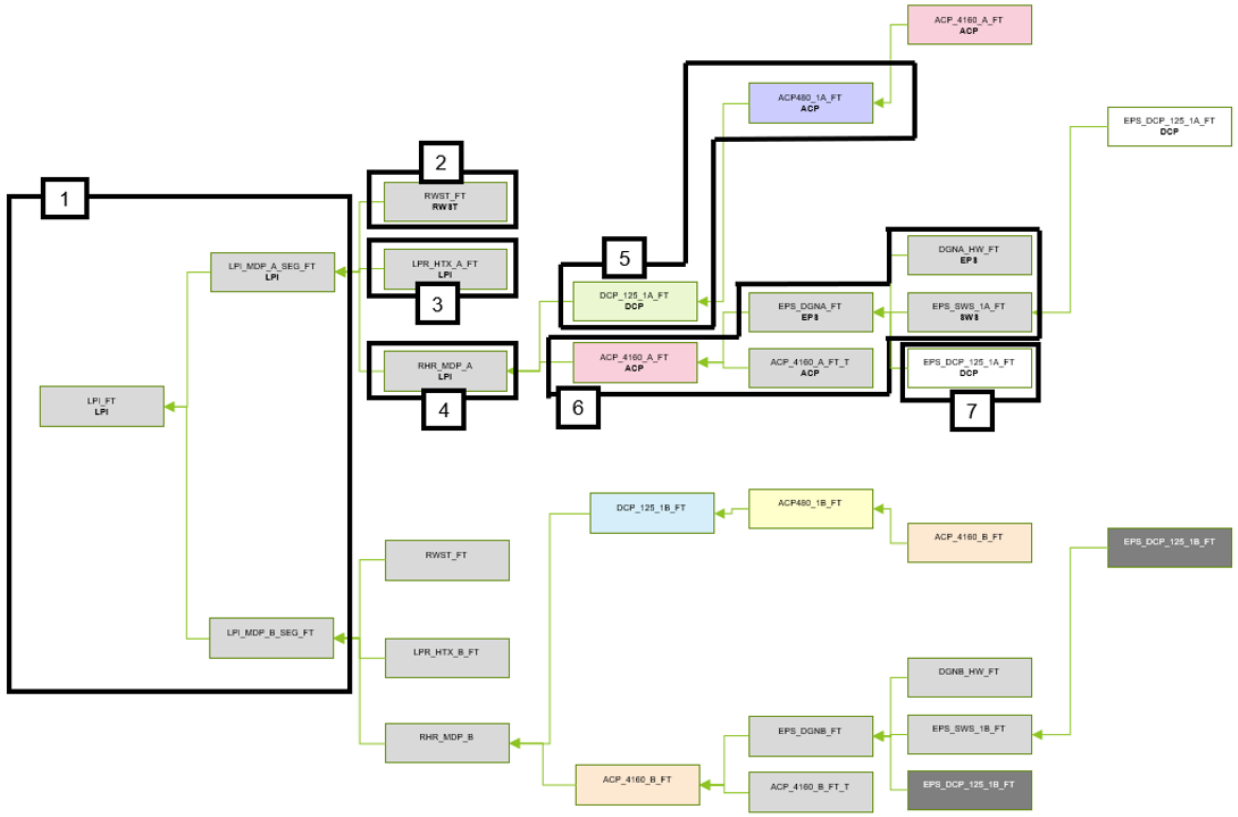


Figure 13. Python script grouping of the LPI system.

The Python script grouping did provide a slightly different result compared to the manual grouping. The script grouping provided more groups than the manual grouping. After reviewing the groups, the script did provide the correct grouping since a couple of the fault trees in the manual grouping were actually called in other systems in the LLOCA IE. This verifies that the Python script grouping does make the grouping determination appropriately.

After the Python script grouping was verified, it was applied to all IEs not just the LLOCA IE. This was not previously done by manual grouping due to the complexity. For the entire generic PWR PRA model, there were 239 fault trees. The initial grouping of the fault trees resulted in 178 groups which is a 25% reduction. Figure 14 shows the groups with the number of fault trees in each group.

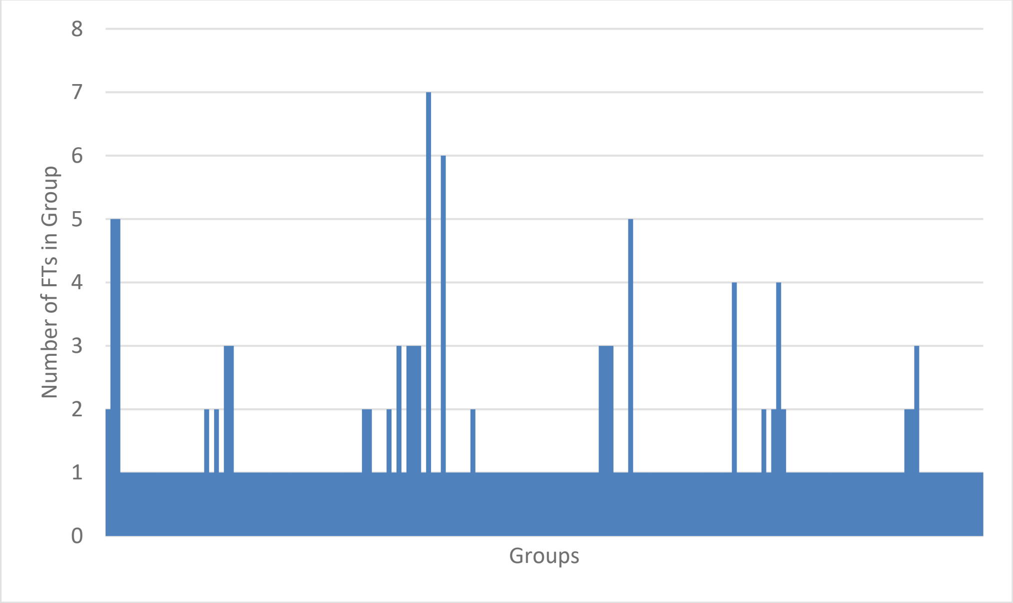


Figure 14. Python script number of fault trees in each group.

Based on Figure 14, most groups still contain only one fault tree, but there are some groups with up to seven fault trees included. However, the initial grouping does not reduce the number of fault trees to a solvable value.

To reduce the problem even further, the Python script allows the user to specify systems that are not applicable to RIM strategies. For example, external events are not applicable to RIM strategies so the user can specify to exclude seismic fault trees. For the generic PWR PRA model, excluded fault trees included external event fault trees (seismic, tornado, high winds, etc.), electrical fault trees (AC power, DC power, emergency power, etc.), and operator fault trees. After excluding those fault trees, the number of groups was reduced to 83. This is over a 50% reduction from the initial grouping. However, the problem is still too large to solve, and further reduction was needed.

The last reduction method included in this revision of the Python script was the removal of multiple trains. If there are multiple trains of a system and the fault tree grouping has the same structure, then only one of the trains needs to be evaluated and the other trains can be removed from the problem. The Python script sorts through the groups to determine whether there are multiple trains. There are several assumptions associated with the code which are: (1) the code assumes trains will have the same starting system characters, (2) the code assumes that trains are denoted by A, B, C, or D, and (3) the code assumes the user will specify fault trees that follow these two assumptions but are not multiple trains in the input file. The reduction of multiple trains reduced the number of groups to 72, which is another 13% reduction.

Currently, the Python script grouping methodology has provided about a 70% reduction from the original number of fault trees. More work needs to be done to reduce the number of groups even further to facilitate the optimization process. Some potential reduction methods include determining similar structures between groups that are not multiple trains and determine fault tree locations in regard to the event tree top events and optimizing those groups where the fault tree is closer to the top event.

Once the problem can be reduced to a solvable value, the BEs in each group will need to be analyzed to determine that the BE is in only one group. This is required so that the BE is only optimized once and not multiple times in different groups, which would result in different values. The next step will be for the Python script to rewrite the SAPHIRE text files using the new groupings. Once the text files are prepared, they can be read into SAPHIRE to obtain the MCSs needed for the optimization.

This project did not try to automate fault tree and BE groupings for PRA models developed in Computer Assisted Fault Tree Analysis (CAFTA). However, the code can be adjusted to read the text files representing CAFTA fault trees and the rest of the process will remain the same.

2.3 Multi-Sequence Target Allocation Analysis

This analysis expands the previous analysis as it is designed to handle multiple sequences in the frequency-consequence (F-C) curve rather than one as shown in [5]. Again, the following PRA model steps were followed:

1. Consider three separate sequences (rather than one as indicated in [5]) to be considered in the F-C curve; then, the full set of MCSs generated for the LLOCA IE are divided into three groups, one group for each sequence
2. Partition the set of fault trees (FTs) into groups and solve separately (i.e., the set of MCSs for each group has been generated)
3. Obtain the Pareto frontier point for each of the FT groups identified in Step 2; in this respect, Table 2 provides the number of Pareto frontier points for each of the 10 groups identified in Step 2 while Figure 15 shows the set of options (blue points) and Pareto frontier options (red points) for the ACP4160 and LPI systems
4. Construct a RIM model which receives a specific Pareto frontier point as input for each of the ten considered groups of FTs (see Table 2) and provides in output the corresponding values of O&M cost and the frequency values for the three sequences identified in Step 1
5. Perform single-objective optimization using the model presented in Step 4; note that throughout the optimization process, the decision space is 10-dimensional (see Table 2) and the model output variable to be minimized is the O&M costs while the frequency values for the three sequences identified in Step 1 are considered as constraints to be satisfied.

The sequence of steps presented above were performed using two codes:

- SAPHIRE: to construct the MCSs for each of the three sequences and for each group of FTs as described in Steps 1 and 2, respectively
- RAVEN: to construct the RIM model described in Step 4 using the EnsembleModel capability and to perform the optimization analyses described in Steps 3 and 5.

Table 2. List of Pareto frontier points for the system identified in the LLOCA PRA model.

System ID	# of Pareto frontier points
ACC	5
ACP-480	8
ACP-4160	23
CCW	17
DCP-125	5
EPS-SWS	9
LPI	13
LPR	6
RWST	4
SWS-TRNA	6

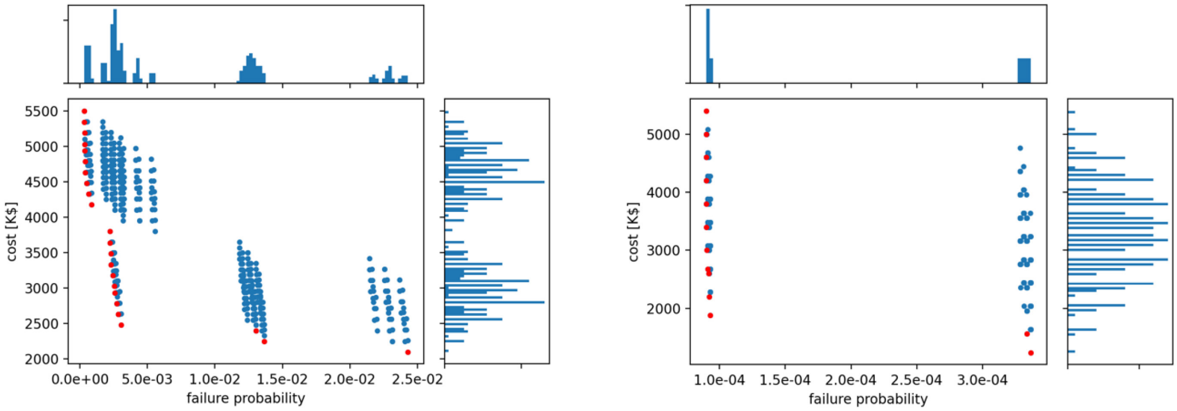


Figure 15. Complete set of options (blue points) and Pareto frontier options (red points) for the ACP4160 (left) and LPI (right) systems.

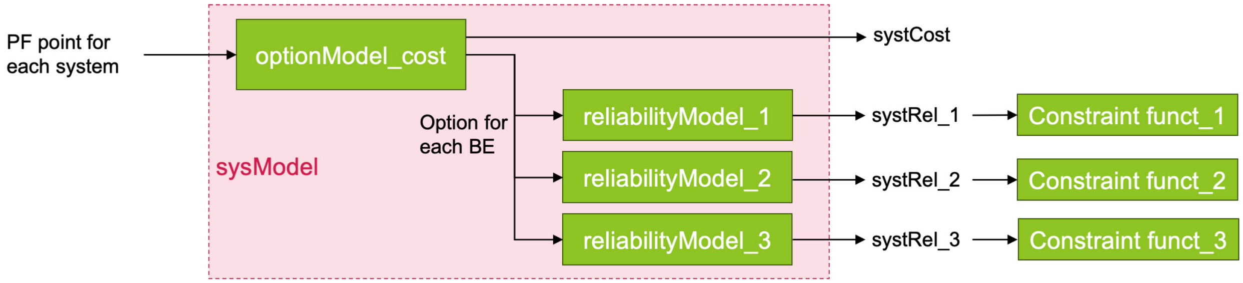


Figure 16. Graphical representation of the PWR LLOCA model employed to optimize the RIM strategy.

Given the discrete structure of the decision space, Step 5 can be performed using an evolutionary-based optimization method which relies on a classical genetic algorithm (GA). The outcome of such an analysis is a specific Pareto frontier for each group of FTs (see Table 2) and, consequently, a specific reliability target for each of the 92 SSCs (see Section 2.1.3). The graphical representation of the PWR LLOCA model is presented in Figure 16.

For this specific analysis, the models shown in Figure 16 were coupled with the GA optimizer class available in RAVEN where the basic chromosome structure consisted of a 10 dimensional array (one for each group of FTs indicated in Table 2). An initial population of 60 chromosomes was chosen by randomly sampling the discrete value of each element of the 10 dimensional array (e.g., an integer value between 1 and 5 was sampled for the element corresponding to the ACC system of Table 2). By performing a series of crossover, mutation, and selection operations on the initial population of chromosomes it was possible to obtain the optimal chromosome which minimizes plant costs and satisfy the three defined constrains (see Figure 16). Such chromosome is indicated in Table 3 where, for each, group of FTs, it indicates a specific Pareto frontier point.

Table 3. Optimal RIM strategy for the considered test case obtained by GA algorithm.

System ID	Optimal Pareto frontier point
ACC	5
ACP-480	8
ACP-4160	15
CCW	17
DCP-125	5
EPS-SWS	9

LPI	3
LPR	6
RWST	4
SWS-TRNA	6

2.4 Identified Difficulties, Gaps, and Needs for Additional Research

Allocating reliability targets proved to be a very complex task due to its multifaceted nature and broad scope. Specific areas of difficulty were identified in [5] and are discussed below for completeness.

2.4.1 Identified Difficulties

The previous research identified difficulties listed below and research this year focused on addressing them.

Passive-only components consideration for the RIM program. ASME Section XI, Division 2 is developed for passive-only components. However, this brings some concerns since the starting point of reliability target allocation is the plant-level: "The RIM program shall identify plant-level risk and reliability targets for RIM. Plant-level reliability shall be derived from regulatory limits on the risks, frequencies, and radiological consequences of licensing basis events that are defined in the probabilistic risk assessment (PRA) [1]." The plant-level reliability targets are addressed per accident sequence to satisfy requirements of NEI 18-04 guidance, and they are determined with consideration of both active and passive components unless a given mitigating system is purely passive. Allocation of reliability targets to only passive components may prove to be problematic because the overall system reliability is not addressed. Also, since the reliability of active components is not specifically considered, the cumulative effect of decreased reliability in both active and passive components is not addressed.

In this report, we describe the research that includes reliability and capability target allocation for both active and passive components simultaneously. The allocated targets may later be described in two separate programs, e.g., RIM program for passive components and a program resembling an LWR maintenance rule program for active components. However, we propose that RIM could be a single program that encompasses reliability / capability targets and later performance monitoring for all plant SSCs, regardless of active or passive functionality.

The problem is too large to solve. As discussed in previous chapters, the problem of allocating reliability targets to all plant SSCs at once is too large to solve even with modern computational power. As such, the task must be subdivided to subtasks which brings associated concerns such as:

- Population size of SSCs that would be considered all at once for reliability target allocation
- Selection of SSC groups could be based on a number of factors including importance measures, physical component type (e.g., pipe, valve), system that components belong to, component material, etc.

In this report, we described an approach that allows to reduce the size of the problem by splitting optimization process into two steps – components within a system (i.e., group), and then optimization of groups. We also developed an approach to automatically group components represented by BEs into groups generally reflecting systems and mitigating functions, including the process of reduction of problem size by removing some of the PRA BEs from considerations (e.g., external hazard BEs, opposite train BEs).

Interdependence of SSCs. Very few SSCs at a NPP are entirely independent. Most commonly, each SSC is dependent on other SSCs to various extents. This interdependency significantly complicates the optimization process of reliability target allocation.

We have proposed an approach of separating SSCs into groups which allows independence needed for optimization process.

SSCs supporting multiple event sequences. It is common that a system provides mitigation for multiple accidents. Some event sequences may be similar such as various sizes of loss of coolant accidents (LOCAs) at LWRs. However, some mitigating systems and their SSCs may provide support that is unrelated to other accidents. For example, an AC power system provides mitigation for most of the accident sequences at LWRs. Given that an SSC may support mitigation for multiple events, the difficulty is with the selection of an appropriate reliability target that would satisfy all the sequences. The most logical and simple way is to select the most limiting reliability target (i.e., lowest failure probability). However, this solution limits future plant operations flexibility since the SSC's performance will have to satisfy the prescribed reliability target. Another solution that can be considered is having multiple reliability targets, but this creates difficulties with associated performance monitoring strategies.

In this year report, we have expanded the research from a single IE to multiple IEs being considered in the reliability target allocation process.

Circular dependence between SSC failure rate and importance measures. The PRA importance measures (e.g., Fussell-Vesely and Birnbaum) are typical metrics used to identify how important a given component is to the overall undesirable consequence. However, the probability of the undesirable consequence is directly dependent on each contributing component reliability, and a change in a component failure rate affects both the probability of the top event and importance measures of all the contributing events. As such, the use of importance measures to assign reliability targets creates a circular dependency that impedes optimization techniques.

The research conducted in this project has explored options for reliability target allocation that relies on importance measures. The process based on importance measures was determined to be not feasible for automated optimization of reliability target allocation and we have proposed an alternative approach.

2.4.2 Identified Data Gaps

Plant and SSC-level reliability targets are directly related to the state of knowledge and data available for quantification of SSC probabilities of failure. For LWR SSCs, multi-year operational and testing data are available, and techniques for data quantification are well-established. This is not the situation with ARs where operational data are either limited or not available at all. Testing data may be available, but usually they are insufficient for deriving failure data with narrow uncertainty ranges. As such, data limitation could complicate RIM program development.

This limitation also affects licensing processes that follow RG 1.233 guidance because scarce data typically result in a wider range of uncertainties. It is important per NEI 18-04, "the upper bound consequences for each DBA, defined as the 95th percentile of the uncertainty distribution, shall meet the 10 CFR 50.34 dose limit at the exclusion area boundary." The uncertainties also affect DID strategies since, "One of the primary motivations of employing DID attributes is to address uncertainties, including those that are reflected in the PRA estimates of frequencies and consequence" [2].

As such, data collection and establishment of proper data processing and quantification methods are vitally important for successful licensing of ARs following RG 1.233 and for development of the RIM program. Given the limited OE, data supporting PRA model may be based on other industry data for similar components, materials, and/or operating conditions with uncertainty parameters specified to cover this extrapolated data. When OE becomes available, PRA data should be adjusted to reflect as-built, as-operated conditions using approaches currently employed by operating reactors for data updates (e.g., Bayesian update).

This research investigated the opportunity for dealing with data limitation through the emphasized reliance on monitoring strategies where large uncertainties may exist in reliability values of a given SSC. In this case, various monitoring strategies can be explored and the ones with highest probability of degradation detection may be preferred to overcome the limitation associated with the reliability value.

2.4.3 Substantial Complexity of RIM Program Management

The initial research of the RIM program highlighted the substantial complexity of the program and its activities requiring significant knowledge and efforts to properly manage RIM program development and later its maintenance. The program is complex because it has multiple elements that are cross-connected, it relies on a large set of data, and it requires integration of multiple disciplines. In FY-23, we proposed an approach that manages complexity of the RIM program effectively and efficiently. The approach is based on systems engineering principles and employs an MBSE solution as discussed in Section 3.

3. MODEL-BASED SYSTEMS ENGINEERING TO SUPPORT RIM PROGRAM DEVELOPMENT

Systems engineering is an interdisciplinary and holistic approach to the development of solutions for complex problems. Systems engineering integrates both business and technical needs with the goal of providing the optimal solution from the perspective of the entire system rather than optimizing individual parts of the system. The systems engineering discipline is relatively young. It emerged a few decades ago as an effective way to manage complexity. The need for a systemic, holistic approach to develop solutions for complex systems is now higher than ever due to the constantly increasing complexity of the world around us. The RIM program is a perfect example of a complex problem–it necessitates close interactions of multiple technical disciplines (e.g., materials, mechanical, electrical, nuclear, reliability engineering, along with non-technical considerations such as business goals and the licensing process). The RIM program is developed through a multistep process requiring iterations between steps until the final product (i.e., strategies for managing reliability and integrity) is developed. Last, the RIM program is connected to the entire lifecycle of a NPP, from the plant design decisions to plant operations and later plant decommissioning. As such, systems engineering is the well-suited approach to guide the development of the RIM program.

Given the continuous increase in systems complexity, more rigorous and robust systems engineering practices are needed. In response to this need, the practice of systems engineering is undergoing a major transition from a document-centered approach to a model-based approach, called Model-Based Systems Engineering (MBSE). MBSE, supported by advanced computer technologies, offers substantial benefits compared to producing and controlling a large set of documents, see Figure 17.

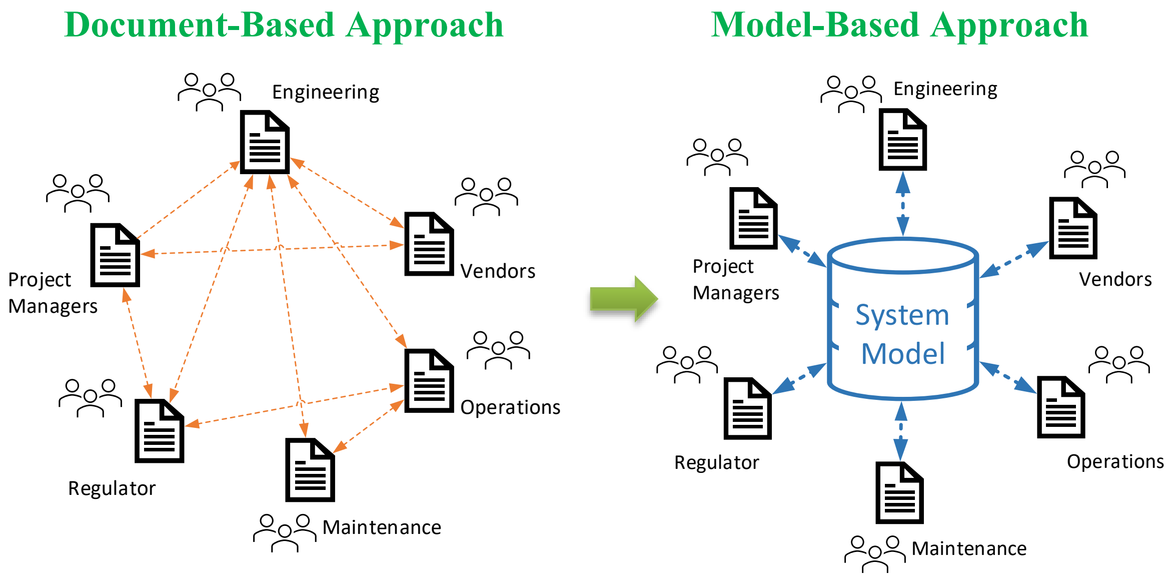


Figure 17. Document-based vs. Model-Based Systems Engineering.

MBSE helps to manage complexity by applying a comprehensive, robust approach and using advanced computer technologies. It enables better communication between numerous system stakeholders and dramatically improves knowledge retention and transfer.

3.1 Background – What is Model-Based Systems Engineering?

The International Council on Systems Engineering defines MBSE as "the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the [concept stage] and continuing throughout development and later life cycle [stages] [6]." In a typical document-based design approach, information is contained in system description documents, specifications, interface control documents, and design analysis reports. It is difficult to synchronize, access, and maintain this information as well as assess its correctness, completeness, and consistency. A model-based approach has become essential to capture, analyze, share, and manage the complexity of information. A model is a graphical, mathematical, or physical representation of a concept, structure, or system to facilitate understanding. The original concept of MBSE was the idea of transforming from a document-based approach to a "model-based" approach, where the documentation was generated from the models. As applied in this work, initial models have been created from regulatory / guidance documents. A model of the RIM process was created utilizing the guidance within ASME standard [1] and a generalized model of the reactor cavity cooling system (RCCS) was created from existing design information. It should be noted that the ASME standard is focused on passive-only components while the MBSE model in this project replicated the same RIM process but without differentiation between passive and active components. In fact, steps in the RIM process were not altered at all (i.e., process RIM-2.2 through RIM-2.8). This helped to demonstrate that RIM program could be successfully applied to all the components regardless of functionality.

The elements of the RIM process and of the RCCS are captured in the model along with the relationships between the elements. The model serves as the repository of the information. All the documents required to support any part of the RIM process per RG 1.246 supporting demonstration of performance monitoring required as part of the licensing process per RG 1.233 can be generated directly from the model reflective of the most up-to-date information.

3.2 MBSE for RIM Program Development

The objective of using MBSE for this project was to (a) develop a model of the RIM process as established in Section XI, Division 2 and (b) to implement the RIM process using a generalized version of a RCCS system modeled in the MBSE tool. Accomplishing these objectives provides the ability to (a) evaluate the correctness, completeness, and consistency of the Section XI, Division 2, RIM process and

(b) to demonstrate the benefits of applying MBSE to a typical AR design. The MBSE tool Innoslate by Spec Innovations [7] was utilized for development of the RIM process and system models.

The two models (RIM process and System Architecture) demonstrate the interconnectivity of requirements and design for use with a RIM Program. This interconnectivity provides the capability to link component designs and their potential degradation mechanisms with monitoring and non-destructive examination (MANDE) to mitigate degradation effects. The sum of the MANDE corresponds to the RIM strategy for the component. The sum of the RIM component strategies provides the RIM strategy for the system they comprise.

3.2.1 RIM Process Model

The MBSE tool was used to establish a model of Section XI, Division 2, RIM process. The top-level RIM process model is shown in Figure 18. The model captures steps in the RIM process as activities and links the activities together by their inputs and outputs. Activities are depicted in white boxes and inputs/outputs are depicted by green parallelograms. Some of the activity boxes have a blue bar stating, "Decomposed." This indicates that the activity has been further detailed by sub-activities. Activity numbers (e.g., RIM-2.2) correspond to the article and sub-article numbering in the ASME standard. Activity descriptions entered into the MBSE tool are verbatim extracts from the corresponding article/sub-article of the ASME standard.

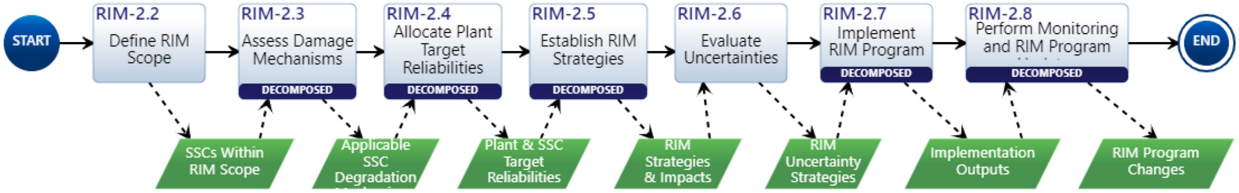


Figure 18. RIM process in Innoslate.

A report generated from the MBSE tool is included as Appendix A, RIM MBSE Process Model. This report provides a model of the RIM process that is more detailed than the flowcharts provided in Mandatory Appendix 1 of the ASME standard. Activity diagrams clearly depict the serial or parallel relationships between activities. The diagrams also show what information (input/output) is exchanged between activities. The ability to visualize the relationships and input/output(s) between activities provides enhanced understanding of the RIM process.

The objective of developing the RIM process model was to evaluate the correctness, completeness, and consistency of the process established in Section XI, Division 2. In applying MBSE, the ASME standard was deconstructed, and its elements modeled in the tool. This provided the ability to identify and examine the RIM process to better understand the interrelationships and identify any areas within the standard where improvements are needed. Despite the complexity and difficulties associated with RIM development and implementation, the RIM process itself was found to be implementable and, in general, correct, complete, and consistent. As with any new standard, there are areas where improvements are needed.

3.2.2 Reactor Cavity Cooling System Model

Component information needed for the input to the RIM process was developed and populated utilizing a generalized version of a RCCS design (i.e., this design does not correspond to any exact design of a real system but is a reasonable replica of an actual design). The main focuses of the MBSE effort were a concept of operations (ConOps) diagram, a functional requirements document, placeholder performance requirements, reliability requirements, and a system design diagram that satisfies these requirements.

The RCCS is a closed-loop water cooling system that provides cooling for the reactor cavity via embedded standpipes. The system is designed to provide a single failure mitigation and to function during and after seismic events. The system receives heat from the reactor cavity and rejects it to a secondary cooling system via a heat exchanger. The RCCS operation is primarily in forced flow mode but includes a natural convection cooling mode with system make-up in the event of a loss of power to the coolant pumps as well as a maintenance mode for inspection, testing, and service of components.

Development of the system model was performed by utilizing existing RCCS designs and the above system description to develop a generalized ConOps and define its associated functional requirements. Each action within the ConOps is linked to associated functional requirements. The development of functional requirements provided the basis for the development of the system model and components. Performance requirement placeholder values were developed for each of the functional requirements to provide criteria for which component performance can be measured. The highest level of the system ConOps diagram is presented in Figure 19.

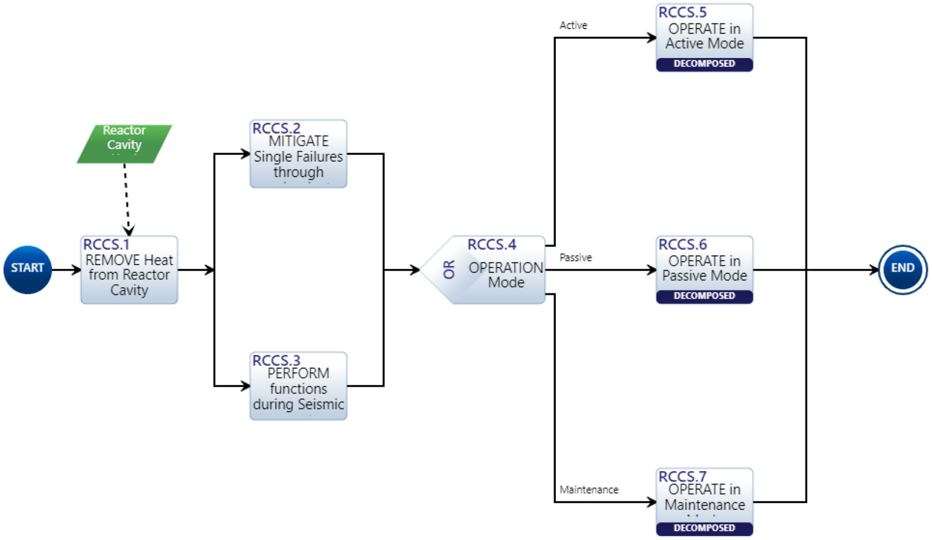


Figure 19. RCCS concept of operations (ConOps).

The RCCS system model presented in Figure 20 was developed to satisfy the desired operational concept and the functional requirements. All components included in the model exist to satisfy a system functional requirement and action in the ConOps. The RCCS was designed with two independent trains to meet the single failure criteria requirement. Only Train A was modeled for this effort.

Information required to perform steps in the RIM process was included in the attributes for each component within the system model. Component characteristics, operating conditions, PRA BEs, applicable requirements (functional, performance, and reliability), and identified degradation mechanisms were information included for components.

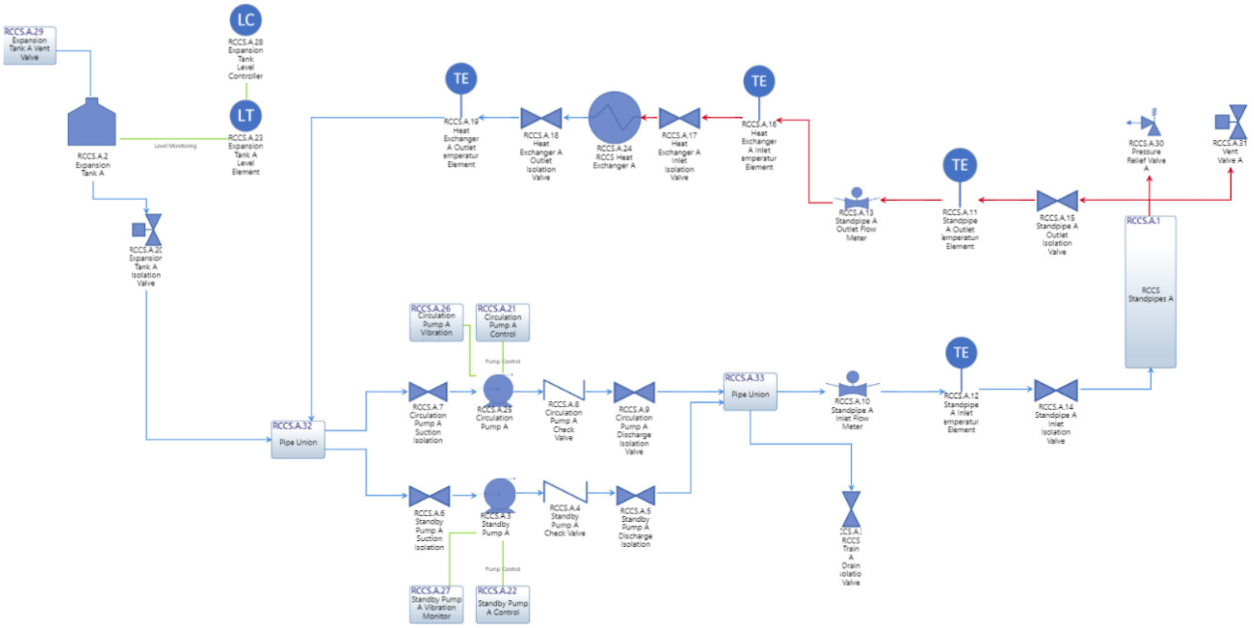

RCCS.A.29 Expansion Tank A Vent Valve
LC
RCCS.A.28 Expansion Tank Level Controller
LT
RCCS.A.23 Expansion Tank A Level Element
Level Monitoring
RCCS.A.2 Expansion Tank A
RCCS.A.20 Expansion Tank A Isolation Valve
TE
RCCS.A.19 Heat Exchanger A Outlet emperatur Element
RCCS.A.18 Heat Exchanger A Outlet Isolation Valve
RCCS.A.24 RCCS Heat Exchanger A
RCCS.A.17 Heat Exchanger A Inlet Isolation Valve
TE
RCCS.A.16 Heat Exchanger A Inlet emperatur Element
RCCS.A.13 Standpipe A Outlet Flow Meter
TE
RCCS.A.11 Standpipe A Outlet Temperatun Element
RCCS.A.15 Standpipe A Outlet Isolation Valve
RCCS.A.30 Pressure Relief Valve A
RCCS.A.31 Vent Valve A
RCCS.A.1
RCCS Standpipes A
RCCS.A.26 Circulation Pump A Vibration
RCCS.A.21 Circulation Pump A Control
Pump Control
RCCS.A.32
Pipe Union
RCCS.A.7 Circulation Pump A Suction Isolation
RCCS.A.25 Circulation Pump A
RCCS.A.8 Circulation Pump A Check Valve
RCCS.A.9 Circulation Pump A Discharge Isolation Valve
RCCS.A.33
Pipe Union
RCCS.A.10 Standpipe A Inlet Flow Meter
TE
RCCS.A.12 Standpipe A Inlet emperatur Element
RCCS.A.14 Standpipe A Inlet Isolation Valve
RCCS.A.6 Standby Pump A Suction Isolation
RCCS.A.3 Standby Pump A
RCCS.A.4 Standby Pump A Check Valve
RCCS.A.5 Standby Pump A Discharge Isolation
CCS.A.I RCCS Train A Drain solatio Valve
Pump Control
RCCS.A.27 Standby Pump A Vibration Monitor
RCCS.A.22 Standby Pump A Control

Figure 20. RCCS model.

The system model represented the culmination of RIM process step RIM-2.2. The scope of the components within RIM for the system and the supporting information utilized for the RIM process were included. Associated reliability requirements were created and developed for the components. All information, from actions to requirements and degradation mechanisms, are linked through relationships in the model so that they can be traced from components. Figure 21 (below) shows the relationships between requirements, actions, and assets for a selected component (RCCS.A.7 Circulation Pump A Suction Isolation Valve).

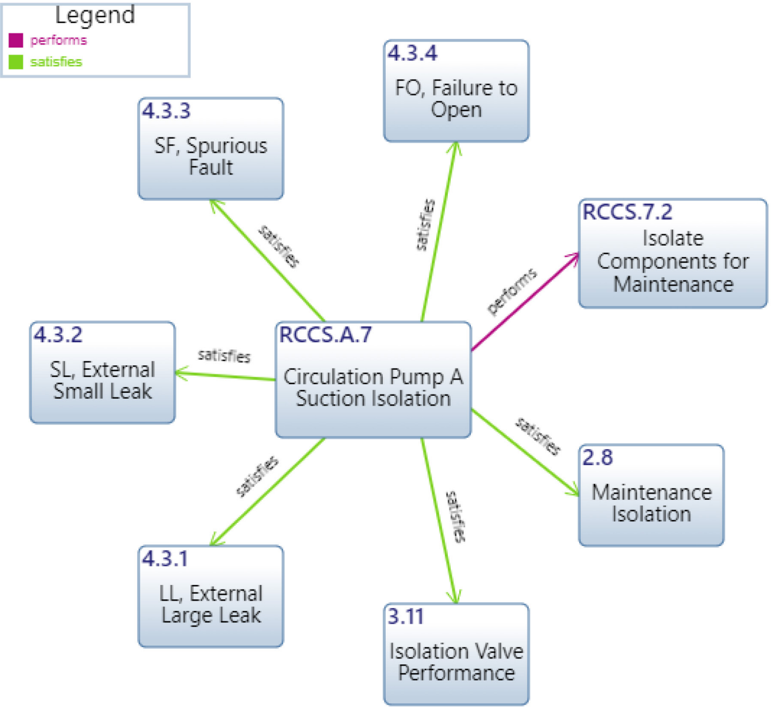


Figure 21. Requirement and action tracing to assets example.

3.2.3 RIM Process Implementation Using Model-Based Systems Engineering

A demonstration evaluation to assign degradation mechanisms, an analysis of potential failure mechanisms, and an assignment of MANDE categories to a selection of equipment was performed. These processes were implemented through the Innoslate tool and integrated into the system model through entity relationships. The various mechanisms and exams were represented by custom classes of entities in the database. The relationships assigned to these custom classes reference the assets (components) and conduits (piping, power cabling, etc.) that comprise the system model. Degradation mechanisms are caused by the operating environments of assets and conduits.

Additional failure mechanisms[a] were created for active portions of assets such as valves to provide input for Preventive Maintenance (PM) strategies. MANDE categories mitigate these mechanisms experienced by each asset or conduit through examinations or PMs. ASME Division 2 addresses passive pressure boundary components and degradation mechanisms. Active component failures and mitigation strategies were included in the system model to develop an overall system integrity management strategy within a single tool. This approach demonstrated that a RIM type process can be applied to active components. Since the various mechanisms affect the diverse types of assets and conduits differently, the relationship is formed between MANDE and assets/conduits rather than directly to degradation mechanisms or failure mechanisms. The relationships between these classes and the assets were designed to allow for a full tracking and tracing of the component information. Figure 22 represents these relationships.

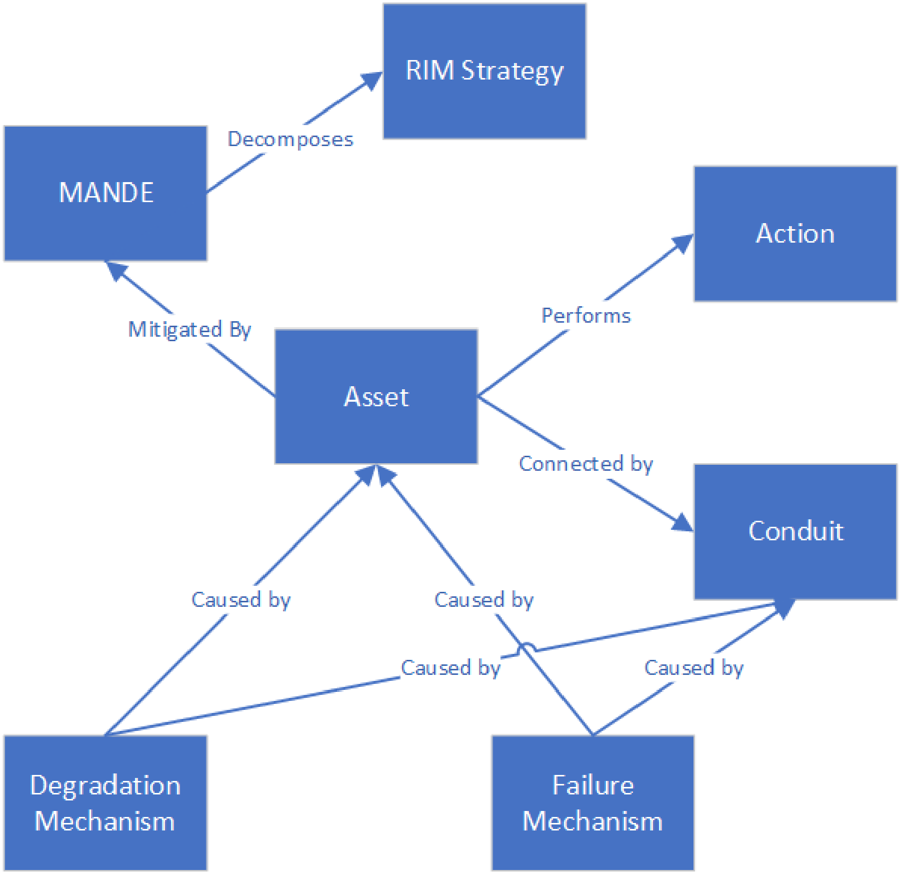


Figure 22. Custom class relationships.

[a] Investigation of failure mechanisms for active components is outside of the scope of this research, reactor developer would have active failure mechanisms identified and investigated either as part of the RIM program development or as a separate activity.

The evaluation focused on four components: RCCS.A.7 Circulation Pump A Suction Isolation Valve, RCCS.A.25 Circulation Pump A, RCCS.A.8 Circulation Pump A Check Valve, RCCS.A.9 Circulation Pump A Discharge Isolation Valve, and their interconnected piping. These pipe segments and components were arbitrarily selected for the evaluation to include both active and passive components of different types. Demonstration components are shown in Figure 23.

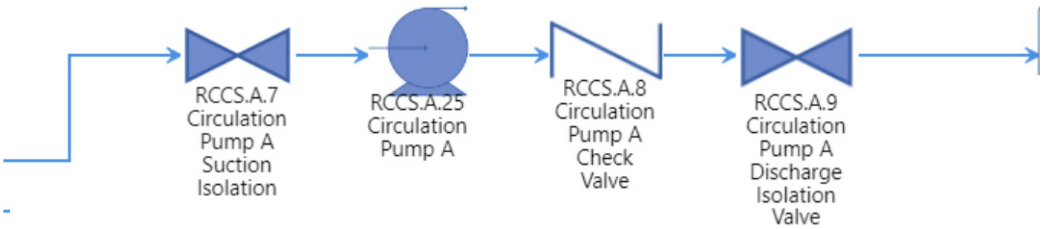

RCCS.A.7
Circulation Pump A Suction Isolation
RCCS.A.25
Circulation Pump A
RCCS.A.8
Circulation Pump A Check Valve
RCCS.A.9
Circulation Pump A Discharge Isolation Valve

Figure 23. Demonstration components.

Each of the demonstration pipe segments underwent a Degradation Mechanism Assessment as shown in RIM Step 2.3. The assessment results were loaded into the Innoslate model utilizing the previously mentioned relationship types. Similarly, based upon the assigned degradation mechanisms and the component information, MANDE categories were assigned to each component. The figures below show the relationships between these degradation mechanisms and MANDE for the pipe segment (Figure 24) and the degradation mechanisms and MANDE for the Circulation Pump A Suction Isolation Valve (Figure 25).

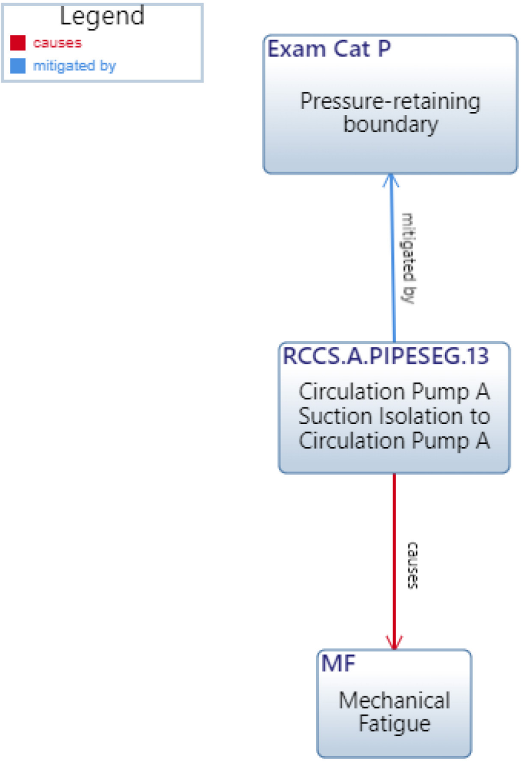


Figure 24. Degradation mechanism and MANDE relationships for conduits.

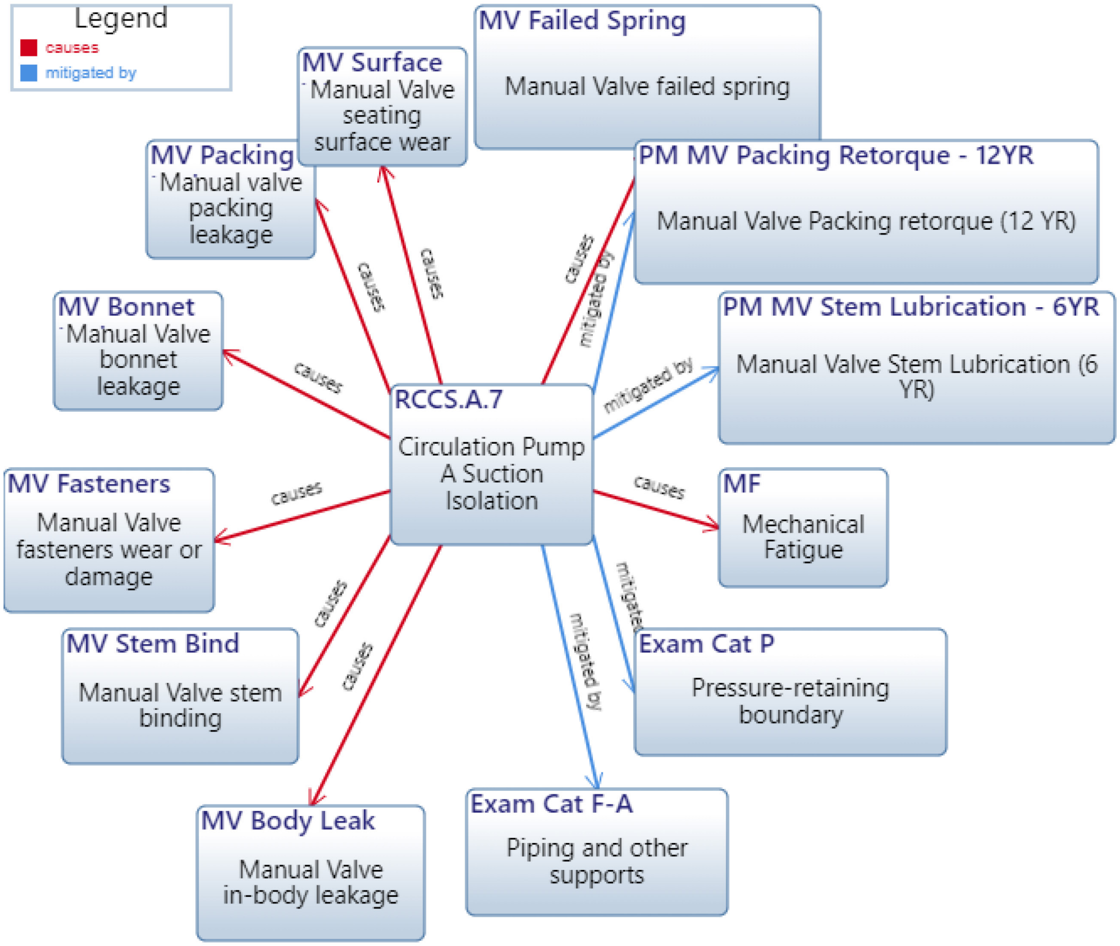

Legend
🟥 causes
🟦 mitigated by
MV Failed Spring
Manual Valve failed spring
MV Surface
Manual Valve seating surface wear
MV Packing
Manual valve packing leakage
PM MV Packing Retorque - 12YR
Manual Valve Packing retorque (12 YR)
MV Bonnet
Manual Valve bonnet leakage
PM MV Stem Lubrication - 6YR
Manual Valve Stem Lubrication (6 YR)
RCCS.A.7
Circulation Pump A Suction Isolation
MV Fasteners
Manual Valve fasteners wear or damage
MF
Mechanical Fatigue
MV Stem Bind
Manual Valve stem binding
Exam Cat P
Pressure-retaining boundary
MV Body Leak
Manual Valve in-body leakage
Exam Cat F-A
Piping and other supports
causes
mitigated by
mitigated

Figure 25. Degradation mechanisms, failure mechanisms, and MANDE relationships for assets.

Various MANDE items that were selected to mitigate the failure and degradation mechanisms were then collected into RIM strategies associated with a specific pipe or component. The strategies were completed utilizing the Entity Definition feature combined with the spider diagrams pictured above in Innoslate. This allowed for the selection of failure mechanisms, degradation mechanisms, and ultimately MANDE items associated with a specific component to be represented in one report along with the visual representation. Since both the spider diagram and the entity report were pulled from the database, this meant that if a component was reevaluated and the associated MANDE updated, the information for that component would update within the tool. The RIM strategy would then simply need to be re-downloaded to be complete. A RIM strategy print-out for the pipe segment connecting Circulation Pump A Suction Isolation Valve to Circulation Pump A and the Circulation Pump A Suction Isolation Valve are located in Appendix B.

3.3 Risk Assessment Techniques for Reliability and Integrity Management Program

The objective of the RIM program is to define, evaluate, and implement strategies to ensure that reliability targets for SSCs are defined, achieved, and maintained throughout the plant lifetime. There are other widely used methods to evaluate risks and implement strategies to avoid and mitigate those risks. A comparative review of RIM to some of the commonly used risk evaluation processes was performed as an additional activity to evaluate the correctness, completeness, and consistency of the Section XI, Division 2, RIM process. Risk assessment processes that were used in the comparison are described in Table 4,.

Table 4. Risk Evaluation Methods for Comparison with RIM

Guidance Document / Method Name	Description	Reference
Guidelines for Hazard Evaluation Procedures / Failure Modes and Effects Analysis (FMEA)	Tabulates failure modes of equipment and their effects on a system or plant.	[8]
IEC 60812 / FMEA and Failure Modes, Effects, and Criticality Analysis (FMECA)	Explains how FMEA, including the FMECA variant, is planned, performed, documented, and maintained.	[9]
Mil STD 1629A / FMECA	Used to systematically evaluate and document by item failure mode analysis the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability, and maintenance requirements. Each potential failure is ranked by the severity of its effect so that appropriate corrective actions may be taken to eliminate or control the high risk items.	[10]
Army Regulation 702-19 / Reliability, Availability, and Maintainability (RAM)	Sets forth policies for planning and managing Army systems reliability, availability, and maintainability during development, procurement, deployment, and sustainment.	[11]
Different Methods for Assessing System Failure Criticality in the RAMI Approach / Reliability, Availability, Maintainability, and Inspectability (RAMI)	In the RAMI engineering approach used in nuclear fusion research; criticality identifies the failure modes that have the greatest impact on the availability of the studied system.	[12]
Plant Systems Design (PSD) Standard	Provides a technology independent framework, including requirements and guidance, for organizations to perform the following activities: a) Conduct plant process hazard and risk evaluations and analysis in the early phases of design that advance as the design matures and provide structure to the development of qualitative and quantitative risk assessment. b) Integrate existing systems engineering design processes, practices, and tools with traditional architect engineering design processes, practices, and tools. c) Integrate probabilistic design processes, practices, and tools with traditional deterministic design processes using reliability and availability targets.	Draft Plant Systems Design Standard, ASME

A comparison of these methods to RIM is included in Appendix C. The first column in the Appendix C table is titled “Common.” It provides a common name for activities that are similar in the different risk evaluation methods.

The following highlights areas of the comparison relative to the correctness, completeness, and consistency of the RIM process.

- RIM
  - RIM focus is on component reliability.
  - RIM main applicability is to operating plants (i.e., to monitor performance during plant operation). However, RIM program could also inform plant design to account for future operability.
  - RIM is focused on passive components.
  - RIM allocates plant safety requirements to SSCs and evaluates impacts of these on plant level risks using a PRA model.
  - RIM uses PRA and fault trees to evaluate the operation, interrelationships, and interdependencies of SSCs.
  - RIM also evaluates uncertainties.
- RIM vs. FMEA
  - FMEA focus is on identifying failure modes.
  - FMEA applicability is to new design and includes both active and passive components.
  - FMEA uses a matrix to identify failure modes, effects, and safeguards and identifies actions to reduce likelihood of the effects.
  - Traditional FMEA does not use target reliabilities, PRA models, or evaluate uncertainties.
- RIM vs. FMECA
  - FMECA focus extends FMEA by including a criticality analysis, to chart the probability of failure modes against the severity of their consequences.
  - FMECA applicability is to new design and includes active and passive components.
  - FMECA uses functional and reliability block diagrams to evaluate the operation, interrelationships, and interdependencies of SSCs.
- RIM vs. RAM
  - RAM focus is on operating plant reliability and maintainability.
  - RAM applicability is to operating plants and includes both active and passive components.
  - RAM includes FMECA as part of the process so comparisons for FMECA also apply to RAM.
  - RAM does not use uncertainty evaluations but does include confidence intervals for uncertainty in data.
  - RAM classifies each potential failure mode according to severity or risk probability number.
- RIM vs. RAMI
  - RAMI extends RAM by adding inspectability.
  - RAMI applicability is to new plant design and includes both active and passive components.
  - RAMI includes FMECA as part of the process so comparisons for FMECA also apply to RAMI.
  - RAMI evaluates availability against acceptance criteria. If criteria are not met, mitigation actions are considered and a new cycle of analyses is performed until an acceptable availability is achieved.
- RIM vs. PSD
  - PSD focus is on availability, which includes reliability.

- PSD applicability is to new plant designs and includes active and passive components.
- PSD uses functional and reliability block diagrams to evaluate the operation, interrelationships, and interdependencies of SSCs.
- PSD plant risk evaluations include hazard identification, event sequences identification, event likelihood and consequence evaluation, risk characterization, risk acceptability determination, identification of additional barriers to avoid or mitigate the risk, and determination of availability targets.
- Plant risk evaluations and availability determinations continue during preliminary and detail design where they are performed for system and component designs.

Correctness, Completeness, and Consistency of the RIM Process.

RIM is essentially correct, complete, and consistent within its limited scope and applicability. However, RIM is limited by its focus on reliability, its applicability to passive components of operating plants, and its dependence on PRA models. RIM would benefit by (a) referencing or incorporating methodologies of FMECA for identifying and evaluating the operation, interrelationships, and interdependencies of SSCs that are not included in PRA models and (b) broadening its focus to include availability.

4. RIM DECISIONS THROUGHOUT PLANT LIFECYCLE

As indicated in the ASME Boiler and Pressure Vessel Code (BPVC.XI.2-2019) [1], an SSC reliability target is defined as "*a performance goal established for the probability that an SSC will complete its specified function….*" As indicated so far, the process of assigning a reliability target to a generic SSC appears to be an exercise meant to be completed at the design phase (i.e., prior to plant operation). On the other hand, once the plant is operating and the considered SSC is an integral part of plant operations, information regarding SSC reliability becomes available. In more detail, Figure 26 represents the relation between an SSC form and its function-SSC form supports its function. When the SSC is operating, degradation and aging (e.g., caused by radiation or stress corrosion cracking) affect the SSC form which can subsequently induce a loss of SSC function (i.e., its failure). From a RIM point of view, if a failure event is observed, then the failure rate of the SSC can be updated through a Bayesian updating process. Consequently, such an updating process might affect the overall reliability target allocation results obtained using the methods described in Section 2. The relevant notion to be highlighted here again is that, when the plant is operating, there is a continuous comparison between an SSC reliability target and the observed SSC reliability (i.e., observed vs. target dichotomy).

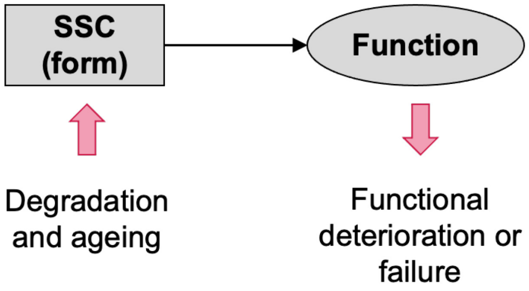


Figure 26. Graphical representation of the relations between degradation/aging and SSC deterioration/failure.

Another relevant element is that plant personnel might be performing quantitative assessments of the SSC health by focusing on its form and SSC performance by focusing on its function. Note that these assessments would not normally affect the SSC failure rate and, hence, the overall RIM analysis results. On the other hand, they would be employed to trend degradation or functional deterioration and act through appropriate maintenance operations designed to restore SSC health (i.e., its form) and avoid a failure event. As a consequence, these operations might impact the overall RIM analysis results since SSC reliability would notionally improve.

This allows us to show the reader that a plant RIM program's breadth of scope is expanded during the operational phase of the plant (see Figure 27). The historic and current reliability performance of an SSC would directly affect the SSC's reliability value (e.g., its failure rate) which is periodically compared to its corresponding reliability target. The analysis of trends about SSC functional performance, for example flowrate generated by a centrifugal pump, and health indications such asthickness of a pipe subject to corrosion, would inform system engineers on the optimal maintenance strategies designed to avoid SSC failure and restore SSC health and functional performance. Consequently, such strategies would improve SSC reliability performance.

From an operational point of view, maintenance operations would be performed once specific criteria or targets are met; such criteria/targets can be set by:

- SSC operational tech specs;
- Plant safety/PRA success criteria (e.g., minimum water flow rate generated by a centrifugal pump which is part of a safety cooling system);
- SSC historic operational conditions which might be available if a prognostic and health management system is available.

Note that it would not be required to assign a health, performance, and reliability target for all the SSCs that are part of the plant RIM program. Depending on the SSC operating context and the available data elements (indicated in Figure 27), the observed vs. target dichotomy mentioned above would apply in terms of reliability, health, or performance.

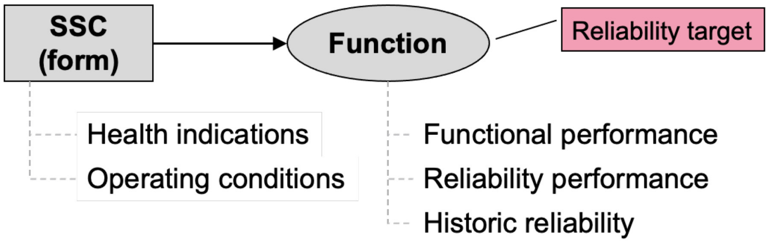


Figure 27. Typologies of RIM targets (highlighted in purple) during plant operation phases and their required reliability sources.

5. CONCLUSIONS AND RECOMMENDATIONS

The research conducted in this project supports advanced nuclear power reactor community with an initial technical framework that can support RIM program development and implementation. As part of the research, the team offers the following recommendations to the AR developers.

A Need for Holistic System Analyses

There is a significant push within nuclear industry to use lessons-learned and best practices from other industries to facilitate successful design, development, deployment, and operation of new nuclear reactors. The success of new NPPs is essential to many national goals, particularly to increasing energy resiliency and independence and to achieving climate goals. One of the best practices in other industries is the application of system thinking and system engineering principles and practices to finding optimal solutions that improve the system as a whole. This is a radically different approach compared to the vision that incremental improvements to individual parts of the system guarantee the best solution for the system overall. The Three Mile Island accident proved this vision incorrect, forcing nuclear industry to take a broader approach to assessing system successes and failures. The new reactors have the opportunity to do so, and the RIM program is where a holistic way of system analysis could be extremely beneficial.

The holistic approach to the RIM program development offers a tremendous opportunity to identify the most optimal system solutions that would increase safety and reduce costs, both in the manufacturing and construction stages and later in the operational stage. The plant construction costs may be reduced by considering alternative components and materials that offer only slight decreases in reliability with significant differences in price. Similar considerations should be applied to the selection of RIM strategies. Some of RIM strategies may involve installation of condition monitoring sensors or allowing personnel access for visual inspections. It is significantly more cost-effective to account for these strategies in the design stage instead of fitting them in after the plant is built.

Holistic systems assessments enable informed decision-making for the selection of optimized system solutions, and we highly encourage new reactor developers to take advantage of the "system-as-a-whole" principles practice.

Expand the Focus from Passive-Only SSCs to All SSCs

The RIM program, as written in the 2019 version of ASME Section XI, Div. 2 and endorsed in RG 1.246, is specifically focused on passive components. As a result, the reliability target allocation process described in the code is also focused on passive-only components. This leaves active components outside of the RIM program scope and forces separation of reliability targets allocation into passive and active components. However, as required by the guidance in Reg. Guide 1.233, reliability targets should be established and allocated simultaneously for all plant systems and components, regardless of active and passive functionality. The simultaneous process ensures that the plant-level reliability target is appropriately decomposed to the function- and system-level and then further to the component level. This holistic process also ensures that plant-level reliability targets are properly informed by the expected SSC performance.

The research conducted in this project demonstrated feasibility of using the RIM process for all system components, both active and passive, as described in Section 3.

Reliability Target Values

Reactor developers should be extremely cautious about setting reliability targets that are overly optimistic because these targets will dictate potentially unrealistic expectations for the plant systems and components performance and result in an increase of operational costs. For example, it would be overly optimistic to have a reliability target equal to the best estimate reliability value used in the PRA model since probabilities in the PRA model are expected to change to reflect OE.

The optimized approach for reliability target allocation described in Section 2 allows reactor developers to assign targets that are as conservative as possible without exceeding limits set forth by regulations or by reactor developers. The intentionally conservative reliability targets are intended to support licensing application where both reactor developers and regulator understand that expected (i.e., best estimate) SSC probability of failure will remain much lower than the probability of failure reflected in the reliability targets. These intentionally conservative reliability targets submitted as part of licensing application offer maximum margin between the target and actual performance allowing flexibility in meeting the targets during plant operation with actual performance and associated reliability values fluctuating given the OE.

Reliability Target Allocation Process

The reliability target allocation process should follow an approach that is:

- Aligned with methodology and guidance provided in both RG 1.233 and RG 1.246
- Based on proven and sound technical theories that are repeatable and demonstratable
- Technology-inclusive (i.e., any reactor design should be able to follow developed methods)
- Capable of addressing uncertainty considerations

- Simple and clear to minimize industry efforts and reliance on subject-matter experts.

The research conducted in this project and described in Section 2 offers an approach that satisfies all the points above.

PRA Model Development

The process of separating the PRA model into independent fault trees could be significantly simplified or even avoided by an intentionally-developed PRA model where fault trees for the plant main systems (e.g., heat removal from the reactor) and for supporting systems (e.g., electrical power, cooling water) are independent. However, Section 2.2 describes the process to deal with interdependence in the PRA model.

Model-Based Systems Engineering Approach for RIM Program

As highlighted in this report, the RIM program is a very complex problem. RIM development necessitates close interactions of multiple technical disciplines, and it is a multistep process requiring iterations between multiple steps. RIM is also connected to the entire lifecycle of a NPP. As such, a robust, comprehensive approach, such as MBSE (see Section 3), is highly recommended to support RIM program development, implementation, and future use during plant operation. MBSE helps to manage complexity, enables better communication between numerous stakeholders, and dramatically improves knowledge retention and transfer.

Extend RIM Throughout Plant Life

As highlighted in Section 4, a RIM program is a “living entity” that is updated when new SSC reliability data become available. In addition, given that SSC reliability data cover only a portion of what can be observed (e.g., SSC monitored indications of its health or functional performance), an SSC reliability target alone may not be adequate to support decision-making in an operational context such as planning for SSC maintenance activity. Therefore, many SSCs require the establishment of observable and measurable health and performance targets, e.g., a flowrate for a pump or corrosion rate and wall thickness for a pipe. The performance targets are correlated to reliability targets either directly (e.g., given the pipe wall thickness we could estimate a probability of a crack initiation using fracture mechanics techniques) or indirectly (e.g., a success criterion for a pump is associated with a range of normal, i.e., expected, flowrate and a minimum flowrate).

The outcome from this project is a framework that the nuclear power industry can use when developing a RIM program in compliance with RG 1.246 and establishing reliability targets which must comply with the requirements of both RG 1.246 and RG 1.233. Another outcome is an efficient and effective approach to manage complexity of the RIM program by employing MBSE methods and tools.

6. REFERENCES

[1] ASME Section XI, Division 2, "Requirements for Reliability and Integrity Management (RIM) Programs for Nuclear Power Plants," 2019 ASME Boiler & Pressure Vessel Code, Section XI: Rules for Inservice Inspection of Nuclear Power Plant Components, Division 2, 2019.

[2] NEI, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," Nuclear Energy Institute, Technical Report 18-04, 2019.

[3] NRC, "Regulatory Guide 1.233 Revision 0: Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors," U.S. Nuclear Regulatory Commission, ML20091L698, 2020.

[4] NRC, "Regulatory Guide 1.246: Acceptability of ASME Code, Section XI, Division 2, Requirements for Reliability and Integrity Management (RIM) Programs for NPPs, for non-LWRs," U.S. Nuclear Regulatory Commission, October 2022.

[5] D. Mandelli, T. Anselmi, C. Smith, S. Lawrence and C. Otani, "Reliability and Integrity Management Program Implementation Approach," Idaho National Laboratory, INL/RPT-22-68899, 2022.

[6] INCOSE, Systems Engineering Handbook, Fourth Edition, Wiley, 2015.

[7] Spec Innovations, "INNOSLATE," Spec Innovations, [Online]. Available: https://specinnovations.com/. [Accessed September 2023].

[8] Center for Chemical Process Safety, "Guidelines for Hazard Evaluation Procedures, 3rd Edition," Wiley & Sons, 2008.

[9] IEC 60812, "Failure modes and effects analysis (FMEA and FMECA)," International Electrotechnical Commission, 2018.

[10] Mil STD 1629A, "Procedures for Performing a Failure Mode, Effects, and Criticality Analysis," U.S. Department of Defense, 1980.

[11] Army Regulation 702-19, "Reliability, Availability, and Maintainability," U.S. Department of the Army, Washington D.C., 2020.

[12] D. Elbèze, D. v. Houtte and E. Delchambre, "Different Methods for Assessing System Failure Criticality in the RAMI Approach," *ANS Fusion Science and Technology,* 2019.

Page intentionally left blank

APPENDIX A: RELIABILITY AND INTEGRITY MANAGEMENT MODEL-BASED SYSTEMS ENGINEERING PROCESS MODEL

This Appendix contains material that is reprinted from ASME 2021 Edition, Section XI, Division 2, (pages 4-9), by permission of The American Society of Mechanical Engineers. All rights reserved. No copies of the material granted can be made or used without written permission from ASME.

Implement Reliability and Integrity Management Process

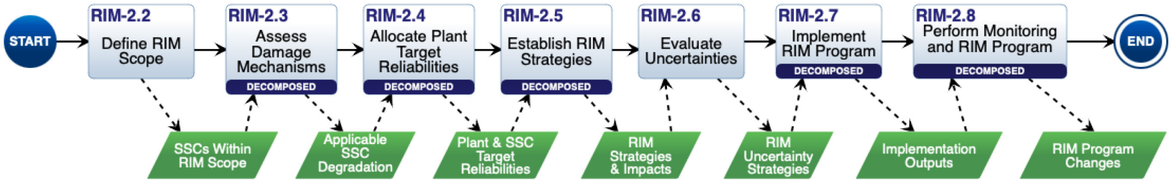


Figure A-1. Innoslate representation of the RIM process.

RIM-2.2 Define Reliability and Integrity Management Scope

The Owner shall document the specific list of SSCs to be evaluated for inclusion within the scope of the RIM program. The scope shall include SSCs where failure could adversely affect plant safety and reliability. The Owner shall also document the basis for the exclusion of any SSC considered to be outside the scope of the RIM program.

RIM-2.3 Assess Damage Mechanisms

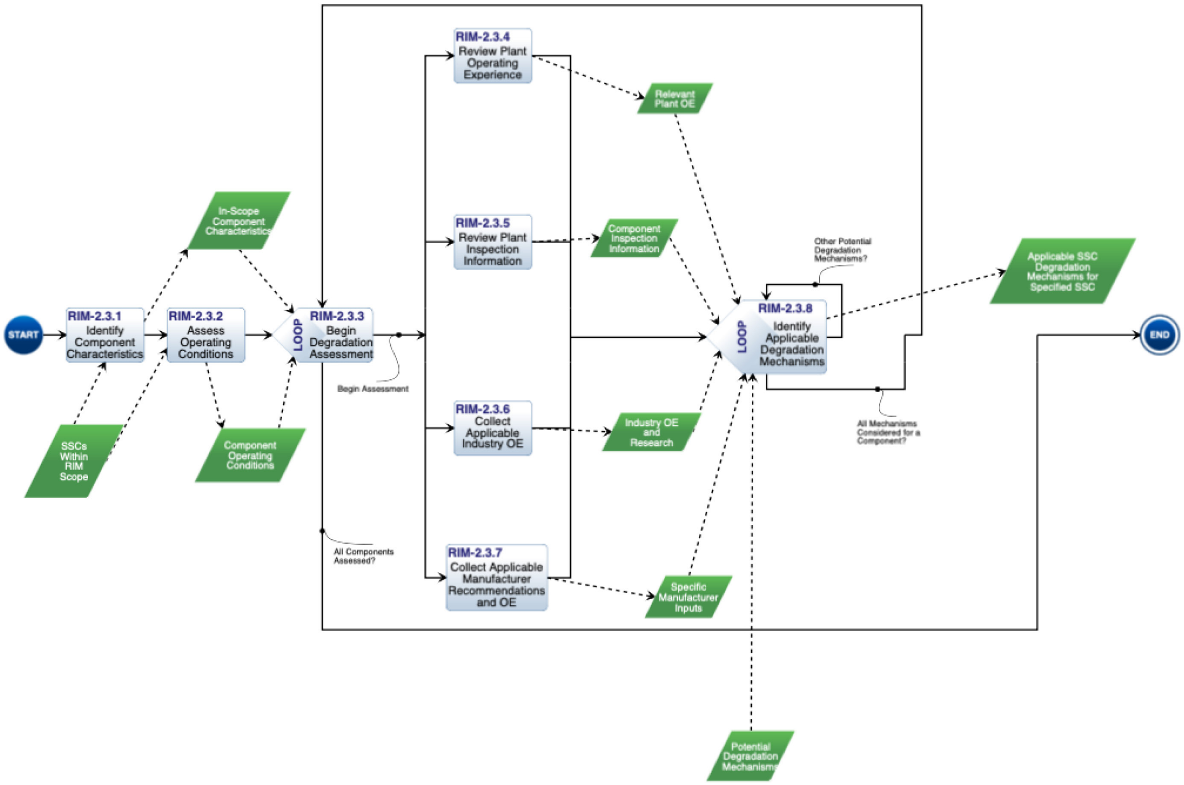

RIM-2.3.4
Review Plant Operating Experience
Relevant Plant OE
In-Scope Component Characteristics
RIM-2.3.5
Review Plant Inspection Information
Component Inspection Information
Other Potential Degradation Mechanisms?
Applicable SSC Degradation Mechanisms for Specified SSC
START
RIM-2.3.1
Identify Component Characteristics
RIM-2.3.2
Assess Operating Conditions
LOOP
RIM-2.3.3
Begin Degradation Assessment
LOOP
RIM-2.3.8
Identify Applicable Degradation Mechanisms
END
Begin Assessment
RIM-2.3.6
Collect Applicable Industry OE
Industry OE and Research
All Mechanisms Considered for a Component?
SSCs Within RIM Scope
Component Operating Conditions
All Components Assessed?
RIM-2.3.7
Collect Applicable Manufacturer Recommendations and OE
Specific Manufacturer Inputs
Potential Degradation Mechanisms

Figure A-2. RIM damage mechanism assessment.

(a) The following conditions shall be considered in the damage mechanism assessment (DMA):

(1) Design characteristics, including material, pipe size and schedule, component type (e.g., standard fittings, elbows, flanges), and other attributes related to the system configuration

(2) Fabrication practices, including welding and heat treatment

(3) Operating and transient conditions, including temperatures, pressures, quality of primary and secondary fluid, and service environment (e.g., humidity, radiation)

(4) Plant-specific, industry-wide service experience and research experience

(5) Results of preservice, in-service, and augmented examinations and the presence and impact of prior repairs in the system

(6) Applicable degradation mechanisms, including those identified in Mandatory Appendix VII for the applicable plant type

(7) Recommendations by SSC vendors for examination, maintenance, repair, and replacement

(b) The criteria used to identify and evaluate the susceptibility of each SSC to degradation mechanisms shall be specified in the RIM program documentation. The screening criteria found in Mandatory Appendix VII are minimum requirements to be considered but may be augmented by the Reliability and Integrity Management Expert Panel (RIMEP).

RIM-2.3.1 Identify Component Characteristics

Identify the component design and design characteristics. Design characteristics can include:

(1) Component function (active or passive)

(2) Component type (valve, pump, transmitter, motor, pipe, support, etc.)

(3) Component material, pipe size, and schedule (as applicable), component construction (e.g., standard fittings, elbows, flanges, custom fabrication), and other attributes related to the system configuration

(4) Fabrication practices, including welding and heat treatment

RIM-2.3.2 Assess Operating Conditions

Assess the operating conditions of the in-scope components: Operating and transient conditions, including temperatures, pressures, quality of primary and secondary fluid, and service environment (e.g., humidity, radiation).

RIM-2.3.3 Begin Degradation Assessment

The degradation assessment looks at in-scope components to determine the applicable mechanisms for each. Components may be evaluated individually or as groups of similar components. Once all in-scope components have been evaluated, the process is complete.

RIM-2.3.4 Review Plant Operating Experience

Review the component and system operating experience for the component/groups. This includes corrective actions, identified component or maintenance issues, system transients, and trends.

RIM-2.3.5 Review Plant Inspection Information

Review the results of preservice, in-service, and augmented examinations and the presence and impact of prior repairs in the system.

RIM-2.3.6 Collect Applicable Industry OE and Research for Component Type

Collect any applicable **industry** OE on the specific component type from relevant industry sources. Includes industry-wide service experience and research experience.

RIM-2.3.7 Collect Applicable Manufacturer Recommendations and OE

Collect any recommendations from the SSC vendors for examination, maintenance, repair, and replacement.

RIM-2.3.8 Identify Applicable Degradation Mechanisms

Degradation mechanisms are identified using the previously collected information. The component/group characteristics, operating conditions, relevant operating experience, inspections, and any industry operating experience or manufacturer recommendations are all inputs to determining the applicable degradation mechanisms from the list of potential mechanisms.

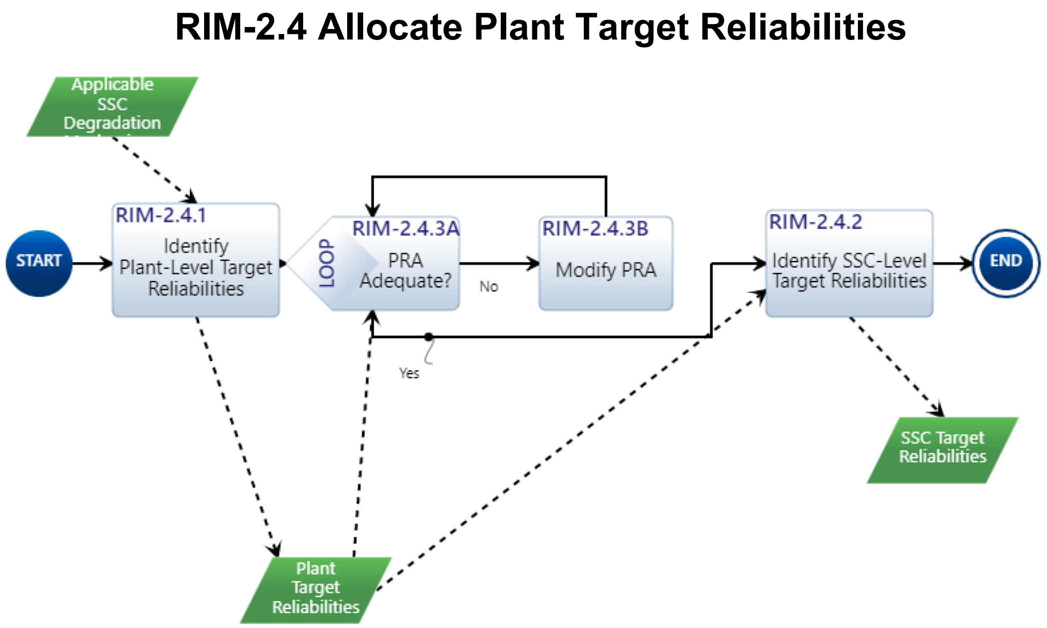

RIM-2.4 Allocate Plant Target Reliabilities
Applicable SSC Degradation
START
RIM-2.4.1
Identify Plant-Level Target Reliabilities
LOOP
RIM-2.4.3A
PRA Adequate?
No
RIM-2.4.3B
Modify PRA
Yes
RIM-2.4.2
Identify SSC-Level Target Reliabilities
END
SSC Target Reliabilities
Plant Target Reliabilities

Figure A-3. RIM target reliability allocation.

The RIMEP shall identify plant-level risk and reliability targets for RIM and use information provided by the plant specific PRA to identify SSC-level reliability targets for SSCs relied upon to prevent and mitigate the consequences of accident scenarios and in a manner that is consistent with the plant-level reliability goals.

RIM-2.4.1 Identify Plant-Level Target Reliabilities

(a) The RIMEP shall identify plant level risk and reliability targets for RIM. Plant-level reliability shall be derived from regulatory limits on the risks, frequencies, and radiological consequences of licensing basis events that are defined in the PRA.

The RIM program may be developed for single reactor module or plants with two or more reactor modules. Event sequence frequencies shall be expressed in terms of events per plant-year where the plant may include a single reactor or multiple reactor modules. The event sequence consequences may involve source terms from single or multiple reactor modules, or source terms from non-core related radionuclide sources and associated off-site radiological consequences.

(b) Plant-level RIM goals may include additional goals to meet plant availability.

RIM-2.4.2 Identify SSC-Level Target Reliabilities

(a) The RIMEP shall use information provided by the plant specific PRA to identify SSC-level reliability targets for SSCs relied upon to prevent and mitigate the consequences of accident scenarios and in a manner that is consistent with the plant level reliability goals.
(b) The PRA model shall be used to allocate SSC reliability targets from and consistent with the plant-level reliability goals.
(c) The allocation of SSC-level reliability targets shall consider the uncertainties inherent in the prediction of SSC reliability.

(d) SSC-level reliability targets may also be identified by the RIMEP for overall plant availability considerations.
(e) The methodology for deriving reliability targets is contained in Mandatory Appendix II.

RIM-2.4.3A PRA Adequacy

(a) The scope of the PRA used to allocate SSC reliability targets shall address:
   1) The plant operating states relevant to the plant level risk and reliability goals and SSC-level reliability targets
   2) A full set of IEs including internal events and events associated with external plant hazards
   3) Event sequence development that is sufficient to support the quantification of mechanistic source terms and off-site radiological consequences consistent with applicable regulatory limits on the frequencies and consequences of accident scenarios.

Although all plant operating modes and hazard groups shall be addressed, it is not always necessary to have a full scope PRA as outlined above. Qualitative treatment or hazard groups may be sufficient if it can be demonstrated that those risk contributions would not affect the reliability targets or other aspects of the RIM program.

(b) The level of detail required of the PRA is that which is sufficient to establish reliability targets for the SSCs to be included in the RIM program. If the SSCs of interest cannot be associated with elements of the PRA, the PRA should be modified accordingly. PRA models for current LWR types frequently exclude passive components (e.g., piping) due to their much lower failure probabilities than active components. For implementation of RIM and the allocation of reliability targets, such components would need to be included in the PRA if included within the scope of the RIM program.

(c) Technical adequacy refers to the suitability of the PRA modeling and the reasonableness of the underlying assumptions and approximations. The PRA shall meet the requirements of the PRA Standard for Advanced Non-LWR for Nuclear Power Plants, latest edition, to the extent necessary to support RIM program development. The PRA standard provides technical supporting requirements in terms of Capability Categories. The delineation of Capability Categories is such that the PRA scope, level of detail, plant specificity and realism increase from Capability Category I to Capability Category II. Current good practice (Capability Category II) is generally expected to be necessary to support RIM, although Capability Category I may be sufficient for some requirements. All significant PRA peer review findings shall be reviewed and dispositioned by incorporating changes into the PRA model, performing sensitivity studies to evaluate the identified issue, or providing justification for the original PRA model. The results of the PRA peer review and the review of other risk information used in the RIM program development shall be documented in a characterization of the adequacy of the PRA.

See also RIM-2.10, Additional considerations for RIM Program Implementation

RIM-2.4.3B Modify PRA

Revision of the PRA model to address any deficiencies identified. The PRA model is modified until deemed adequate for identification.

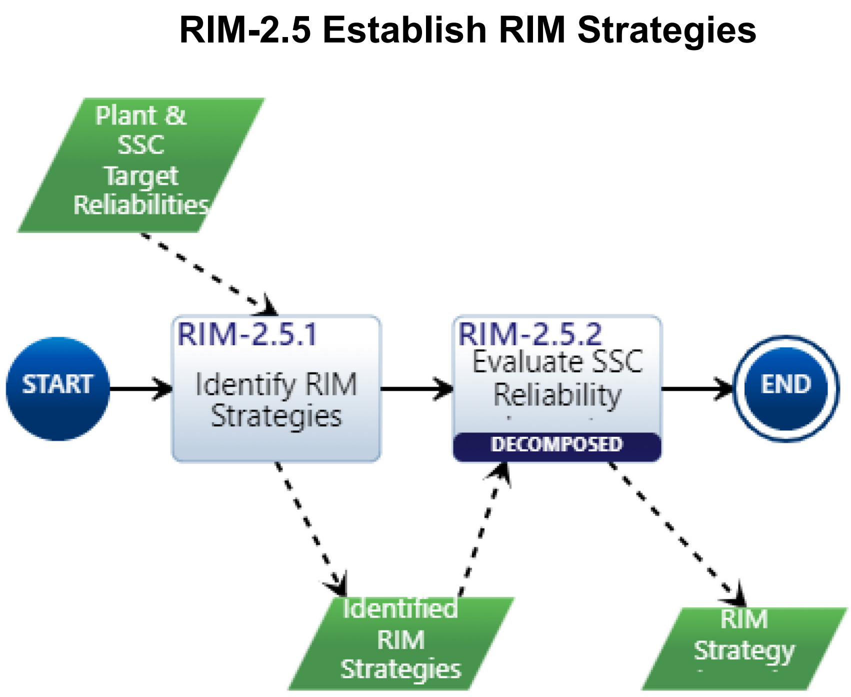


Figure A-4. RIM strategy establishment.

The RIMEP shall identify the RIM strategies that are available to meet the reliability targets and evaluate and select combinations of strategies that will meet and maintain the reliability targets.

RIM-2.5.1 Identify RIM Strategies

(a) The strategies shall account for all factors that contribute to reliability. These factors shall include but not necessarily be limited to:
  (1) Design strategies, including material selection
  (2) Fabrication procedures
  (3) Operating practices
  (4) Preservice and in-service examinations
  (5) Testing
  (6) MANDE
  (7) Maintenance, repair, and replacement practices

(b) The evaluated RIM strategies shall account for the potential for specific degradation mechanisms applicable to each SSC in the scope of the RIM program identified in Mandatory Appendix VII.

(c) The RIMEP shall select the RIM strategies or combinations of strategies that are necessary and sufficient to achieve and maintain SSC reliability consistent with SSC reliability targets established in RIM-2.4.2.

(d) In addition to the use of probabilistic methods that are permitted by this Division for establishing MANDE criteria, deterministic methodology for examinations and acceptance criteria, as outlined in Nonmandatory Appendix A, A-3.5 may be used.

RIM-2.5.2 Evaluate SSC Reliability Impacts

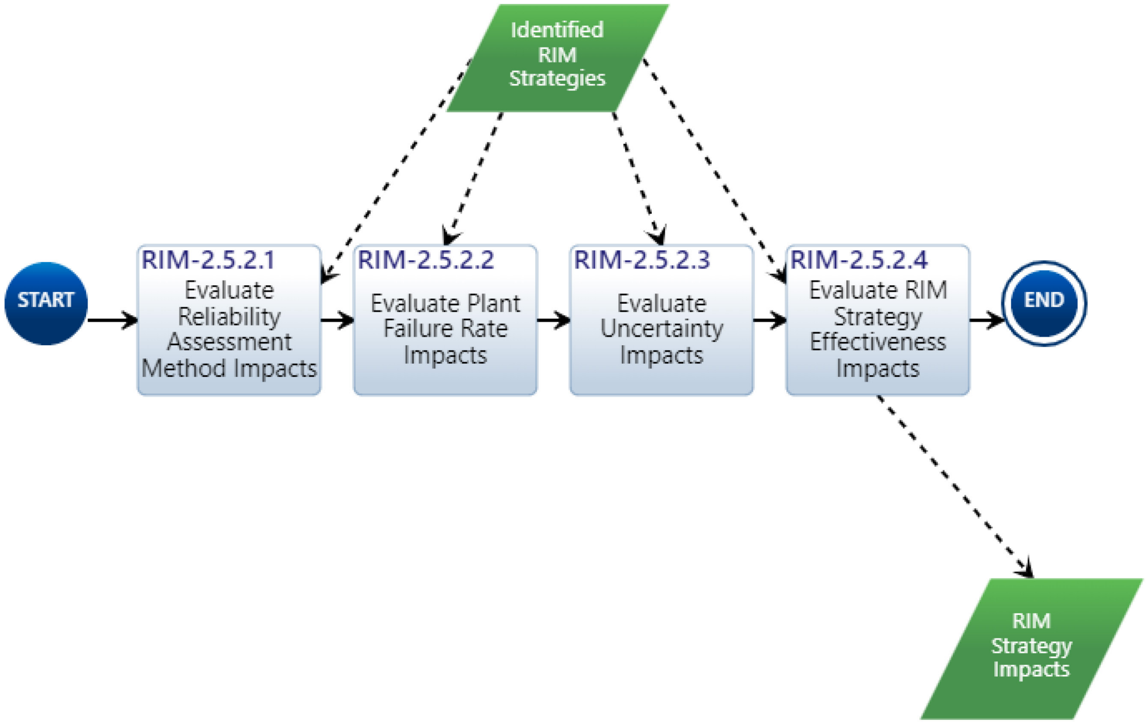

Identified
RIM
Strategies
START
RIM-2.5.2.1
Evaluate Reliability Assessment Method Impacts
RIM-2.5.2.2
Evaluate Plant Failure Rate Impacts
RIM-2.5.2.3
Evaluate Uncertainty Impacts
RIM-2.5.2.4
Evaluate RIM Strategy Effectiveness Impacts
END
RIM
Strategy
Impacts

Figure A-5. RIM strategy impact assessment.

RIM-2.5.2 Evaluation of RIM Strategy Impacts on SSC Reliability

(a) The impact of each RIM strategy that is considered for inclusion into the RIM program in accordance with RIM-2.5 on the reliability of each SSC in the scope of the RIM program shall be assessed for comparison against the SSC-level reliability targets.

RIM-2.5.2.1 Evaluate Reliability Assessment Method Impacts

Application of acceptable SSC reliability assessment methods, such as statistical analysis of failure data, probabilistic fracture mechanics, Markov modeling, expert elicitation, or appropriate combinations of these methods.

RIM-2.5.2.2 Evaluate Plant Failure Rate Impacts

Assessment of SSC plant-specific failure rates that correspond to the frequencies of IEs and PRA and SSC failure probabilities for mitigating events in the PRA model. This formulation shall be consistent with the reliability metrics selected for the SSC reliability target allocation in accordance with RIM-2.4.2.

RIM-2.5.2.3 Evaluate Uncertainty Impacts

Evaluation of the effectiveness of the RIM strategy that accounts for the quantity and applicability of applied failure data, uncertainty in the estimates of component exposure populations, materials, variability of operating conditions, and variability of expert opinion.

RIM-2.5.2.4 Evaluate RIM Strategy Effectiveness Impacts

Identification and evaluation of the effectiveness and extent of the RIM strategy or combination of strategies including the percentage of the SSCs to which the strategy is applied, probability of detection, inspection frequency, flaw sizing accuracy, time to detect, accessibility, and other factors of the RIM program that influence the SSC reliability.

RIM-2.6 Evaluate Uncertainties

The RIMEP shall identify additional RIM strategies over and above those determined in accordance with RIM-2.5 that are necessary to provide additional assurance that the reliability targets will be achieved and maintained during the SSC service lifetime in order to address uncertainties in predicting SSC reliability performance. Specific RIM strategies that are included to address these uncertainties shall be documented in accordance with RIM-2.7.1.

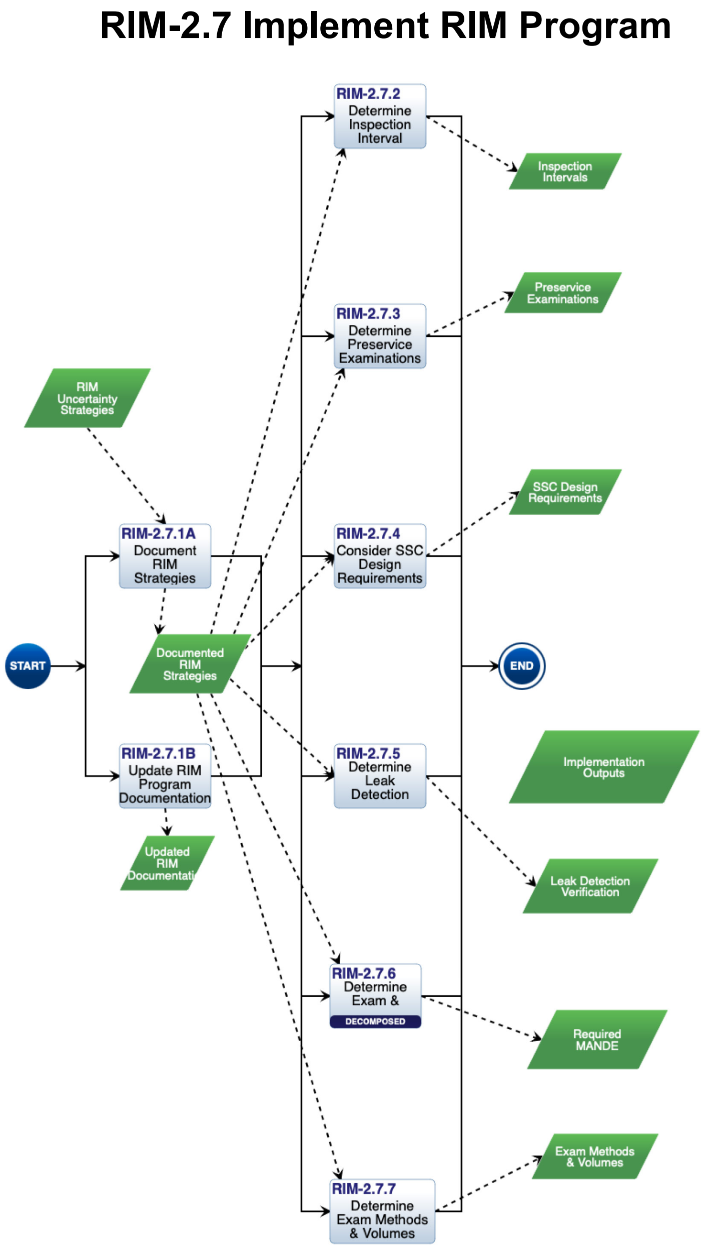

RIM-2.7 Implement RIM Program
START
RIM Uncertainty Strategies
RIM-2.7.1A Document RIM Strategies
Documented RIM Strategies
RIM-2.7.1B Update RIM Program Documentation
Updated RIM Documentati
RIM-2.7.2 Determine Inspection Interval
Inspection Intervals
RIM-2.7.3 Determine Preservice Examinations
Preservice Examinations
RIM-2.7.4 Consider SSC Design Requirements
SSC Design Requirements
END
Implementation Outputs
RIM-2.7.5 Determine Leak Detection
Leak Detection Verification
RIM-2.7.6 Determine Exam &
DECOMPOSED
Required MANDE
RIM-2.7.7 Determine Exam Methods & Volumes
Exam Methods & Volumes

Figure A-6. Selected RIM strategy to achieve desired target reliabilities.

RIM-2.7.2 Determine Inspection Interval

(a) In-service examinations selected for inclusion into the RIM program for specific SSCs shall be completed during each inspection interval for the service lifetime of the plant. The inspections shall be performed in accordance with the schedule for implementing the RIM program. (See XI, Div. 2 for interval requirements).

(b) The inspection interval shall be determined by the RIMEP and shall not exceed 12 years.
(c) The interval shall be divided into two or more approximately equal inspection periods for planning the examinations over the inspection interval. The examinations that are required for each interval shall be approximately equally distributed over the inspection periods.
(d) Each inspection interval may be reduced or extended by as much as 1 year. Adjustments shall not cause successive intervals to be altered by more than 1 year from the original pattern of intervals. If an inspection interval is extended, neither the start and end dates nor the RIM program for the successive interval need be revised.
(e) Examinations may be performed to satisfy the requirements of the extended interval in conjunction with examinations performed to satisfy the requirements of the successive interval. However, an examination performed to satisfy requirements of either the extended interval or the successive interval shall not be credited to both intervals.
(f) The portion of an inspection interval described as an inspection period may be reduced or extended by as much as 1 year to enable an inspection to coincide with a plant outage. This adjustment shall not alter the requirements for scheduling inspection intervals.
(g) The inspection interval for which an examination was performed shall be identified on examination records.
(h) In addition to (d), for plants that are out of service continuously for 6 months or more, the inspection interval during which the outage occurred may be extended for an inspection period equivalent to the outage and the original pattern of intervals extended accordingly for successive intervals.
(i) The inspection intervals for items installed by repair/replacement activities shall coincide with remaining intervals, as determined by the calendar years of plant service at the time of the repair/replacement activities.

RIM-2.7.3 Determine Preservice Examinations

(a) For those categories of SSCs for which examinations have been selected as a RIM strategy for inclusion in the RIM program, a preservice examination shall be performed. If any percentage of the SSC category has been selected for in-service examination, then 100% of the SSCs shall be subjected to a preservice examination using the same examination method used for in-service examination. The purpose of these preservice examinations is to establish a baseline in the event an in-service examination is required at each location. These preservice baseline examinations shall be performed using personnel, procedures and equipment that have been qualified and demonstrated to the Inspector to reliably detect and accurately characterize fabrication flaws. These examinations shall be documented using encoded equipment and scanners (no manual examinations allowed) and a permanent archival record of the flaws identified shall be created for the material examined. The examination records and results shall be reviewed by the Inspector to ensure that potential flaws are assessed, and completeness of records is established. Flaws identified in these examinations shall be evaluated for service in accordance with the flaw acceptance criteria in Article RIM-3. Selection of the analytical evaluation method is the responsibility of the monitoring and non-destructive examination expert panel (MANDEEP).

(b) The examinations required by this article for those components initially selected for examination in accordance with the RIM program shall be completed prior to initial plant startup.

(c) Shop and field examinations may serve in lieu of the on-site preservice examinations, provided
  (1) In the case of vessels only, the hydrostatic test required by the Construction Code has been completed
  (2) Such examinations are conducted and meet the requirements under (a)

(3) The shop and field examination records are, or can be, documented and identified in a form consistent with those required in Article RIM-6.

RIM-2.7.4 Consider SSC Design Requirements

(a) The RIM program shall consider the design requirements of SSCs that are identified as part of the RIM strategies established in RIM-2.5 and as may be required to prevent or reduce the susceptibility to degradation mechanisms determined in RIM-2.3 or otherwise needed to support a selected RIM strategy, e.g., provision for an online leak detection system.

(b) The design requirements that result from any plant modifications to an SSC within the scope of the RIM Program shall include considerations to assure that adequate access is maintained in order to be able to perform MANDE over the life of the SSC(s).

RIM-2.7.5 Determine Leak Detection Requirements

The leak detection capabilities of monitoring systems that are employed as a selected RIM strategy shall have performance characteristics such as probability of detection, time to detect, minimum detectable leak rate, and system reliability and availability characteristics that are sufficient to meet SSC RIM reliability targets established in RIM-2.4.2. Verification of adequate performance of online leak detection systems shall be demonstrated in accordance with RIM-5.2.

RIM-2.7.6 Determine Exam & Inspection Requirements

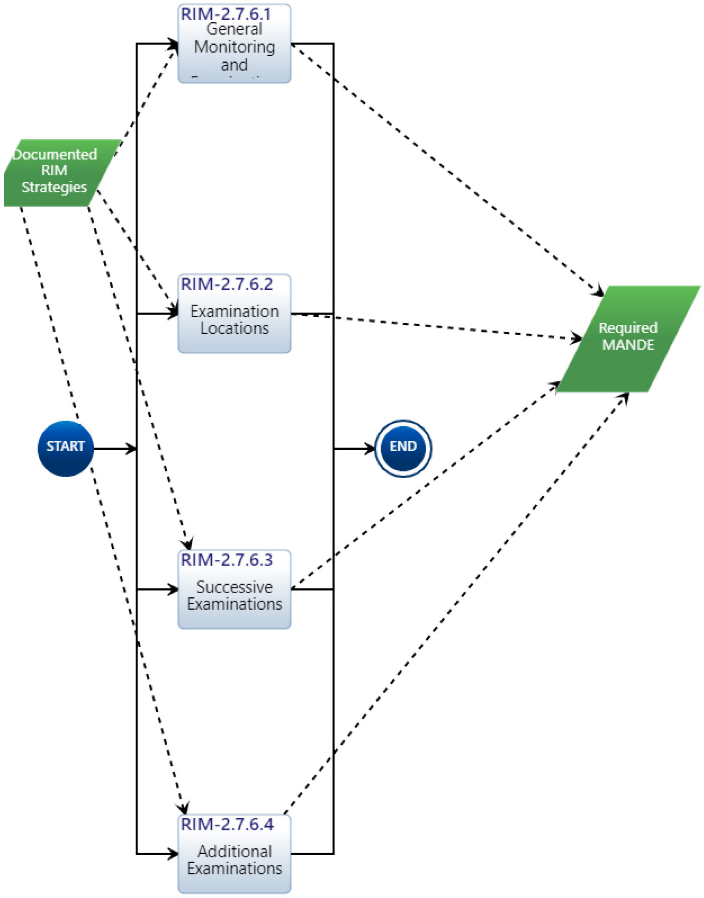


Figure A-7. RIM inspection requirements.

(a) MANDE criteria shall be defined so the scope, method, detection reliability, frequency, and performance demonstration provides information to demonstrate that the reliability targets continues to be met for the SSCs included in the RIM program as established in RIM-2.4.2.
(b) MANDE performed to provide and maintain SSC reliability targets shall meet, where applicable, the following requirements: (See XI, Div. 2)
(c) MANDE requirements for the SSCs within the scope of the RIM program for which specific requirements have not been specified shall be defined by the RIMEP and documented with a technical basis.
(d) The MANDE methods and procedures shall account for the potential degradation mechanisms identified in Mandatory Appendix VII.
(e) Examination volumes, methods, and frequencies appropriate for each degradation mechanism are provided in RIM-2.7.7 and Mandatory Appendix V and augmented for specific reactor designs as outlined in the relevant reactor design article contained in Mandatory Appendix VII.

RIM-2.7.6.1 General Monitoring and Examination Requirements

(a) MANDE criteria shall be defined so the scope, method, detection reliability, frequency, and performance demonstration provide information to demonstrate that the reliability targets continue to be met for the SSCs included in the RIM program as established in RIM-2.4.2.
(b) MANDE performed to provide and maintain SSC reliability targets shall meet, where applicable, the following requirements:
    (1) The functional or structural reliability of a system or system components shall be monitored using a program that may include one or more of the following activities that could be done either periodically or continuously:

        (-a) Operating fluid leakage detection and monitoring
        (-b) Monitoring the amount of make-up fluid
        (-c) Walk downs to monitor the operating fluid level in storage tanks
        (-d) Monitoring fluid level or flow in drains
        (-e) Monitoring humidity levels
        (-f) Monitoring radiation levels
        (-g) Auxiliary operator plant walk-through.

    (2) MANDE activities shall be conducted on any SSC within the RIM program scope. It may include: continuous leakage monitoring or periodic leak testing as required to meet the allocated SSC reliability target.
    (3) The functional or structural reliability of a system or system components shall be monitored using a program that considers the following factors:

        (-a) Potential for active degradation mechanisms
        (-b) Radiological consequences of SSC failure
        (-c) Personnel radiation exposure
        (-d) Insights from plant and industry service or research experience.

(c) MANDE requirements for the SSCs within the scope of the RIM program for which specific requirements have not been specified shall be defined by the RIMEP and documented with a technical basis.

(d) The MANDE methods and procedures shall account for the potential degradation mechanisms identified in Mandatory Appendix VII.

(e) Examination volumes, methods, and frequencies appropriate for each degradation mechanism are provided in RIM-2.7.7 and Mandatory Appendix V and augmented for specific reactor designs as outlined in the relevant reactor design article contained in Mandatory Appendix VII.

RIM-2.7.6.2 Examination Locations

The location and number of non-destructive examinations (NDE) shall be defined using the following requirements in each inspection interval:

(a) The minimum number of locations shall be selected to meet the SSC reliability target.
(b) Examination locations shall be selected in accordance with the following criteria:
    (1) Locations where the consequence of a postulated rupture would result in high risk.
    (2) To maintain personnel exposure within acceptable limits, examinations generally will be performed away from areas with high irradiation levels.
    (3) Locations where 100% of the areas of concern can be examined.

RIM-2.7.6.3 Successive Examinations

(a) If an SSC is accepted for continued service in accordance with Article RIM-3, the areas containing flaws or relevant conditions shall be reexamined based on the MANDE and periodicity criteria established by the flaw evaluation results.
(b) If the reexaminations required by (a) reveal that the flaw or relevant condition remain essentially unchanged, the SSC MANDE schedule may revert to the original schedule of successive inspections.

RIM-2.7.6.4 Additional Examinations

(a) Examinations performed in accordance with Mandatory Appendix V and any augmented provisions from Mandatory Appendix VII supplements applicable to a specific reactor design, that reveal a flaw or a relevant condition exceeding the acceptance standards of Mandatory Appendix XII, Table VII-1.3.3-1 or Table VII-3.3.3-1 shall be extended to include additional examinations during the current outage. The additional examinations shall include an additional number of welds, areas of interest, or parts and shall be determined by and the basis documented by MANDEEP. The additional examinations shall be selected from welds, areas of interest, or parts of similar material and service. This additional selection may require inclusion of SSCs other than the one containing the flaws or relevant conditions.

(b) If the additional examinations required by (a) reveal a flaw or a relevant condition exceeding the acceptance standards of Mandatory Appendix VII, Table VII-1.3.3-1 or Table VII-3.3.3-1, the examinations shall be further extended to include additional examinations during the current outage. These additional examinations shall include the remaining welds, areas of interest, or parts of similar material and service subject to the same type of flaws or relevant conditions.

(c) For the inspection period following the period in which the examinations of (a) or (b) were completed, the examinations shall be performed as originally scheduled.

(d) No additional examinations are required if either of the following applies: (1) There are no other SSC subject to the same apparent or root cause conditions. (2) The degradation mechanism no longer exists.

RIM-2.7.7 Determine Exam Methods & Volumes

(a) Examination programs developed in accordance with Article RIM-2 shall use examination techniques suitable for specific degradation mechanisms and examination locations. The examination volumes and methods that shall be considered by MANDEEP in establishing MANDE criteria, and that are applicable to each degradation mechanism, are provided in the applicable article of Mandatory Appendix VII and Mandatory Appendix V.

(b) The personnel, equipment, and procedures used for the examinations shall be qualified to reliably detect and size the relevant degradation identified for each element in accordance with Mandatory Appendix IV. Examinations shall be conducted and documented in accordance with RIM-2.8.

RIM-2.7.1A Document RIM Strategies

(a) The Owner shall document the RIM strategies that are selected for inclusion into the RIM program as part of the RIM program documentation. This documentation shall include the following:
   (1) The scope of SSCs selected for inclusion in the RIM program
   (2) The results of the DMA evaluation for the SSCs in the RIM program
   (3) The plant-level risk and reliability goals
   (4) SSC reliability targets derived from the plant-level risk and reliability goals
   (5) Technical adequacy of the PRA and risk information used to derive the SSC reliability target
   (6) The specific RIM strategies selected for the RIM program for each SSC including associated performance parameters that are required to achieve reliability targets, (e.g., probability of detection, inspection intervals)
   (7) The evaluation of the impact of RIM strategies and combination of RIM strategies on the SSC reliability performance
   (8) The quantification of uncertainties and evaluation of additional RIM strategies selected to address uncertainties.

RIM-2.7.1B Update RIM Program Documentation

(b) The RIM program documentation shall be updated periodically to evaluate changes to any of the technical inputs as described in RIM-2.8, but no later than the end of each established inspection interval.

RIM-2.8 Perform Monitoring and RIM Program Updates

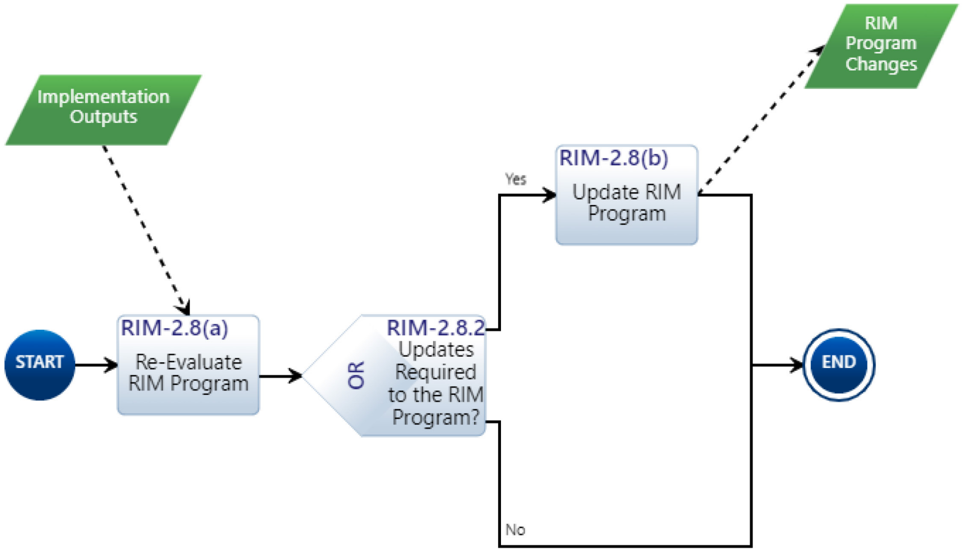


Figure A-8. RIM monitoring and update.

(a) The affected portions of the RIM program shall be reevaluated to incorporate results from SSC performance MANDE and new information affecting implementation of the program as it becomes available. New information may include the following: (See XI, Div. 2)

(b) RIM program updates may include adjustment of SSC reliability targets based on new information described in (a) and/or PRA updates.

(1) Reliability targets should not be decreased to correspond with changes in SSC performance or service-related degradation, without determining the risk impact and the effect on other reliability target allocations based on the derivation methodology in Mandatory Appendix II and additional considerations in RIM-2.10.

(2) The minimum frequency of RIM program updates shall be at each inspection interval as specified in RIM-2.7.2(b). RIM program updates should be more frequent if dictated by PRA updates or if new degradation mechanisms are identified.

RIM-2.8.2 Updates Required to the RIM Program?

Determination of required updates is based upon the re-evaluation of current RIM strategies under 2.8.a.

RIM-2.8(a) Re-Evaluate RIM Program

(a) The affected portions of the RIM program shall be reevaluated to incorporate results from SSC performance MANDE and new information affecting implementation of the program as it becomes available. New information may include the following:

(1) Changes to plant design, which may introduce (or remove) SSCs within the scope of the RIM program, as well as changes in materials, configurations, stresses, etc. Changes to plant design may also result in significant changes to plant risk, as determined by PRA update, which may require update of the reliability target allocations.

(2) Changes to plant procedures, such as operating parameters, system lineups, equipment, and operating modes, may result in different degradation mechanisms or MANDE capability, as well as changes to plant risk, as determined by PRA update.

(3) Changes in SSC performance, indicating a potential change in reliability.

(4) MANDE results indicate service-related degradation.

(5) Industry or research experience, including SSC failure or reliability data or degradation mechanisms.

RIM-2.8(b) Update RIM Program

RIM program updates may include adjustment of SSC reliability targets based on new information described in 2.8(a) and/or PRA updates.

(1) Reliability targets should not be decreased to correspond with changes in SSC performance or service-related degradation, without determining the risk impact and the effect on other reliability target allocations based on the derivation methodology in Mandatory Appendix II and additional considerations in RIM-2.10.

(2) The minimum frequency of RIM program updates shall be at each inspection interval as specified in RIM-2.7.2(b). RIM program updates should be more frequent if dictated by PRA updates or if new degradation mechanisms are identified.

APPENDIX B: INNOSLATE RIM STRATEGY EXAMPLE

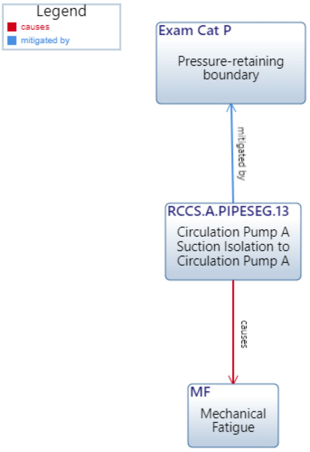


Figure B-1. Pipe segment 13 Innoslate relationships.

Table B-1. PipeSeg 13 Entity Definition

Attributes	
Attribute Name	**Attribute Value**
Material	Carbon Steel
External Environment	Indoor Controlled Air
Internal Environment	Treated Water
Operating Temperature	150°F
Operating Pressure	35psi
System Chemistry (pH)	8
Specific Operating Concerns	Vibration Potential
Capacity	0.0
Monitoring/Testing Strategy	
Latency	1.0 HOURS
Frequency of Performance	
Units	
PRA Basic Event	Small Break, Medium Break, Large Break

Relationships		
Relationship	**Relationship Attribute**	**Relationship Target**
causes		Mechanical Fatigue
connects to	Origin: No	Circulation Pump A
connects to	Origin: Yes	Circulation Pump A Suction Isolation
mitigated by		Pressure-retaining boundary
satisfies		SB, Small Break
satisfies		MB, Medium Break
satisfies		LB, Large Break

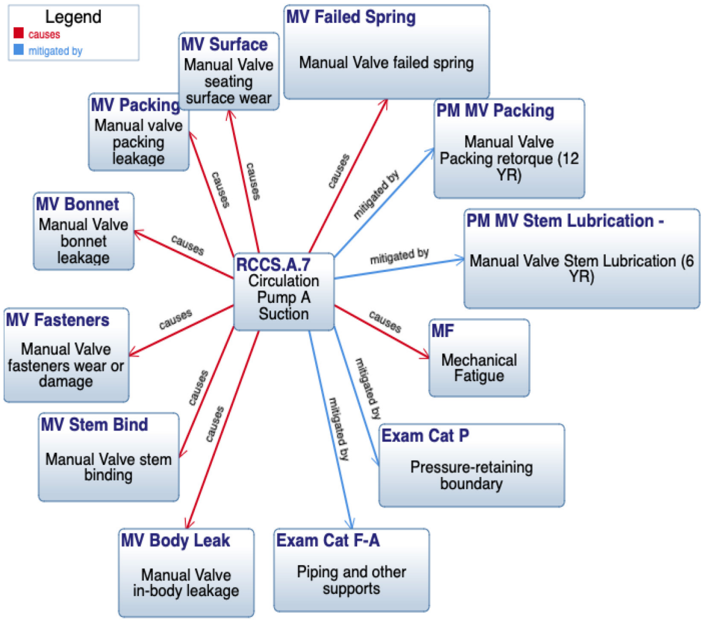

Legend
causes
mitigated by
MV Failed Spring
Manual Valve failed spring
MV Surface
Manual Valve seating surface wear
MV Packing
Manual valve packing leakage
PM MV Packing
Manual Valve Packing retorque (12 YR)
PM MV Stem Lubrication -
Manual Valve Stem Lubrication (6 YR)
MV Bonnet
Manual Valve bonnet leakage
RCCS.A.7
Circulation Pump A Suction
MV Fasteners
Manual Valve fasteners wear or damage
MF
Mechanical Fatigue
MV Stem Bind
Manual Valve stem binding
Exam Cat P
Pressure-retaining boundary
MV Body Leak
Manual Valve in-body leakage
Exam Cat F-A
Piping and other supports
causes
mitigated by

Figure B-2. RCCS.A.7 Isolation valve Innoslate relationships.

Table B-2. RCCS.A.7 Entity Definition

Attributes	
Attribute Name	**Attribute Value**
Operating Temperature	150°F
Frequency of Performance	
System Chemistry (pH)	8
Internal Environment	Treated Water
PRA Basic Event	External Large Leak, External Small Leak, Spurious Fault
External Environment	Indoor Controlled Air
Material	Carbon Steel
Specific Operating Concerns	Vibration Potential
Monitoring/Testing Strategy	

Relationships		
Relationship	**Relationship Attribute**	**Relationship Target**
causes		Manual Valve bonnet leakage
causes		Manual Valve seating surface wear
causes		Mechanical Fatigue
causes		Manual Valve stem binding
causes		Manual Valve failed spring
causes		Manual Valve fasteners wear or damage
causes		Manual valve packing leakage
causes		Manual Valve in-body leakage
connected by	Origin: Yes	Circulation Pump A Suction Isolation to

Attributes	
Attribute Name	**Attribute Value**
Operating Pressure	35psi

Relationships		
Relationship	**Relationship Attribute**	**Relationship Target**
		Circulation Pump A
connected by	Origin: No	Pipe Tee to Circulation Pump A Suction Isolation
decomposes		RCCS Train A
mitigated by		Manual Valve Stem Lubrication (6 YR)
mitigated by		Manual Valve Packing retorque (12 YR)
mitigated by		Piping and other supports
mitigated by		Pressure-retaining boundary
performs		Isolate Components for Maintenance
satisfies		Isolation Valve Performance
satisfies		FO, Failure to Open
satisfies		SF, Spurious Fault
satisfies		Maintenance Isolation
satisfies		LL, External Large Leak
satisfies		SL, External Small Leak

APPENDIX C: COMPARISON OF RISK EVALUATION METHODS WITH RIM

Table C-1. Comparison of RIM evaluation methods

Common	**RIM ASME XI, Div. 2**	**FMEA Center for Chemical Process Safety**	**IEC 60812 International Electrotechnical Commission (IEC)**	**FMECA MIL STD 1629A**	**RAM Army Regulation 702-19**	**RAMI ANS Fusion Science and Technology**	**PSD-1 ASME (Draft)**
Define scope	Define RIM Scope	Defining the study problem	Plan the FMEA/FMECA: scope, boundaries, decision criteria, documentation requirements, and resources	Define the system to be analyzed.	The design activities planned and conducted should include:	**Functional Analysis**; functional breakdown of the system	**SEDI;** Systems Engineering Design Integration, incl.: **-** Technical requirements definition - Functional architecture development - Physical architecture development - Physical design - V&V planning
Identify items		Performing review; equipment identification, equipment description		Construct block diagrams.	(1) Reliability and maintainability allocations, block diagrams and predictions.		
Perform analysis	Assess Degradation Mechanisms	Performing the review; failure modes, effects, safeguards, actions	Perform FMEA: process into elements; identify functions, performance standards, failure modes, detection methods and existing controls, effects of failure modes, failure causes; determine severity; estimate likelihood and other criticality parameters; and identify actions	Identify all potential item and interface failure modes and define their effect	(2) Refining the failure definition and scoring criteria that provides reliability failure definitions and functionality thresholds applied during reliability design, testing, and assessment.	**FMECA**; identifies all the failure modes of the components used to carry out the functions; it also evaluates the mode failure rate and the mean time to restore the components	**PRE;** Plant Risk Evaluation, incl. - hazard identification - event sequences identification - event likelihood evaluation-consequence evaluation - risk characterization

Common	**RIM** **ASME XI, Div. 2**	**FMEA** **Center for Chemical Process Safety**	**IEC 60812** **International Electrotechnical Commission (IEC)**	**FMECA** **MIL STD 1629A**	**RAM** **Army Regulation 702-19**	**RAMI** **ANS Fusion Science and Technology**	**PSD-1** **ASME (Draft)**
Evaluate risk	Identify Plant/SSC Target Reliabilities			Evaluate each failure mode in terms of the worst potential consequences Identify failure detection methods and compensating provisions for each failure mode	(3) Estimation of operational and environmental life cycle loads. (4) Engineering or physics-based models in order to identify potential failure mechanisms and the resulting failure modes. (5) Failure Mode, Effects and Criticality Analysis.	**RBD**; reliability block diagram analysis; calculates availability of the system's functions. If availability does not meet the acceptance criteria, mitigation actions are then considered, and a new cycle of analyses is performed until an acceptable availability is achieved	
		N/A	Evaluates relative importance of failure modes, determines severity of final effect (consequence), and estimates likelihood of failure mode	[The FMEA] … analysis shall also be used to assess high risk items … minimize failure risk	Classify each potential failure mode according to its severity or risk probability number.	Focus is on schedule risk	**PRE;** Plant Risk Evaluation, incl. - risk acceptability determination - identification of additional barriers - availability target determination
Identify corrective actions	Establish RIM Strategies	Performing the review; actions	Identifies treatment options	Identify corrective design or other actions required to eliminate the failure or control the risk	(6) Maintainability analysis and demonstrations.		

Common	RIM ASME XI, Div. 2	FMEA Center for Chemical Process Safety	IEC 60812 International Electrotechnical Commission (IEC)	FMECA MIL STD 1629A	RAM Army Regulation 702-19	RAMI ANS Fusion Science and Technology	PSD-1 ASME (Draft)
	Evaluate Uncertainties			Identify effects of corrective actions or other system attributes, such as requirements for logistics support			
Implement corrective actions	Implement RIM Program		Perform actions & re-evaluate risk		(7) Reliability testing including growth at the system and subsystem level.		
Monitor results	Perform Monitoring and RIM Program Updates		Distribute, review & update analysis		(8) Failure reporting and corrective action system.		