INL-EXT-19-55808

Light Water Reactor Sustainability Program

Plant Integral Risk-informed System Health Program

September 2019

U.S. Department of Energy

Office of Nuclear Energy

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-EXT-19-55808

Plant Integral Risk-informed System Health Program

D. Mandelli, Z. Ma, R. Youngblood, S. St Germain, C. Smith, P. Talbot
(Idaho National Laboratory)

S. Hess, D. Dube (Jensen Hughes)

C. Pope, J. Miller, M. Robbins (Idaho State University)

D. Das, M. Azarian (University of Maryland)

J. Coble (University of Tennessee-Knoxville)

September 2019

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

EXECUTIVE SUMMARY

Industry Equipment Reliability (ER) programs are an essential element that support safe and economic plant operations. The effectiveness of these programs is addressed in several industry-wide and regulatory programs. However, as currently implemented, these programs are labor intensive and expensive. There is an acute industry need to leverage advanced monitoring technology (including pattern recognition, diagnostics, and prognostics) to reduce costs and improve engineering effectiveness. Although the use of advanced monitoring has been successfully implemented to assess equipment and system performance in a number of industries (e.g., commercial and military aviation, transportation, gas turbine electrical generation), these technologies have not penetrated extensively into the commercial nuclear power sector. As a result, deployment of these technologies has the potential to provide significant improvements in the performance of critical Structures, Systems and Components (SSCs) (e.g., via detection and diagnosis of degraded performance at an incipient stage) and reduce costs associated with monitoring and regulatory compliance.

The objective of this project is to leverage advanced computational capabilities to support enhanced system performance and health management. A fundamental objective of this effort is to integrate various elements of system health monitoring, management, and reporting in a manner that is significantly less labor intensive and is at least as technically effective as current programs. This will be accomplished by integrating various elements of system health monitoring, management, and reporting in a manner that is significantly less labor intensive and is at least as technically effective as current programs. The final goal is to manage equipment and system performance and its financial risk and reduce costs associated with monitoring and regulatory compliance.

This report summarizes the activities of the Plant Health Management (PHM) project which started in October 2018 in response to the need to develop data analytics tools coupled with risk-informed methods to manage nuclear power plant health. The first application of this project targets the integration of risk-informed applications with the plant system health program. The goals are essentially the following: 1) apply innovative data analytics methods to assess component/system health, and, 2) link the system health program with risk models. These goals are designed to target the fact that the U.S. commercial nuclear power industry is aggressively pursuing implementation of several risk-informed applications to reduce regulatory burden and operating costs. These applications include Alternative Treatments (10CFR50.69) and Risk-Managed Technical Specifications (TSTF-505). To obtain maximum value from these applications, their execution must be strongly integrated with a robust and automated System

Health program. While typically plant risk models focus only on the safety aspects of the plant, we are extending plant risk models to include the economic plant risk.

The overall outcome of this work will be a framework that will apply plant health data to provide actual risk (both safety and economic) information that can support more informed and effective decision-making. Risk-informed applications are linked to this analysis framework by identifying their direct impact on plant risk models. The foreseen outcomes of this framework are: 1) the reduction of nuclear power plant owner resources to manage equipment reliability, and, 2) the ability to provide, in real time, assessments of the safety and economical risks associated with plant equipment as plant configuration changes.

CONTENTS

FIGURES

TABLES

ACRONYMS

AC	Alternate Current
AIT	Augmented Inspection Team
AOT	Allowed Outage Time
API	Application Programming Interface
ASME	American Society for Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BPV	Boiler and Pressure Vessel
BWR	Boiling Water Reactor
CDF	Core Damage Frequency
CM	Corrective maintenance
CST	Condensate Storage Tank
DNP	Delivering the Nuclear Promise
DOE	Department of Energy
ECCS	Emergency Core Cooling Systems
EER	Economic Enterprise Risk
EFPH	Effective Full Power Hours
EHC	Electro-Hydraulic Control
EPIX	Equipment Performance and Information Exchange
EPRI	Electric Power Research Institute
ER	Equipment Reliability
ERWG	Equipment Reliability Working Group
ET	Event Tree
FEG	Functional Equipment Group
FIELD	FANUC's Intelligent Drive Link Drive
FMEA	Failure Modes and Effects Analysis
FMMEA	Failure Modes, Mechanisms, and Effects Analysis
FT	Fault Tree
FV	Fussell-Vesely
HPCI	High Pressure Coolant Injection
HSS	High Safety Significance
HUMS	Health and Usage Monitoring
ICCDP	Incremental Conditional Core Damage Probability

ICLERP	Incremental Increase in Large Early Release Probability
IDP	Decision-Making Panel
IEC	International Electrotechnical Commission
IIT	Incident Investigation Team
ILCM	Integrated Life Cycle Management
IMC	Inspection Manual Chapter
INL	Idaho National Laboratory
INPO	Institute of Nuclear Power Operations
IoT	Internet of Things
IR	Issue Report
IVHM	Integrated Vehicle Health Management
JH	Jensen Hughes
KPI	Key Performance Indicator
LCM	Life Cycle Management
LERF	Large Early Release Frequency
LHS	Latin Hypercube System
LSS	Low Safety Significance
LWRS	Light Water Reactor Sustainability
MCS	Minimal Cut Set
MCSA	Motor Current Signature Analysis
MFW	Main Feedwater
MPFF	Maintenance Preventable Functional Failures
MPSA	Motor Power Signature Analysis
MSET	Multivariate State Estimation Technique
MSIV	Main Steam Isolation Valve
MSPI	Mitigating Systems Performance Index
MTE	Molecular Test Equipment
MTTD	Mean Time To Degradation
MTTF	Meant Time To Failure
MTTR	Meant Time To Repair
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NPSH	Net Positive Suction Head
NPV	Net Present Value

NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
NUMARC	Nuclear Management and Resources Council
OOS	Out-Of-Service
O&M	Operation and Maintenance
PCDF	Product’s Construction Data Form
PHM	Plant Health Management
PI	Performance Indicator
PM	Preventive maintenance
PMDB	Preventive Maintenance Basis Database
PoF	Physics of Failure
PRA	Probabilistic Risk Assessment
PSH	Plant System Health
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
QCM	Quiescent Current Monitor
RAM	Reliability, Availability, and Maintainability
RAVEN	Risk Analysis Virtual Environment
RAW	Risk Achievement Worth
RCIC	Reactor Core Isolation Cooling
RCM	Reliability Centered Maintenance
RG	Regulatory Guide
RI	Risk-Informed
RIAM	Risk-Informed Asset Management
RICT	Risk-Informed Completion Time
RIDM	Risk-Informed Decision-Making
RISA	Risk Informed Safety Analysis
RI-PSH	Risk Informed Plant System Health
RI-ISI	Risk-Informed In-Service Inspection (of piping)
RMTS	Risk-Managed Technical Specifications
RNN	Recurrent Neural Network
ROP	Reactor Oversight Process
RRW	Risk Reduction Worth
RUL	Remaining Useful Life
R&D	Research and Development

SAMA	Severe Accident Mitigation Alternative
SBO	Station Blackout
SCS	Supply Chain Surveillance
SDP	Significance Determination Process
SFCP	Surveillance Frequency Control Program
SIT	Special Inspection Team
SLR	Second License Renewal
SMART	Self-Monitoring Analysis And Reporting Technology
SP	Suppression Pool
SPRT	Sequential Probability Ratio Test
SQA	Software Quality Assurance
SSCs	Structures, Systems, and Components
STI	Surveillance Test Intervals
SVM	Support Vector Machine
SVP	Single Point Vulnerability
TDR	Time Domain Reflectometry
TS	Technical Specification
TTF	Time To Failure
TS	Technical Specifications
T&M	Testing and Maintenance
WO	Work Orders
VBM	Value Based Maintenance

Plant Integral Risk-Informed System Health Program

1. INTRODUCTION

Industry Equipment Reliability (ER) programs are an essential element that support the safe and economic plant operation of all commercial Nuclear Power Plants (NPPs). The effectiveness of these programs is addressed in several industry-wide and regulatory programs. For example, U.S. NPPs have implemented the ER process defined in INPO AP-913 "Equipment Reliability Process Description" (see Section 2). Additionally, performance of plant Structures, Systems, and Components (SSCs) is monitored within a regulatory context within the Maintenance Rule (10 CFR 50.65) and the Mitigating Systems Performance Index (MSPI) program. However, as currently implemented, these programs are labor intensive and expensive to perform and maintain.

In management of system health, utilities focus on achieving an optimization between the reliability and availability of plant SSCs while simultaneously minimizing costs. Over the 40+ years of commercial NPP operation, numerous approaches have been implemented to achieve this balance. The most recent of these, Value Based Maintenance (VBM), has been adopted across the industry as a part of the Delivering the Nuclear Promise (DNP) initiative (see Section 2). A summary of the approaches used by the industry to manage system health, including VBM, will be presented in Section 7 of this report.

To achieve additional cost reductions and improvements in plant safety and economic performance, there is an industry need to leverage advanced methods to reduce costs and improve engineering effectiveness. Although the use of advanced monitoring has been successfully implemented to assess equipment and system performance in a number of industries (e.g. commercial and military aviation, transportation, gas turbine electrical generation), these technologies have not penetrated extensively into the commercial nuclear power sector. As a result, deployment of these technologies has the potential to provide significant improvements in the performance of critical SSCs (e.g., via detection and diagnosis of degraded performance at an incipient stage) and reduce costs associated with monitoring and regulatory compliance.

As part of implementing VBM, the host utility for this research project indicated that they were pursuing the use of a modeling and simulation approach to evaluate the entire planned maintenance process. A fundamental question that was posed is: could they translate cost information into a metric that is representative of SSC health? Such an approach would allow addressing both Operation and Maintenance (O&M) costs (by leveraging information infrastructure) to reduce engineering analysis needed to assess SSC health impacts and also generate better short-term and long-term cost projections. The host utility also indicated that improved user-friendly data analytics are needed as a tool to allow decisions to be made without requiring engineering personnel to be involved in each assessment and decision. This was considered by the host utility to be crucial to achieving additional cost reductions.

This research project is intended to provide an initial development and demonstration of a Risk-Informed Plant System Health (RI-PSH) management process and automation tools that can be integrated with an existing plant system health program. The objective is to leverage advanced computational capabilities to support enhanced system performance and health management. A fundamental objective of this effort is to integrate various elements of system health monitoring, management, and reporting in a manner that is significantly less labor intensive and is at least as technically effective as current programs.

The overall approach (see Figure 1) for this project during Fiscal Year (FY) 19 and FY20 targets the following items:

1) integration of system health program and risk-informed applications
2) integration of equipment failure data/models with the existing plant system health program
3) integration of equipment diagnostics and prognostics to system health

The overall objective of this effort will be to develop and deploy an integrated plant system health program that maximizes automation and advanced data analytics to minimize cost and enhance performance. This is accomplished by providing timely high-quality information to decision makers that characterizes all aspects of system health, including uncertainties and risks.

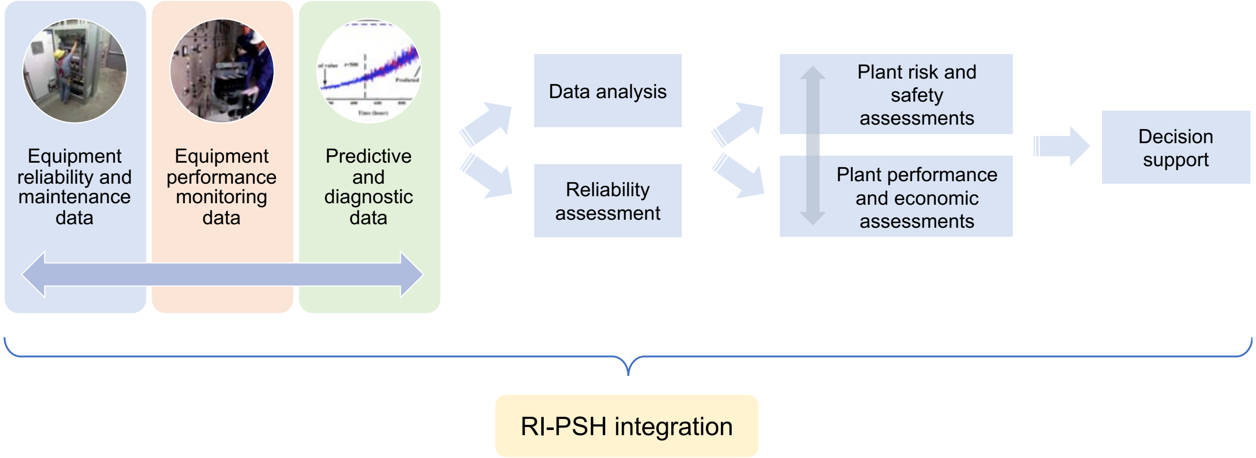

Equipment reliability and maintenance data
Equipment performance monitoring data
Predictive and diagnostic data
Data analysis
Reliability assessment
Plant risk and safety assessments
Plant performance and economic assessments
Decision support
RI-PSH integration

Figure 1. High level diagram of the RI-PSH program elements.

The research described in this report targets the collaboration with the host utility to conduct initial work to target item 1. The objective of this portion of the research is to retrieve equipment performance and monitoring data to update existing models and processes to support Risk-Informed Decision-Making (RIDM) across the host utility's operating NPPs. It should be noted that, in the context of the RISA approach, RIDM incorporates a broad interpretation of risks to include not only the traditional focus on nuclear safety (as evaluated in a plant PRA), but also broader elements of risk such as financial aspects.

A longer-term objective of this research is to employ equipment performance and monitoring to create SSC ageing models. Such models will be employed to predict SSC Remaining Useful Life (RUL). Once these models are available, plant economic risk models will be developed with the objective to identify plant risks (from an economic perspective). The near-term objective is to develop basic models and validate them using plant data provided by the host utility. This will set the stage for initial deployment in one or more pilot applications at host utility sites to support real time analysis and decision-making. For this initial application, a specific plant pilot system was identified with analysis performed focusing on that system while keeping the development generic for future applications on other systems and plants.

The following specific tasks were performed and are described in this report.

- Task 1: System identification and characterization. In collaboration with the host utility, pilot systems were selected at one of their operating NPPs
- Task 2: Selection of plant data. Failure, unavailability, and cost data were gathered from the selected power plant for the system(s) chosen in Task 1. The operating data were reviewed and characterized to support further analysis

- Task 3: Identification of system analytics methods and SSC reliability models. For a specific subset of components for the system(s) chosen in Task 1, system analytics methods and SSC reliability models were investigated and tested using the processed data from Task 2
- Task 4: Evaluate outcomes and develop plan for pilot process for integrated system health management

The results from the assessments and evaluations conducted in Tasks 2 and 3 were reviewed with the host utility to identify applicable insights and develop an appropriate path forward which will be conducted in Fiscal Year 20.

1.1 PHM Project Structure

In order to proceed with the creation of a comprehensive RI-PSH framework which can assist plant owners to identify risk associated to the operating plant, we investigated several components of the scheme shown in Figure 1. In the main structure of the report we have reported the highlights of our work while we have reported in the appendices the technical details of our development/analysis. Each section and appendix of this report is linked to this scheme as shown in Figure 2. Note that we have expanded the decision support block of Figure 1 by expanding it into two categories: maintenance and asset management.

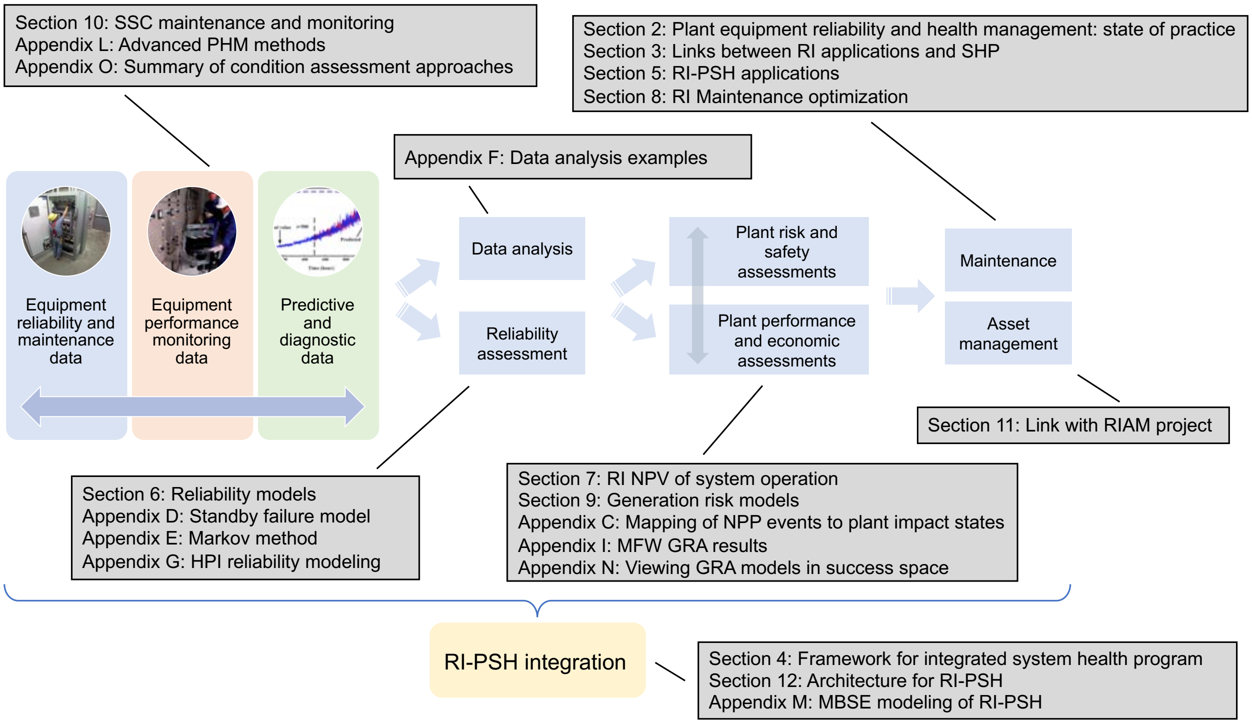

Section 10: SSC maintenance and monitoring
Appendix L: Advanced PHM methods
Appendix O: Summary of condition assessment approaches
Section 2: Plant equipment reliability and health management: state of practice
Section 3: Links between RI applications and SHP
Section 5: RI-PSH applications
Section 8: RI Maintenance optimization
Appendix F: Data analysis examples
Equipment reliability and maintenance data
Equipment performance monitoring data
Predictive and diagnostic data
Data analysis
Reliability assessment
Plant risk and safety assessments
Plant performance and economic assessments
Maintenance
Asset management
Section 11: Link with RIAM project
Section 6: Reliability models
Appendix D: Standby failure model
Appendix E: Markov method
Appendix G: HPI reliability modeling
Section 7: RI NPV of system operation
Section 9: Generation risk models
Appendix C: Mapping of NPP events to plant impact states
Appendix I: MFW GRA results
Appendix N: Viewing GRA models in success space
RI-PSH integration
Section 4: Framework for integrated system health program
Section 12: Architecture for RI-PSH
Appendix M: MBSE modeling of RI-PSH

Figure 2. Structure of the report as function of the RI-PSH functional blocks.

2. PLANT EQUIPMENT RELIABILITY AND HEALTH MANAGEMENT: STATE OF PRACTICE

In the United States, the impact of plant equipment reliability and system health on safety is regulated by 10CFR50.65 (the Maintenance Rule) [1]. Implementation of this rule at operating NPPs across the industry follows guidance provided in NEI 93-01 “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants” [2] which has been endorsed by the Nuclear Regulatory Commission (NRC) in Regulatory Guide 1.160 [3] as providing an approach that is acceptable to the NRC for NPPs to meet the requirements of the rule. The implementation guidance requires the following activities:

- Identification of plant SSCs within the scope of the rule
- Establishing applicable risk and performance criteria
- Setting appropriate performance goals and monitoring SSC performance
- Ensuring conduct of an effective preventive maintenance (PM) program
- Evaluation of the plant risk impacts that result from the performance of maintenance activities
- Conducting periodic assessments of maintenance effectiveness

In addition to monitoring the performance of plant SSCs within the scope of the Maintenance Rule, additional monitoring also is required as part of the Mitigating Systems Performance Index (MSPI) program [4]. As currently implemented, these programs are labor intensive and expensive and there is an acute industry need to leverage advanced technologies to reduce costs and improve engineering effectiveness.

In the management of system health at operating NPPs, the Institute of Nuclear Power Operations (INPO) “Equipment Reliability Process Description,” AP-913, provides a common set of requirements and bases that are applied to the plant equipment reliability process [5]. This document serves as the primary detailed guidance used by the industry in plant Equipment Reliability (ER) programs. However, because AP-913 is a proprietary document, the following descriptions of its contents are limited to information that can be obtained from publicly available sources.

The basic elements of a plant ER process described in INPO AP-913 consists of six basic elements [6] as shown in Figure 3:

- Scoping and identification of critical components
- Performance monitoring
- Preventive maintenance (PM) implementation
- Corrective action
- Continuing equipment reliability improvement
- Life cycle management (LCM)

In NPP ER programs, a fundamental activity is the identification of components that are critical to plant safety and operations. Over the years, a number of approaches have been taken by the industry to identify which plant SSCs are considered to be critical. In the late 1980’s through early 1990’s use of Reliability Centered Maintenance (RCM) techniques were widely applied. Initial pilot applications across the industry were performed under the sponsorship of the Electric Power Research Institute (EPRI) [7]. Application of the complete RCM process (as initially developed and applied in the commercial aviation industry) in these pilot plant applications was considered too time consuming, resource intensive, and expensive to perform. As a result, industry investigated methods to address these impediments. This lead to the development of Streamlined RCM (S-RCM) approaches which were more fully adopted by the industry [8]. The development of streamed approaches to identify critical plant SSCs and deploy cost-effective Preventive Maintenance (PM) programs has continued to the present time.

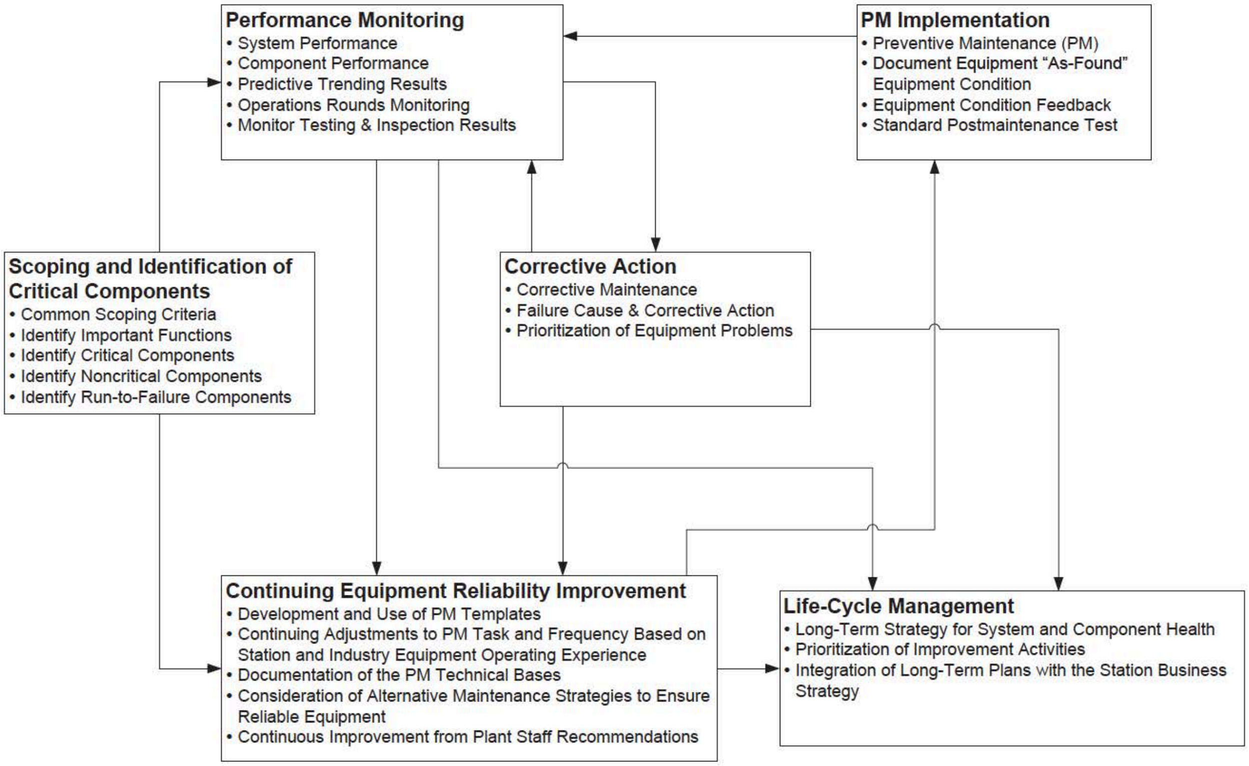

Performance Monitoring
• System Performance
• Component Performance
• Predictive Trending Results
• Operations Rounds Monitoring
• Monitor Testing & Inspection Results
PM Implementation
• Preventive Maintenance (PM)
• Document Equipment "As-Found" Equipment Condition
• Equipment Condition Feedback
• Standard Postmaintenance Test
Scoping and Identification of Critical Components
• Common Scoping Criteria
• Identify Important Functions
• Identify Critical Components
• Identify Noncritical Components
• Identify Run-to-Failure Components
Corrective Action
• Corrective Maintenance
• Failure Cause & Corrective Action
• Prioritization of Equipment Problems
Continuing Equipment Reliability Improvement
• Development and Use of PM Templates
• Continuing Adjustments to PM Task and Frequency Based on Station and Industry Equipment Operating Experience
• Documentation of the PM Technical Bases
• Consideration of Alternative Maintenance Strategies to Ensure Reliable Equipment
• Continuous Improvement from Plant Staff Recommendations
Life-Cycle Management
• Long-Term Strategy for System and Component Health
• Prioritization of Improvement Activities
• Integration of Long-Term Plans with the Station Business Strategy

Figure 3. Nuclear power plant equipment reliability process [6].

One of the outcomes of the evolution of PM programs in the industry is that the definition of what makes a particular SSC critical was, to some extent, a decision made by each plant. Over the past several decades, work performed by the industry Equipment Reliability Working Group (ERWG) developed additional guidelines for these decisions which were incorporated into AP-913. Recently, as part of the Delivering the Nuclear Promise (DNP) initiative, the industry reviewed industry performance and developed a revised set of criteria that were to be used by all operating NPPs to specify which SSCs would be classified as critical. These criteria were published by the Nuclear Energy Institute (NEI) as an Efficiency Bulletin (EB) with operating plants assigned a due date for completion and report back. The criticality criteria provided in the EB [9] are as follows:

- A credible single active component failure that will directly result in any of the following consequences:
  - Reactor scram/trip (referred to as a Single Point Vulnerability – SPV)
  - Significant power transient of greater than 20 percent (Operational Loss Event – OLE)
  - MSPI monitored component failure
  - Any single failure that causes a complete loss of any of the following critical safety functions:
    - Core, reactor coolant system or spent fuel pool heat removal
    - Containment isolation, temperature, pressure
    - Reactivity control
    - Vital AC electrical power
- A single equipment failure that results in the loss of a Maintenance Rule high-safety-significant (HSS) or risk-significant function.

The EB directed all U.S. NPPs to revise applicable fleet/station processes and procedures to incorporate the new criticality definition and to implement the changes through a dedicated, cross-functional team to identify the subset of critical components that can be reclassified as noncritical with a completion date of June 2017. Note that AP-913 also was revised to reflect these changes.

A second element of ensuring high levels of performance (including availability and reliability of plant SSCs) is the implementation of a cost-effective PM program. NPP PM programs have evolved over the years. During the initial application of RCM techniques, an approach using maintenance templates was developed and achieved widespread adoption across the industry [8]. This approach also began a transition from traditional time-based PMs (e.g., overhauls) to much more extensive use of condition-based PMs that employ various monitoring technologies (e.g., vibration, thermographic, and oil/lubrication analysis) to determine when conditions exist that warrant performance of intrusive maintenance activities. In response to these evolutions, the EPRI developed the Preventive Maintenance Basis Database (PMBD) software application [10] to permit NPPs to more efficiently develop, assess, and modify plant PM programs. This software is proprietary and available only to EPRI members. However, a "Quick Start" guide for the PMBD that is publicly available has been published by EPRI [11]. This "Quick Start" guide provides an overview of the tool's capabilities and functionality.

Over time, industry performance has increased substantially, both in terms of safety and operational performance (e.g. increased plant capacity factors). This was demonstrated in a recent EPRI study [12] that showed an increasing trend in average plant capacity factor (from ~70% in 1992 to 85% to 90% since ~2005) while displaying a significant improvement in safety as measured by an ~80% reduction in calculated Core Damage Frequency (CDF) over this same period of time. Figure 4 (taken from the EPRI report [12]) graphically depicts this improvement. However, at the same time that these performance improvements were occurring, there has been a commensurate increase in operational and maintenance costs. This situation led to the industry developing a Value Based Maintenance (VBM) process to reduce costs while simultaneously maintaining current high levels of performance and safety. VBM also was disseminated to the industry via an NEI Efficiency Bulletin with operating plants assigned a due date for completion and report back [13].

VBM has the objective of "changing the industry's culture of *reliability at any cost* and *more is better* to one where maintenance is treated as a highly valued and limited resource (that) is key to advancing safety and reliability in a cost-effective manner". The VBM initiative is complementary to the critical component definition (described in EB 16-25). The transition to VBM is intended to achieve more cost-effective maintenance strategies for those components whose failures do not result in the consequences identified in EB 16-25 as indicated above.

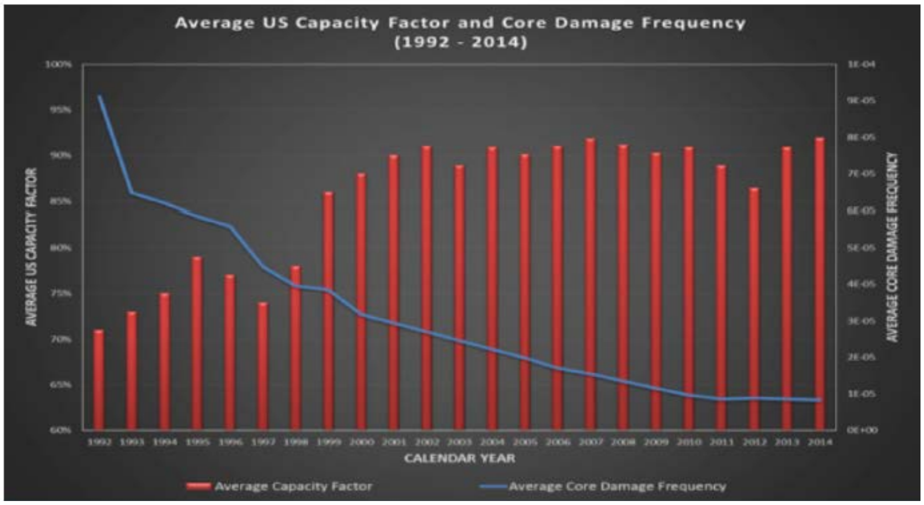


Figure 4. Trends in nuclear capacity factors and core damage frequencies (from [12]).

VBM provides a maintenance strategy that is intended to optimize safety and reliability while aggressively managing the cost of component maintenance. The approach requires evaluation of possible adverse costs caused by a resulting increase in failure rates associated with a change in a maintenance strategy for a particular SSC. The approach recognizes that simply reducing the number of PMs likely will not reduce costs if it results in a corresponding increase in corrective maintenance, reduced plant safety or system reliability, or increased regulatory scrutiny. The VBM approach is intended to transition from a point of maximum SSC reliability to a point of minimum total maintenance cost as shown in Figure 5. Note that the key to this approach is that the emphasis is on implementing a holistic maintenance program that minimizes total maintenance costs.

Another area related to plant ER programs is that related to monitoring and reporting of performance. The areas of system and program health reporting are critical for communicating issues related to plant system performance and ensuring that appropriate levels of system performance, reliability, and availability are maintained. Because this area is critical to decision-making, it has developed into a process at operating NPPs which require extensive time and administrative support to accomplish. This situation was identified during the DNP effort. As a result, two separate Efficiency Bulletins were developed that have the objectives of significantly reducing the cost and administrative burdens associated with system health reporting (EB 16-33) [14] and plant program health reporting (EB 16-34) [15].

Both of these Efficiency Bulletins provide a graded approach to health reporting. Each prescribes decreasing levels of reporting requirements as the functional importance of the system or the impact of the program on plant risk/safety/production decreases. The system health reporting Efficiency Bulletin EB 16-33 [14] characterizes plant systems into three "tiers" based on functional importance. The identified system classifications are as follows:

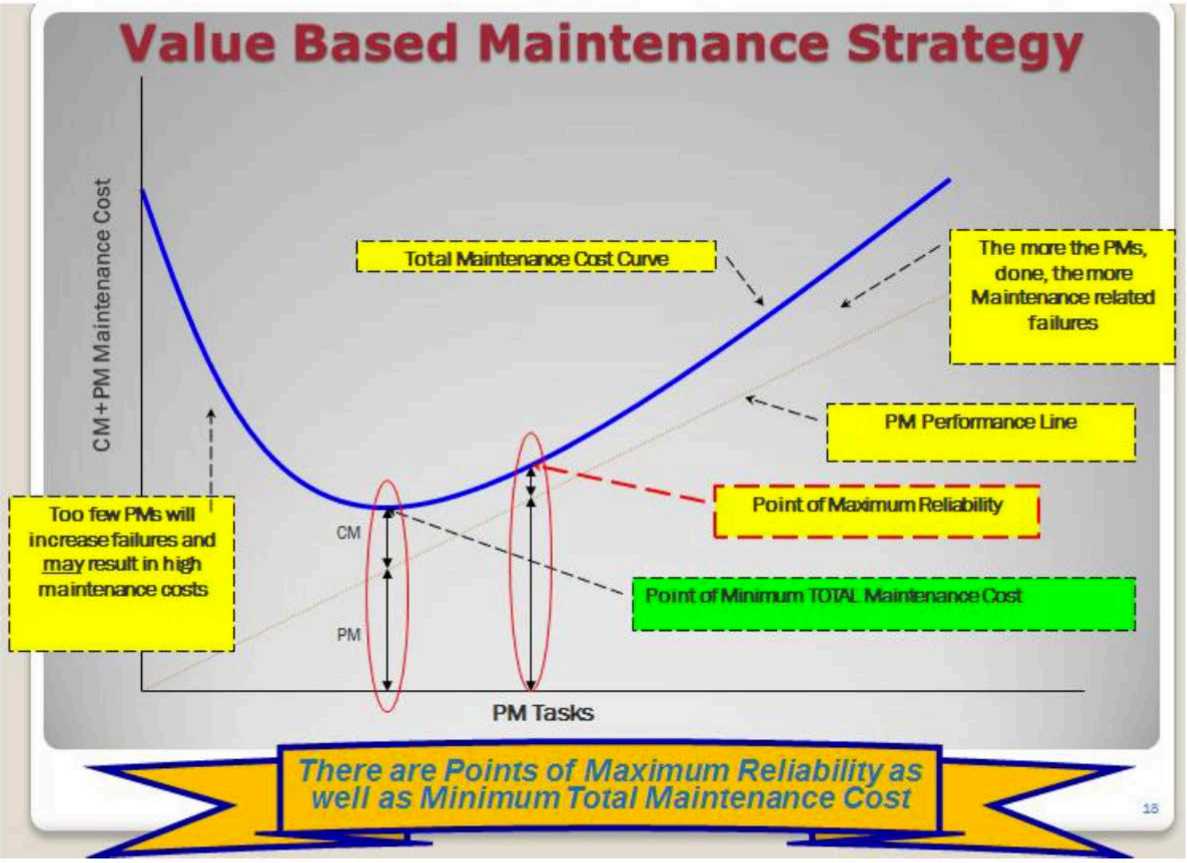
- Tier 1 systems are the most important to nuclear safety and plant reliability:
  - MSPI systems
  - Scram Vulnerable Systems
    - Condensate & Feedwater (including main condenser)
    - Main Turbine (including auxiliary systems)
    - Main Generator (including auxiliary systems) Electrical Distribution systems. (including transformers/switchyard)
    - Reactor Recirculation/Reactor Coolant
- Tier 2 systems also are important from a nuclear safety, plant reliability and risk standpoint but do not meet the Tier 1 criteria:
  - Systems with critical components as defined in AP-913 Revision 5.
  - Systems with high safety significant/risk significant components/functions that do not meet the criteria in Tier 1.
- Tier 3 systems are those that do not meet the criteria of either Tier 1 or Tier 2.

A similar classification system is presented for plant programs in the plant health reporting Efficiency Bulletin EB 16-34 [15]. The identified system classifications are as follows:

- Tier 1 typically are complex programs with potential for high consequence failures. These programs apply standard industry scorecards with indicators in each of four cornerstones (personnel, infrastructure, implementation, and equipment). Each Tier 1 program has an assigned owner at each plant (or across the fleet).
- Tier 2 programs also have assigned program owners. Program health is monitored through a set of standard industry Key Performance Indicators (KPIs) that should be reviewed at least annually or following each refueling outage.

- Tier 3 programs are managed through station procedures but do not always have an assigned program owner. Use of KPIs for these programs is at the discretion of the utility.

Attachment 1 to EB 16-34 provides examples of program health scorecards for several different programs.



Value Based Maintenance Strategy

There are Points of Maximum Reliability as well as Minimum Total Maintenance Cost

Figure 5. VBM strategy (from [13]).

3. LINKS BETWEEN RISK-INFORMED APPLICATIONS AND SYSTEM HEALTH

We define System Health here as the integrated assessment of NPP equipment performance and condition within the context of system functions. Some of the key objectives of a System Health program include:

- Implementation of a graded approach to equipment reliability
- Balancing the cost of maintaining equipment with industry and station goals for safety and reliability
- Eliminating critical component failures
- Maintaining acceptable levels of reliability for noncritical components based on their importance to safety, reliability and business objectives.

The health of a system can be measured in many ways, but we focus on the following key attributes:

- Reliability
- Availability
- Performance according to plant design and Technical Specifications
- Aggregated risk and environmental impact
- Corrective action history and backlog (i.e., a measure of equipment condition and economic performance)
- Operator burdens and operator workarounds for the system
- Ageing and obsolescence issues.

Here, aggregated risk and environmental impact refers to the effect that an unreliable but high-importance system may have on risk measures such as CDF and Large Early Release Frequency (LERF) because the system could be in a state of disrepair when called upon to perform its intended function. Operator burdens and workarounds refer to the substitution of operator actions or procedural measures for permanent fixes when a SSC is in a degraded state. In Section 3.1 we illustrate the link between ER processes within the larger context of System Health and risk-informed applications.

3.1 Links Between Equipment Reliability Processes and Risk-Informed Applications

There is a strong link between ER processes and Risk-Informed (RI) applications as illustrated in Figure 6. The key ER processes are implemented through a series of guidance documents prepared by industry organizations including INPO; NEI and its predecessor, the Nuclear Management and Resources Council (NUMARC); and EPRI. Many RI applications can be categorized as those that are primarily regulatory-driven through regulation or NRC programs including the Reactor Oversight Process (ROP). The ROP is the NRC's program to inspect, measure, and assess the safety and security performance of operating commercial NPPs, and to respond to any decline in their performance.

A second category of RI applications is designated as more voluntary in nature. The decision to move forward with any of these programs is determined by each individual licensee. Guidance documents are provided by the NRC, industry, or a combination of the two to provide consistency in the application and implementation of the risk-informed activity. Further discussion is provided below. Appendix B provides a summary of the considered RI applications.

3.2 Equipment Reliability Processes

There are many ER programs and processes to ensure safe and reliable nuclear power generation. Central to many of the guidance documents is INPO's AP-913 [5] that provides a compendium of resources for maintaining equipment reliability and performance. The process description in AP-913 reflects the experience gained from equipment performance assistance visits to operating plants and benchmarking trips to domestic and international utilities. The equipment reliability process was designed with the direct participation of the Equipment Reliability Working Group (ERWG) actively involved in improving processes. However, because AP-913 is a proprietary document, the descriptions of its contents provided there are limited to information that can be obtained from publicly available sources.

NUMARC 93-01 [16] was developed in the 1990s to assist the industry in implementing the Maintenance Rule specified under 10 CFR 50.65 [1] and to build on the significant progress, programs and facilities that had been established at operating NPPs to improve maintenance. The guideline provides a process for deciding which of the many SSCs that make up a commercial NPP are within the scope of the

Maintenance Rule. It then describes the process of establishing plant-specific risk significance and performance criteria to be used to decide if goals need to be established for specific SSCs covered by the Maintenance Rule when it is determined that they do not meet their specified performance criteria. A proposed alternative to the current Maintenance Rule, or Maintenance Rule 2.0 as often referred to, has the potential to streamline and better focus plant maintenance but would not fundamentally change the importance of the Maintenance Rule [18].

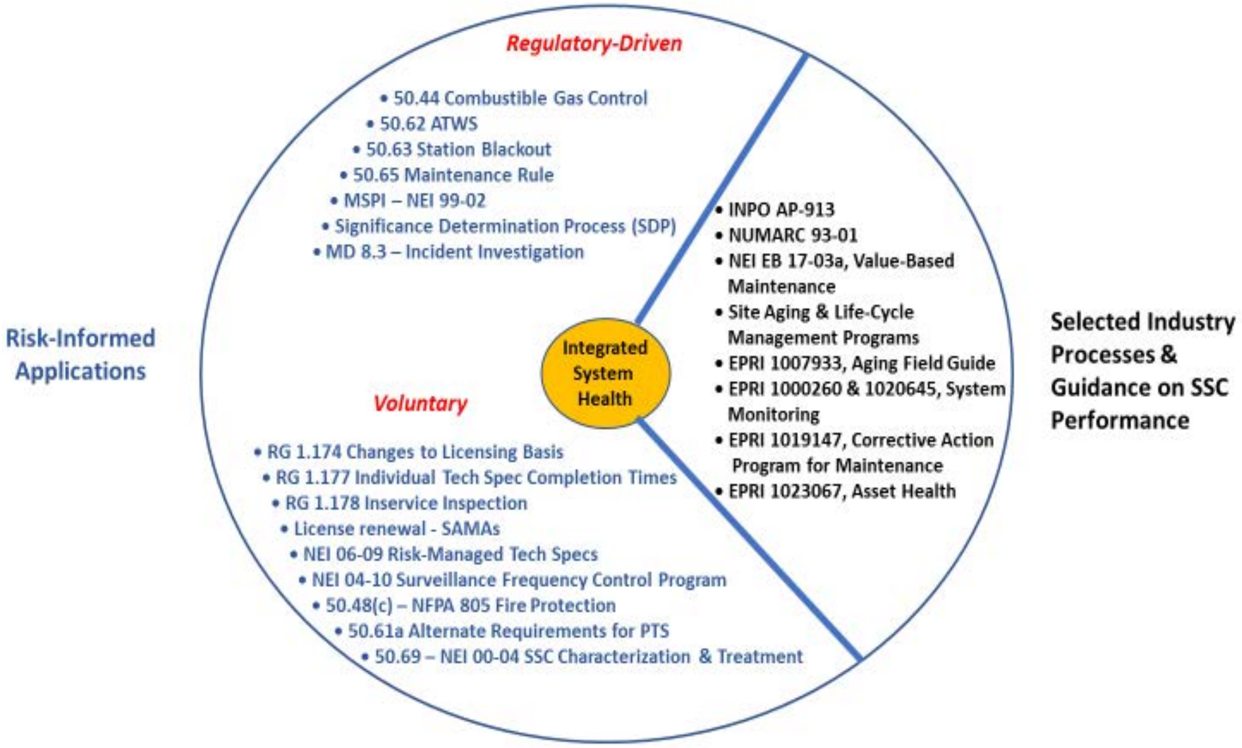

Regulatory-Driven
• 50.44 Combustible Gas Control
• 50.62 ATWS
• 50.63 Station Blackout
• 50.65 Maintenance Rule
• MSPI – NEI 99-02
• Significance Determination Process (SDP)
• MD 8.3 – Incident Investigation
Risk-Informed Applications
Integrated System Health
Voluntary
• RG 1.174 Changes to Licensing Basis
• RG 1.177 Individual Tech Spec Completion Times
• RG 1.178 Inservice Inspection
• License renewal - SAMAs
• NEI 06-09 Risk-Managed Tech Specs
• NEI 04-10 Surveillance Frequency Control Program
• 50.48(c) – NFPA 805 Fire Protection
• 50.61a Alternate Requirements for PTS
• 50.69 – NEI 00-04 SSC Characterization & Treatment
• INPO AP-913
• NUMARC 93-01
• NEI EB 17-03a, Value-Based Maintenance
• Site Aging & Life-Cycle Management Programs
• EPRI 1007933, Aging Field Guide
• EPRI 1000260 & 1020645, System Monitoring
• EPRI 1019147, Corrective Action Program for Maintenance
• EPRI 1023067, Asset Health
Selected Industry Processes & Guidance on SSC Performance

Figure 6. Relationship of RI applications and ER processes to system health.

3.3 Risk-Informed Applications

3.3.1 Regulatory-Driven Risk-Informed Applications

Regulatory-driven RI applications include regulations enacted in the 1980s and 1990s that were formulated largely on the basis of risk insights from early comprehensive risk studies. For example, 10 CFR 50.62, or the Anticipated Transient Without Scram (ATWS) Rule, was implemented considering reliability studies in the 1970s regarding the probability of common cause failures of the reactor trip function and the potentially adverse consequences that could result including fuel damage. The urgency of implementing the rule was highlighted in February 1983 by the Salem Nuclear Generating Station ATWS events. This was the first time a U.S. commercial NPP failed to scram automatically on a valid reactor protection signal. Fortunately, the plant was operating at low power levels on both occasions and minimal consequences resulted.

Similarly, early risk studies identified total loss of Alternating Current (AC) power resulting from loss of offsite power initiating events combined with failures of onsite emergency power sources as significant contributors to CDF. The Station Blackout (SBO) rule promulgated in the 1980s requires licensees to propose and justify an SBO coping duration based on their ability to: (1) maintain highly reliable onsite emergency ac electric power supplies; (2) ensure that the plants can cope with an SBO for some period of time based on the probability of an SBO at the site and the capability to restore power to the site; (3) develop procedures and conduct training to restore offsite and onsite emergency ac power should either become unavailable; and (4) if necessary, make modifications necessary to meet the SBO rule requirements.

Inspection Manual Chapter (IMC) 0305 describes NRC's Operating Reactor Assessment Program (ROP) [19]. The ROP integrates NRC's inspection, Performance Indicator (PI), assessment, and enforcement programs applicable to operating reactors. The ROP evaluates the overall performance of operating commercial NPPs and communicates this information to licensee management, members of the public, and other stakeholders. The ROP collects information from inspections and PIs to enable the NRC to develop objective conclusions about a licensee's safety performance.

To measure plant performance, the oversight program focuses on seven specific "cornerstones" which support the safety of plant operations in three broad strategic areas. These include such focus areas as initiating events, mitigating systems, barrier integrity, and others. Additionally, there are cross-cutting elements such as human performance that are evaluated.

Within each cornerstone, a broad sample of data on which to assess licensee performance in risk-significant areas is gathered from PI data submitted by licensees and from the NRC's risk-informed baseline inspections. The PIs are not intended to provide complete coverage of every aspect of plant design and operation, but they are intended to be indicative of performance within the related cornerstone.

The three specific RI processes usually associated with the ROP include:

- The mitigating systems performance index (MSPI) [20, 21]
- The significance determination process (SDP) for inspection findings [22]
- Management Directive 8.3, Incident Investigation Program [23]

The MSPI monitors the performance of selected NPP systems based on their ability to perform risk-significant functions. It provides a surrogate measure of the change in CDF resulting from departures of component unreliabilities and train unavailabilities from established baselines.

The SDP uses risk insights, where appropriate, to assist NRC staff in determining the safety or security significance of inspection findings identified within the seven cornerstones of safety at operating reactors. The SDP is a risk-informed process and the resulting safety or security significance of findings, combined with the results of the risk-informed performance indicator program, is used to determine a licensee's level of safety performance and the level of NRC engagement with the licensee.

The NRC defines "incident investigation" under MD 8.3 as a formal process conducted for the purpose of accident prevention. The process includes gathering and analyzing information; determining findings and conclusions, including the cause(s) of a significant event; and disseminating the investigation results for the NRC, industry, and public review.

While the MSPI is generated by licensees through the auspices of INPO software, both the SDP process and MD 8.3 are initiated by NRC staff on a case-by-case basis when a potentially risk-significant event or equipment failure occurs.

3.3.2 Voluntary Risk-Informed Applications

Voluntary RI applications, as highlighted in Figure 6, were developed with the intent of enhancing safety, improving operational effectiveness, or obtaining burden reduction [24]. Regulatory Guide (RG) 1.174 [25] describes the key principles and the overall process for risk-informed decision-making. These may be augmented by application-specific guidance for other processes such as risk-informed in-service inspection (RI-ISI) of piping under RG 1.178 [26] and associated industry documents. Additional voluntary RI applications include Risk-Managed Technical Specifications (RMTS) [27], Surveillance Frequency Control Program (SFCP) [28], and SSC characterization under 10 CFR 50.69 [29]. Key applications are discussed in greater detail in Section 5 of this report.

For license renewal, a Severe Accident Mitigation Alternative (SAMA) assessment is necessary to evaluate the cost-benefit of additional measures such as design changes and operations enhancement. The SAMA process is not discussed to any extent here. Likewise, we will not address here the performance-based standard for Fire Protection of light-water reactors under NFPA 805 [30] and alternate requirements for Pressurized Thermal Shock (PTS) of reactor pressure vessels under 10 CFR 50.61a [31].

3.4 Links to System Health

Table 1 shows the relationship between RI applications and key functions for nuclear power plant operations and sustainability. The regulatory-driven applications such as the ATWS, SBO, and ROP programs primarily maintain safe operations. The Maintenance Rule under 10CRF50.65, in addition to maintaining safe operations, serves to further improve plant and SSC reliability through the avoidance of reactor scrams.

The voluntary programs manage safe operations but may also support reliable plant operations. Furthermore, RI-ISI (of piping) under RG 1.178 (and associated industry guidance documents and Code Cases) is an example of an application that manages equipment ageing. Ageing can be managed specifically by addressing environmental stressors such as temperature, radiation, and moisture, and by managing operating stressors such as SSC cycling and vibration. Characterization and treatment of SSCs under 10CFR50.69 may provide the additional benefit of managing obsolescence through commercial procurement practices for obsolete safety-related equipment.

If the SSC is part of a monitored system in the MSPI, additional risk-related information may exist. Likewise, Maintenance-Rule related information also may be available. Table 1 also identifies how four of the most widely implemented voluntary applications relate to System Health, specifically:

- 10CFR50.69 SSC categorization
- SFCP per TSTF-425 and NEI 04-10
- RMTS per TSTF-505 and NEI 06-09
- RI-ISI per RG 1.178 and associated industry ASME Code Cases

These applications provide information that can be useful in assessing System Health.

Table 2 summarizes the key information on SSCs and how they relate to System Health in a broad sense. The key safety functions are standard and include such functions as reactivity control and containment integrity.

Table 1. High-level functions of risk-informed applications.

Risk-Informed Applications	**Manage Safe Operation**	**Manage Reliable Operation**	**Manage Equipment Ageing**		**Manage Obsolescence (critical spares, commercial procurement)**
			Manage Environmental Stressors (temperature, rad, moisture, etc.)	**Manage Operating Stressors (cycling, vibration)**	
Regulatory-Driven Processes					
ATWS, SBO, Combustible Gas Control	✓				
50.65 Maintenance Rule	✓	✓			
Reactor Oversight Process (MSPI, SDP, MD 8.3)	✓				
Voluntary Processes					
RG 1.174 Changes to Licensing Basis	✓	✓			
RG 1.177 Individual Tech Spec Completion Times	✓	✓			
RG 1.178 Inservice Inspection of Piping	✓	✓	✓	✓	
License renewal - SAMAs	✓				
NEI 06-09 Risk-Managed Tech Specs	✓	✓			
NEI 04-10 Surveillance Frequency Control Program	✓	✓		✓	
50.48(c) – NFPA 805 Fire Protection	✓				
50.61a Alternate Requirements for PTS	✓		✓	✓	
50.69 – NEI 00-04 SSC Characterization & Treatment	✓		✓	✓	✓

Core damage-related risk metrics include Risk Reduction Worth (RRW) and Risk Achievement Worth (RAW). Risk metrics such as RRW and RAW tell one how risk-important is the structure or component within a system to situations where the system might be degraded. For example, if the potable water system that provides drinking water to the site is degraded, it has no risk impact. If critical systems such as emergency ac power with high risk importance (i.e., RRW, RAW) are degraded, then the impact on system health can be significant.

Economic enterprise risk metrics are a relatively new concept and are derived from an economic risk model analogous to CDF-derived and LERF-derived Fussell-Vesely (FV) importance measures [32]. The metric denotes how much the SSC failures contribute, on a relative basis, to economic damages from reactor transients and accidents at NPPs where the accidents do not necessarily progress to a state of core damage. The contributions to the economic risk measures include:

- Lost generation
- Regulatory impact
- Equipment damage

Table 2. Key information on SSCs as it relates to system health.

Category	Specific Information	Relation to System Health
Key safety function(s) affected	For example, reactivity control, reactor coolant heat removal, reactor coolant inventory control, and containment integrity (isolation, pressure/temperature control)	None, simply identifies the function(s) of the SSC.
Core damage-related and LERF-related risk metrics	For example, RRW and RAW	Provide quantitative measures of the impact of SSC failures on CDF (or LERF) under opposite assumptions of perfect reliability or complete failure, respectively. Thus, systems with generally high RRW and RAW risk measures that are in a degraded state would have high adverse impacts on system health.
Economic Enterprise Risk metrics	Economic risk FV values that account for • Lost generation • Regulatory impact • Equipment damage	Values derived from an economic risk model analogous to CDF and LERF-derived FV importance measures. The metric denotes how much the SSC failures contribute on a relative basis to economic damages from reactor transients and accidents at NPPs where the accidents do not necessarily progress to a state of core damage.
MSPI-related information	For example, margin available for monitored component,	The MSPI monitors the performance of selected NPP systems based on their ability to perform risk-

Category	Specific Information	Relation to System Health
	historic range of MSPI values, past non-green indicators.	significant functions. It provides a surrogate measure of change in CDF resulting from departures of component unreliabilities and train unavailabilities from established baselines. Repetitive high values of the MSPI may be indicative of poor system health for those systems that have risk-significance.
Maintenance Rule-related information	For example, risk-significance classification, train unavailability, train unreliability, number of Maintenance Preventable Functional Failures (MPFFs), Repeat MPFFs, whether the SSC failure can potentially scram the reactor, SSC (a)(1) status, work backlog, temporary modifications, and maintenance cost.	Provides a variety of information regarding the historic performance of the SSC and its relative risk significance.
50.69 SSC categorization and special treatment (if applicable)	For example, risk-informed safety classification (RISC)	Provides perspective on the safety-importance of the SSC. The SSC chosen for special treatment would have undergone a rigorous categorization process involving the Integrated Decision-making Panel (IDP).
TSTF-425, NEI 04-10, SFCP (if applicable)	For example, surveillance test intervals (STIs) that have been adjusted	The STI chosen for adjustment along with the associated SSCs would have received rigorous consideration by the IDP.
TSTF-505, NEI 06-09, RMTS (if applicable)	For example, whether the system is within scope of RMTS	The system chosen for RMTS along with the associated SSCs would have received rigorous considerations. For example, technical adequacy of the PRA, compensatory actions to retain defense in depth, maintaining safety margins, and monitoring using performance measurement strategies are key elements of risk-informed decision-making.
RG 1.178 RI-ISI of Piping (if applicable)	For example, identification of degradation mechanisms and potential for pipe rupture,	Provides a risk-informed means of prioritizing ASME-required piping inspections to enhance safety. The RI-ISI programs can enhance overall safety by focusing inspections of

Category	Specific Information	Relation to System Health
	categorization of consequences by system or piping class	piping at risk-significant locations and locations where failure mechanisms are likely to be present, and by improving the effectiveness of inspection of components by focusing on personnel qualifications, inspection for cause, and the use of multidiscipline plant review teams.

3.5 Pilot Systems for Characterization

Three pilot systems are proposed for characterization of System Health. These systems were chosen in consultation with the utility host and represent both safety related and power production systems at one of the host utility's Boiling Water Reactor (BWR) NPPs. The systems chosen were the following: two plant safety systems – Reactor Core Isolation Cooling (RCIC) and High Pressure Coolant Injection (HPCI), and one power production system – Electro-Hydraulic Control (EHC) of the main steam turbine. These systems were chosen based on a number of considerations which included:

- System size – each of the selected systems is relatively small so that assessments could be performed within the timeframe and budget of the project.
- System importance – each of the selected systems provides important functions to either plant safety or power production with potentially significant consequences to plant economics if system performance would be degraded.
- Availability of utility resources – the ability of site and corporate personnel responsible for each of the selected systems was considered to ensure utility input and participation.

The RCIC system is designed to provide makeup to the reactor vessel during accidents or transients where the reactor vessel pressure remains high. RCIC allows reactor vessel coolant inventory and pressure control until the reactor is depressurized to a point where low pressure systems are capable of providing adequate makeup. The system is sized to provide adequate Reactor Pressure Vessel (RPV) makeup during events in which the plant is shutdown (i.e. removal of decay heat) where main heat sink (i.e., the main condenser) is not available (i.e., the RPV is isolated). The RCIC system operating pressure overlaps that of the low-pressure Emergency Core Cooling Systems (ECCS). The level control function of RCIC, operated from the main control room, is modeled in the plant PRA. The pressure control function of RCIC is not modeled (note that the same situation exists for HPCI).

The RCIC system consists of a steam turbine-driven pump designed for 38 kg/s (600 gpm) between reactor pressures of 1138 and 7688 kPa (150 and 1100 psig), with associated system piping, valves, controls, and instrumentation. Suction piping comes from both the Condensate Storage Tank (CST) and the Suppression Pool (SP). Initially, water from the CST is used until either an automatic swap-over occurs on low CST level or high SP level, or it is manually transferred. The steam supply for the RCIC turbine is from a main steam line inboard of the Main Steam Isolation Valves (MSIV's). Exhaust steam from the RCIC turbine is discharged to the suppression pool.

HPCI is designed to provide makeup to the reactor vessel during accidents where the vessel pressure remains high. HPCI allows reactor vessel coolant inventory and pressure control until the reactor is depressurized. In contrast to RCIC, the HPCI system is sized to provide adequate reactor pressure vessel (RPV) makeup during events in which the plant is shutdown (i.e., removal of decay heat) and for which coolant inventory may be lost due to a break in small to intermediate sized piping. As a result, the HPCI system is substantially larger than RCIC (on the order of a factor of 10). The HPCI system operating pressure also overlaps that of the low pressure ECCS systems.

The HPCI system consists of a steam turbine-driven pump, associated system piping, valves, controls, and instrumentation. Suction piping comes from both the CST and the SP. Water is injected into the reactor vessel through a core spray loop and a feedwater line. The steam supply for the HPCI turbine is from a main steam line inboard of the MSIV's. Exhaust steam from the HPCI turbine is discharged to the SP.

The primary functions of the EHC system are to:

- Provide normal reactor pressure control by controlling steam flow consistent with reactor power
- Control reactor pressure during startup, heatup, and cooldown evolutions
- Control the speed and electrical load on the turbine generator
- Provide protection for the main turbine, main generator and main condenser

The EHC system has both electronic and hydraulic parts. In addition to normal pressure control, the EHC system also contains the electronic and hydraulic components necessary for positioning of the intercept (control valve) portion of the Combined Intermediate Valves (CIVs) and trip control of the Turbine Control Calves (TCVs), the intercept portion of the CIVs, Turbine Stop Valves (TSVs), and the stop valve portion of the CIVs.

The EHC system is typically not modeled in the PRA except as a potential contributor to turbine trip frequency as an initiating event and perhaps some aspects of steam dump to the condenser via the turbine Bypass Valves (BPVs).

Appendix A summarizes the key functions of RCIC, HPCI and EHC as well as:

- How the three systems interface with risk-informed applications
- How the systems may impact electrical generation and, hence, plant economics
- How the systems may be impacted by or contribute to off-normal transients and accidents
- How adverse system performance may have regulatory impacts.

3.6 Plant Economic Impact Vectors

Economic Enterprise Risk (EER) modeling employs conventional risk assessment techniques but applies those methods to reactor transients and accidents at NPPs where the accidents do not necessarily progress to a state of core damage [32]. EER encompasses those efforts to recover from the transient or accident including:

- Repair cost
- Lost power production (or replacement power cost)
- Regulatory impact

These three components of economic costs are not independent. In some instances, as for many full-power internal events (non-flood), the physical damage may be minimal while the lost generation, at costs of many hundreds of thousands of dollars per day, dominates the overall economic impact of the event. In other instances, particularly for internal flooding and fire events, the physical damage can be significant, in the tens of millions of dollars. To the extent that the physical damage results in an extended forced shutdown to repair or replace damaged equipment, costs can add up substantially.

Regulatory Impact relates to the response of local, state, and federal officials and regulatory bodies to the event. In particular, enhanced reactive inspection under NRC's Management Directive 8.3 [23] could result in a Special Inspection Team (SIT), or the dispatching of an Augmented Inspection Team (AIT), or even an Incident Investigation Team (IIT) depending on the safety impact of the event. Other enforcement actions could result as well, depending on the consequences from the event.

Appendix C shows a consolidated set of casualty events along with their generalized plant impact states (identified as C0 through C13). Cost data from a casualty database as discussed in Reference [32] are used as anchor points to map each event to an impact state. Lost generation from a plant outage is factored into the overall cost consideration and usually dominates the total cost. Some of the data used to develop these plant impact state vectors were obtained from publicly available casualty claims in annual reports of Nuclear Electric Insurance Limited (NEIL), but no relationship to NEIL claim categories is made. It is recognized that because cost data are not available for all the events listed, some degree of judgment is necessary to assign each event to an impact state. In these cases, pairwise comparison is made to fit the event between given anchor points which have reasonably defined outage durations and costs.

Generic plant impact states with associated costs are also shown in Appendix C. Generally, the impact states for non-core damage events reflect a factor of 3 in cost from one value to the next. The exception is C10 because of the large absolute dollar gap between C9 and C11, and because a number of data points had costs in this range. Because of uncertainty in the economic consequences of various events, the uncertainty of costs in Appendix C typically spans three cost bins based on judgment. These cost estimates could be better refined with the collection of plant-specific NPP outage and repair cost data, if available.

The cost data in Appendix C go beyond what are normally considered in Generation Risk Assessment (GRA) studies [33]. The GRA studies attempt to predict the risk of generation loss during future operation by estimating the probability and duration of plant trip or de-rate due to degradation or failure of equipment. The primary reason for implementing GRA is to support the performance of applications that impact plant operations and economic performance by improving reliability, reducing maintenance costs, or reducing future lost generation. The data evaluated here include the potential for Regulatory impact from a spectrum of casualty events up to and including core damage events and radiological release.

On the other hand, Risk-Informed Asset Management (RIAM) [34] consists of a decision-analysis, risk-based, plant-level asset and project evaluator methods and tools that are appropriate for use in a market-driven industry. RIAM is intended to provide plant operators with project prioritization and life cycle management planning methods and tools for making long-term maintenance plans, guiding plant budgeting, and determining the sensitivity of a plant's economic risk to the reliability and availability of SSCs, as well as other technical and economic parameters. As described in Section 11 of this report, there exists substantial interfaces between system health and RIAM approaches such that the perspective of both viewpoints is important in plant operations, maintenance, and investment decision-making.

3.7 Considerations on System Health

In this section we have defined System Health as the integrated assessment of NPP equipment performance and condition within the context of system functions. Some key objectives of a System Health program are provided. Links between equipment reliability processes and risk-informed applications are illustrated. Many risk-informed applications can be categorized as those that are primarily regulatory-driven through regulation or NRC programs including the ROP.

A second category of risk-informed applications is designated as more voluntary in nature. The decision to move forward with any of these programs is determined by each individual licensee. Guidance documents are provided by the NRC, industry, or a combination of the two to provide consistency in the application and implementation of the risk-informed activity. Central to many of the guidance documents on equipment reliability is INPO's AP-913 [5] that provides a compendium of resources for maintaining equipment reliability and performance.

The relationship between risk-informed applications and key functions for nuclear power plant operations and sustainability is shown in Table 1. The regulatory-driven applications such as the ATWS, SBO, and ROP programs primarily maintain safe operations. The Maintenance Rule under 10 CFR 50.65, in addition to maintaining safe operations, serves to further improve plant and SSC reliability through the avoidance of reactor scrams.

Three pilot systems are proposed for characterization of System Health – RCIC, HPCI, and EHC. Appendix A summarizes the key functions of RCIC, HPCI, and EHC as well as:

- How the three systems interface with risk-informed applications
- How the systems may impact electrical generation and hence plant economics
- How the systems may be impacted by or contribute to off-normal transients and accidents
- How adverse system performance may have Regulatory impacts
- What are the key input and output data for each system to optimize overall performance

Some results from initial evaluations of data from these pilot systems at the host NPP are provided in Section 5 of this report.

Finally, EER modeling is discussed. EER employs conventional risk assessment techniques but applies those methods to reactor transients and accidents at NPPs where the accidents do not necessarily progress to a state of core damage. A generic plant economic impact vector corresponding to a spectrum of casualty events is provided. The data include the potential for Regulatory impact resulting from off-normal transients and accidents up to and including core damage and radiological release.

4. FRAMEWORK FOR AN INTEGRATED SYSTEM HEALTH PROGRAM

This section summarizes potential approaches for the application of reliability theory to the operating experience data provided by the nuclear utility host plant in this project. First, principles of reliability concepts are described; however, a full discussion of reliability theory is beyond the scope of this report. We have identified two models for potential use to support optimization of plant maintenance and surveillance activities within a risk-informed system health program. The Standby Failure Model (see Appendix D) is used extensively in PRAs but has limitations when it comes to testing and maintenance cost optimization. Markov Methods (see Appendix E) have even greater potential for application; however, they require additional investment of effort to derive rates of degradation and failure. Repair rates should be readily available from plant data sources. Grouping of the performance data may be a means to reduce the analysis effort.

In PRA, only a few failure rates are used to represent a complex piece of machinery such as a turbine-driven RCIC pump or an emergency diesel generator (e.g., fail to start, fail to run for 4 hours, etc.). This works well for the purpose of the PRA; but for optimizing testing and maintenance it is necessary to represent more degradation and failure mechanisms. On the other hand, there are practical limits as to the number of such mechanisms for which there are meaningful data and for which the reliability models can be solved.

A possible approach is to group the predominant failure mechanisms according to a few attributes such as degradation/failure rate, Mean Time To Repair (MTTR), and PM or repair cost.

Plant data would seem to support a repair time categorization for most mechanical components according to the following breakdown (binning):

- < 8 hr
- 8 – 24 hr

- 24 – 72 hr
- > 72 hr.

Failure rates could possibly be grouped into discrete values by decades such as 10^{-7} to 10^{-6} hr^{-1}, 10^{-6} to 10^{-5} hr^{-1}, and so on. Likewise, repair costs could be grouped by the decade from \$1000 to greater than \$1 million.

For example, a small electrical motor may show signs of degradation at a nominal 10^{-5} /hr to 10^{-4} /hr rate, require between \$10k and \$100k in labor and materials repair cost and result in 60 hours of SSC unavailability (24 to 72 hr category). Simple examples of these data are reflected in Table 33 along with other representative repairs. This characterization and grouping of degradation and failure mechanisms clearly identifies the items that are good candidates for a "run to maintenance" strategy because of low frequency of occurrence, low impact on system unavailability, and low cost of repair[a]. Populating a table similar to Table 3 can also allow focus on those components and failure mechanisms that most impact system test and maintenance costs.

Table 3. Simplified representation of grouping of SSC performance data.

Repair Time or Unavailability (hr)	**Degradation/Failure Rate (/hr)**					
	10^{-7} to 10^{-6}		**10^{-6} to 10^{-5}**		**10^{-5} to 10^{-4}**	
	Repair Cost		**Repair Cost**		**Repair Cost**	
	$\$\,10^{3}$–$10^{4}$	**$\$\,10^{4}$-$10^{5}$**	**$\$\,10^{3}$–$10^{4}$**	**$\$\,10^{4}$-$10^{5}$**	**$\$\,10^{3}$–$10^{4}$**	**$\$\,10^{4}$-$10^{5}$**
< 8	Hand switch					
8 - 24			Pump large oil leak			
24 - 72						Small motor replacement
> 72						

4.1 Effectiveness of STs and PMs

The models and plant-specific SSC performance data discussed above can provide most of the framework for maintenance cost optimization. One additional useful metric relates to the effectiveness of existing STs and PMs. For example, a particular test or series of tests that rarely if ever identified degradation or failure mechanisms through decades of service raises the question whether such testing could be terminated, or in the least, the surveillance test interval extended. This is consistent with the SFCP discussed in Section 5.

An important metric that could provide additional insights as to the effectiveness of STs and PMs is the conditional probability that the inspection or testing resulted in an Issue Report (IR) with follow-up Work Order(s). For example, monthly or quarterly valve stroke testing or pump flow testing may result 20% of the time in an IR being generated. The frequency of the ST or PM, combined with the conditional

[a] Note that the term "run to maintenance" is the current terminology for SSCs that are determined not to have specified PM activities. Previously this strategy was termed "run to failure".

probability of degradation, can allow for the determination of parameters used in reliability modeling (i.e. λ_d, $\lambda_{f,}$ and to a lesser extent λ_{df}) as defined in Appendix E.

5. RI-PSH APPLICATIONS

5.1 Maintenance Rule – 10 CFR 50.65

The U.S. Nuclear Regulatory Commission's (NRC) Maintenance Rule, 10 CFR 50.65, became effective in July 1996 [1]. Detailed industry guidance for implementing the Maintenance Rule is found in NUMARC 93-01 [18]. This guidance provides a process for deciding which of the many SSCs that make up a commercial NPP are within the scope of the Maintenance Rule. It then describes the process of establishing plant-specific risk significance and performance criteria to be used to decide if goals need to be established for specific structures, systems, trains and components covered by the Maintenance Rule that do not meet their specified performance criteria.

The major steps of the guidance in NUMARC 93-01 include:

1) Selecting the SSCs within the scope of the Maintenance Rule
2) Establishing and applying risk significant criteria
3) Establishing and applying performance criteria
4) Goal setting and monitoring of applicable SSCs to ensure plant and system functions are reliably maintained and to demonstrate the effectiveness of maintenance activities
5) Assessing and managing the risk resulting from the performance of maintenance activities
6) Performing the periodic assessment of performance
7) Documenting the information needed to support implementation of the Maintenance Rule

Selection of SSCs in step 1 is prescribed in detail in the guidance. Step 2 is linked to the plant-specific Probabilistic Risk Assessment (PRA) model and risk metrics that are derived from the quantification of the PRA. Performance criteria under step 3 are established to provide a basis for determining satisfactory performance and the need for goal setting. The actual performance criteria used should be SSC availability, reliability, or condition. Goals are established to bring about the necessary improvements in performance. When establishing goals, a licensee is to consider various goal setting criteria such as existing industry indicators, industry codes and standards, failure rates, duty cycles, and performance related data.

As described in NUMARC 93-01, monitoring consists of periodically gathering, trending, and evaluating information pertinent to the performance, and/or availability of the SSCs and comparing the results with the established goals and performance criteria to verify that the goals are being met. Assessing the risk means using a risk-informed process to evaluate the overall contribution to risk of the planned maintenance activities. Managing the risk means providing plant personnel with proper awareness of the risk and taking actions as appropriate to control the risk. Periodic assessments are performed to establish the effectiveness of maintenance actions. These assessments consider, where practical, industrywide operating experience. Finally, all aspects of the process are documented as appropriate.

5.2 Surveillance Frequency Control Program

NEI 04-10 [28] describes the technical methodology to support risk-informed Technical Specifications initiative 5b, which provides a risk-informed method for licensee control of surveillance frequencies. Existing specific surveillance frequencies are removed from plant Technical Specifications for the affected specifications and placed under licensee control pursuant to this methodology. A paragraph is added to the Administrative Controls section of the plant Technical Specifications referencing this methodology document, as approved by NRC, for control of surveillance frequencies. The surveillance test requirements (test methods) are not changed and remain in the Technical Specifications.

The methodology of NEI 04-10 [28] uses a risk-informed, performance-based approach for establishment of surveillance frequencies, consistent with the philosophy of NRC Regulatory Guide (RG) 1.174 [35]. PRA methods are used to determine the risk impact of the revised intervals. Sensitivity studies are performed on important PRA parameters. A multi-disciplinary plant decision-making panel (IDP) is utilized to evaluate determinations of revised surveillance frequencies, based on operating experience, test history, manufacturers' recommendations, codes and standards, and other factors, in conjunction with the risk insights from the PRA. Results and bases for the decision must be documented.

The effect of the proposed changes to surveillance frequencies, aggregate risk impact of the single revised surveillance frequency for all PRA events, and the cumulative risk impact for all surveillance frequency changes are compared to NRC risk acceptance guidelines per RG 1.174. Feedback and periodic re-evaluation of the surveillance frequencies are conducted for SSCs. As noted in NEI 04-10, two important aspects of performance monitoring are whether the test surveillance frequency is sufficient to provide meaningful data and whether the testing methods, procedures, and analysis are adequately developed to ensure that performance degradation is detected. Component failure rates should not be allowed to rise to unacceptable levels (e.g., significantly higher than the failure rates used to support the change) before detection and corrective action take place.

5.3 Risk-Managed Technical Specifications

NEI 06-09 [27] provides guidance for implementation of a generic Technical Specifications improvement that establishes a risk management approach for voluntary extensions of completion times for certain Limiting Conditions for Operation (LCOs). The methodology uses a risk-informed approach for establishment of extended completion times and is consistent with the philosophy of RG 1.174 [35]. PRA methods are used to determine the risk impact of the revised completion times.

The extension of completion time for a plant SSC that is inoperable per the plant Technical Specifications must consider the configuration-specific risk and is an extension of the methods used to comply with paragraph (a)(4) of the Maintenance Rule, 10 CFR 50.65. Plants implementing this initiative are expected to use the same PRA analyses to support their Maintenance Rule (a)(4) programs. A deterministic 30-day backstop value is imposed to limit the completion time extension regardless of low risk impact. Results of implementation are monitored, and cumulative risk impacts are compared to specific risk criteria. Corrective actions are implemented should these criteria be exceeded.

An important element of the RMTS is the programmatic requirement to manage risk and to implement reasonable compensatory measures to reduce risk. As noted in NEI 06-09, compensatory measures may include but are not limited to the following:

- Reduce the duration of risk sensitive activities.
- Remove risk sensitive activities from the planned work scope.
- Reschedule work activities to avoid high risk-sensitive equipment outages or maintenance states that result in high-risk plant configurations.
- Accelerate the restoration of out-of-service equipment.
- Determine and establish the safest plant configuration.

In order to implement RMTS, a process must be in place to monitor plant modifications and other changes which may impact the PRA model to assure that the configuration risk management program (CRMP) correctly reflects the as-built, as-operated plant. The CRMP must be governed by plant procedures, and any deficiencies of the CRMP tool must be addressed and dispositioned in accordance with the requirements and time limits of the licensee's corrective action program.

5.4 SSC Characterization and Special Treatment – 10 CFR 50.69

NEI 00-04 [29] provides detailed guidance on categorizing SSCs for licensees that choose to adopt 10 CFR 50.69, *Risk-Informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors.* There are two steps associated with the implementation of 10 CFR 50.69: (1) the categorization of SSCs and (2) the substitution of alternative treatments as replacements for NRC specified special treatment requirements that are consistent with the safety significance of the equipment categorized in the first step. A licensee wishing to implement 10 CFR 50.69 makes a submittal to the NRC for review and approval.

The 10 CFR 50.69 SSC categorization process is an integrated decision-making process. This process blends risk insights, new technical information and operational feedback through the involvement of a group of experienced licensee-designated professionals. This group, known as the Integrated Decision-making Panel (IDP), is supported by additional working level groups of licensee-designated personnel. 10 CFR 50.69 does not replace the existing "safety-related" and "non-safety-related" categorizations. Rather, 10 CFR 50.69 divides these categories into two subcategories based on High or Low Safety Significance (HSS or LSS respectively). This is depicted schematically in Figure 7.

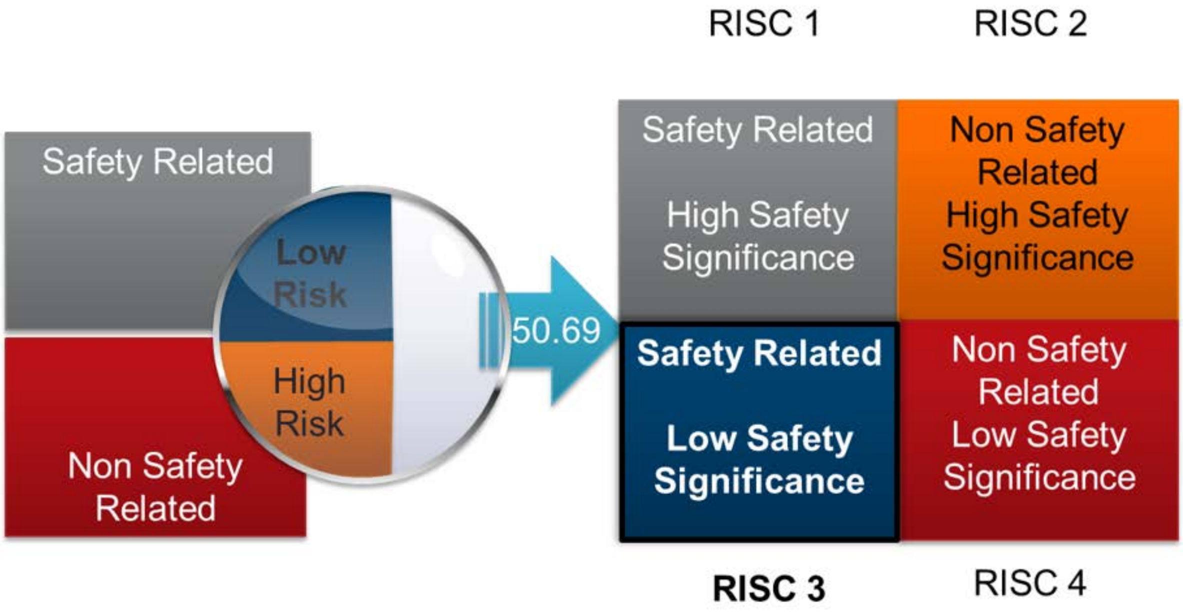

RISC 1
RISC 2
Safety Related
Low Risk
High Risk
Non Safety Related
50.69
Safety Related High Safety Significance
Non Safety Related High Safety Significance
Safety Related Low Safety Significance
Non Safety Related Low Safety Significance
RISC 3
RISC 4

Figure 7. 10 CFR 50.69 classifications.

Special treatment requirements are current NRC requirements imposed on SSCs that go beyond industry-established (industrial) controls and measures for equipment classified as commercial grade and are intended to provide reasonable assurance that the equipment is capable of meeting its design bases functional requirements under design basis conditions. These additional special treatment requirements include design considerations, qualification, change control, documentation, reporting, maintenance, testing, surveillance, and quality assurance requirements.

As described in NEI 00-04, from a safety perspective, the benefits of implementing 10 CFR 50.69 are associated with better licensee and NRC focus of attention and resources on matters that have higher levels of safety significance. A risk-informed SSC categorization scheme should result in an increased awareness on that set of equipment and activities that could impact safety, and hence provide an overall improvement in safety with the potential to reduce costs.

5.5 Characterization of Plant Data

This section summarizes the review and characterization of the operating experience data provided by the nuclear utility host plant for this project. The set of requested data that was provided was complete. The initial review of the data was limited to a single NPP site as a pilot effort. While the HPCI, RCIC and EHC systems are all within scope for this task, emphasis was placed initially on characterization of the RCIC system and to a lesser extent on HPCI.

The sources of plant operational data can be categorized as (a) source data and (b) reviewed, vetted and consolidated data.

5.5.1 Source data

The primary sources of source data include:

- Operations Logs
- Issue Reports (IRs)
- Work Orders (WOs).

Operation Logs are most useful because they clearly state when Technical Specifications action statements were entered and exited, and for particular surveillances (e.g., RCIC valve stroke testing), the exact time that the system was Out-Of-Service (OOS).

IRs provide useful information regarding the origination date, system, severity, operability, and functionality associated with plant SSCs and events. However, the file that was provided did not include a cross-reference to WO number which limited the scalability for this project in linking the work performed following an SSC Issue Report.

WOs provide a description of the task, start and completion dates/times, system/component, type of work (e.g., preventive maintenance) and labor hours. The labor hours are particularly useful to permit assessment of cost and economic impact. The data provided did not have a data field that cross-referenced the IR number (if that was the initial reason for the WO), making it less efficient to link the two for the purpose of this project. It is clear that one could not use the WO start and completion times as a measure of system unavailability since a comparison to Operations Logs indicated they did not often correlate.

5.5.2 Vetted data

Vetted data sources use the above source data that have been reviewed, assessed for applicability, and consolidated for a particular purpose. Examples include:

- 10 CFR 50.69 characterization report
- SFCP documentation
- Maintenance Rule, System Unavailability/Mitigating Systems Performance Index (MSPI), and PRA component failure rate compilations.

The vetted data are directly useful. For example, the System Unavailability data provide a concise tabulation of the event, date and times, unavailable hours, and whether the unavailability was planned or unplanned. The data are input to the MSPI. If the maintenance performed was unplanned, there is a strong possibility the event was due to a functional failure. These entries can be confirmed with a review of the historical MSPI trend plots available on NRC's public web site.

5.6 Use of the Plant Data

The plant performance data for RCIC, HPCI, and EHC provide the minimum set of information for the project. An overview of the use of the plant operational experience data is described below.

Presume that a Surveillance Test (ST) or PM activity detects a degrading condition on a component of a system such as RCIC. Subsequently, an IR and associated WO would be generated. The WO would also generate a number of tasks. Given the date, Operations Logs would indicate the time the system was declared to be INOPERABLE and when it was restored to OPERABLE. The on-line risk monitor would show the calculated change in plant risk level (e.g., from GREEN to YELLOW). The unavailability eventually would be noted in the System Unavailability compilation file. PRA data from a number of sources could be obtained for the RAW for the component/system in question. When combined with the hours of unavailability, the Incremental Conditional Core Damage Probability (ICCDP) and Incremental Increase in Large Early Release Probability (ICLERP) can be quantified. These can be translated to economic risk costs consistent with the economic risk assessment for the pilot plant.

If the event of concern was a functional failure, the potential regulatory implications in terms of increased NRC oversight (White, Yellow, or Red in MSPI or SDP) can also be quantified.

The WO would provide the labor hours which could be translated to calculate the repair costs. If the degradation on a system necessary for plant generation was the issue (e.g., EHC), one could directly relate the incident with the potential for lost electricity generation and the associated lost revenues.

In summary, the available data would directly provide the economic costs of the repair/maintenance activity as well as certain externalities such as Regulatory impact.

The benefit side of the Cost-Benefit equation is more challenging to ascertain. Clearly, if a key component is degrading and PM was not performed, an incipient failure condition would go undetected. The system (e.g., RCIC) would eventually be declared INOPERABLE, leading to the possibility of a plant shutdown and lost generation if the failure were catastrophic and repair time exceeded the Allowed Outage Time (AOT) in the plant Technical Specifications (TS).

Because there have been so few functional failures of HPCI and RCIC in recent years at the host plant, it is not possible to correlate degradation mechanisms with conditional probability of equipment failure to any degree of accuracy. Certainly, manual review of IRs and WOs alone could not generate correlations between certain PMs and ST intervals (STIs), and the probability of eventual equipment failure. Ultimately, advanced data analytics may be applied to act as a screening tool; however, the final determination will always lay with cognizant plant staff.

In the absence of advanced analytics, reliability models may need to be used. For example, Standby Failure Models (1/2 λT) or Markov Methods as described in Appendices D and E, respectively, may be applied. From these models, estimates of the potential for degradation to lead to functional failures may be generated. The benefits of changing the interval of a PM or ST in terms of labor hours saved (extension of interval) or reduced potential for failure (shortened interval) may be estimated but there likely would be large uncertainties in the resulting Cost-Benefit estimates.

A more detailed analysis of plant data is reported in Appendix F.

5.7 Consideration of Data Analysis

A number of risk-informed applications have been identified that directly make use of plant-specific operations data. All of the programs listed here, and other plant processes not described in any great detail in this report, use the data to improve SSC reliability and availability, and thereby maintain or improve plant safety.

Processes such as 10 CFR 50.69 are associated with better licensee and NRC focus of attention and resources on matters that are safety significant. They also aim to reduce procurement and maintenance costs by allowing for the application of NRC special treatment requirements consistent with the safety significance of the equipment categorized.

Applications such as RMTS allow for greater flexibility in the scheduling of equipment outages while monitoring and maintaining plant safety.

SFCP also allows for flexibility in plant operations and maintenance by allowing extensions of routine surveillances when appropriate. Performance monitoring ensures that performance degradation of SSCs subject to the program are readily detected.

Plant performance data have been characterized as *source* data, i.e. unprocessed data from logs and maintenance records, and *vetted* data that have been reviewed and provide big-picture snapshots of overall SSC performance. These data, whether source or vetted, meet the needs of supporting effective risk-informed decision-making.

By way of three examples as provided in Appendix F, it is shown that key information such as the costs for SSC surveillance, PM, and repair can be derived. System Unavailabilities can be combined with PRA risk metrics to assess the reactor risk and economic risk impacts of equipment outages.

While the costs in the Cost-Benefit equation can be readily derived, the benefits of activities such as surveillance test extensions and deferred PM are more challenging to evaluate. In the short term, reliability modeling may be necessary to estimate how SSCs are impacted by various degradation mechanisms. In the long term, advanced data analytics may be developed and applied to make the process more scalable to more than a few plant systems.

6. RELIABILITY MODELS

6.1 Component Failure Models

Due to the stochastic nature of component failures, the assessment of the ability of a component to perform a specific function is typically defined probabilistically. The starting point is the definition of the probability $F(T)$ that at component will not be able to perform a specific function in the $[0, T]$ interval:

$$F(T) = Pr(t \leq T) = \int_{0}^{T} f(\tau)d\tau \qquad \text{provided} \qquad t > 0 \qquad (1)$$

where $f(\tau)d\tau$ represents the probability distribution function that the component fails in the $[\tau, \tau + d\tau]$ interval. From here, it is possible to define the probability that the component will correctly perform its function in the $[0, T]$ interval:

$$R(T) = Pr(t > T) = 1 - F(T) = \int_{T}^{\infty} f(\tau)d\tau \qquad \text{provided} \qquad t > 0 \qquad (2)$$

The next step is definition of the failure rate function which is defined as:

$$\lambda(T) = \lim_{dt \to 0} \frac{Pr(T, T + dt | t > T)}{dt} = \frac{f(t)}{R(t)} \qquad (3)$$

where $Pr(T, T + dt | t > T)$ is the probability that a component will fail in the $[T, T + dt]$ interval assuming the component is functioning at time t.

The objective of the PHM data analysis method is to integrate component data such as failure reports, maintenance data, monitoring data to determine the temporal profile of the component failure rate.

6.2 Integration of Maintenance and SSC Ageing

Component ageing/degradation and component maintenance are correlated variables and, therefore, this coupling needs to be considered in the analysis. Maintenance can be included in component reliability models in several approaches:

1. Basic event in the system Fault-Tree
2. Element in the component unavailability model
3. Markov or Semi-Markov model

In the first approach the maintenance-ageing coupling is poorly considered but it has the advantage that it can be quickly included in existing PRA models.

The second approach, which has been used in Section 8, includes maintenance and ageing in the same component unavailability model. In this model, maintenance is included in the component unavailability model in term of maintenance downtime and maintenance-induced failure. The advantage of this model is that it is possible to inform these models from plant maintenance data.

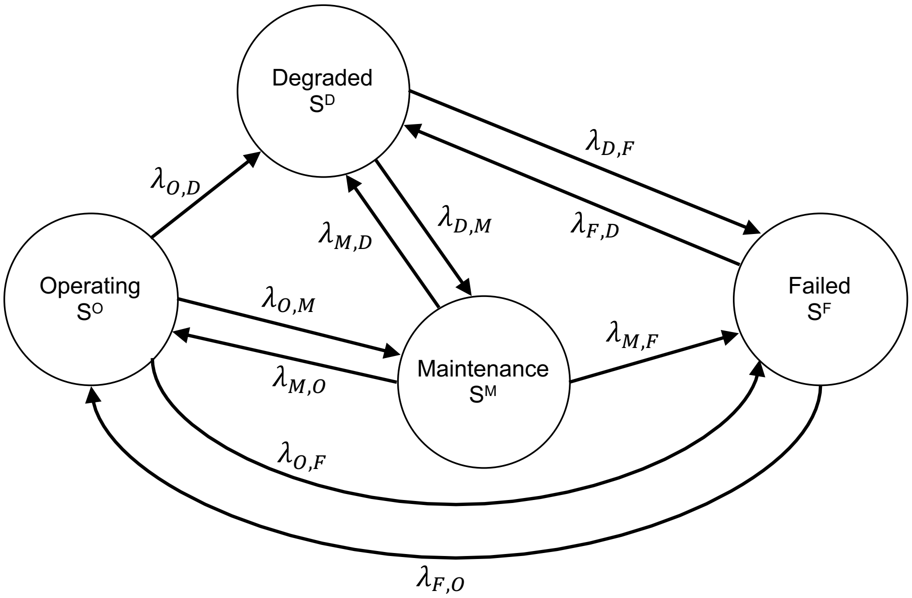


Figure 8. SSC reliability models which integrates maintenance and SSC ageing [64].

The third approach creates a tighter coupling between component ageing and maintenance in a Markov model. Markov models (or Markov chains) are often employed to determine reliability/availability of systems characterized by multiple states, i.e., not only failed or operating states. These models consist of N mutually exclusive states which describe a specific status of the system (e.g., system operating, system under repair, system failed). Transitions among states are stochastic in nature and are described by a set of probability transition rates $M_{p,q}$ $(p, q = 1, \dots, N)$. Mathematically, a Markov model can be described as:

$$\frac{d\boldsymbol{P}(t)}{dt} = \boldsymbol{M} \cdot \boldsymbol{P}(t) \tag{4}$$

where each element $P_i(t)$ $(i = 1, \dots, N)$ of the vector $\boldsymbol{P}(t) = [P_1(t), \dots, P_N(t)]$ represents the probability of being in state i at time t while $\boldsymbol{M} = [M_{p,q}]$ contains all possible transition rates from state p to state q $(p, q = 1, \dots, N)$. In order to include maintenance and component ageing/degradation into a single model, reference [64] proposes a four state Markov model as shown in Figure 8.

7. RISK-INFORMED NET PRESENT VALUE OF SYSTEM OPERATION

The scope of this section is to provide an economic model designed to determine the Net Present Value (NPV) of a system which includes the value of its operation, its related Operation and Maintenance (O&M) costs and the risk associated with its failure. This document is based on [36] which creates a direct link between reliability and NPV for a given system in order to determine the "value of reliability". With the goal to develop a risk-informed economic model for the system health program, i.e., a System Operation NPV, we have extended the work presented in [36] by including:

- The risk associated with the failure of both components and system
- Time dependent failure rates/probabilities
- Component ageing and degradation
- Effectiveness of maintenance and testing

As shown in [36] we have assumed the following:

1. A single system sys is analyzed
2. The considered system is composed of a set of N components
3. System failure can be uniquely determined from the logical status of its components (e.g., by employing a Fault-Tree logic structure)
4. Time horizon is fixed (i.e., $[0, T^{Max}]$) and it is discretized into T time intervals having identical length Δt (i.e., $T^{Max} = T \cdot \Delta t$)

In the following section we follow this notation:

- $p_t(.)$ probability within time interval t
- $R_t(.)$ reliability within time interval t
- ir interest rate

In the System Operation NPV model we want to capture in a single economic model the value, the costs, and the risk/reliability associated with a SSC which is an integral part of a more complex system. These three terms are described and modeled in Sections 7.1, 7.2 and 7.3.

7.1 System Operation Value

The Present Value associated to system operation $PV^{operation}$ can be evaluated in each time interval (with length Δt) as follows:

$$PV^{operation} = \sum_{t=1}^{T} R_{t-1}(sys)\frac{\big(1 - p_t(sys)\big) \cdot V_t}{(1 + ir)^t} \tag{5}$$

where:

- $R_{t-1}(sys)$: reliability of the considered system sys within time interval $t - 1$
- $p_t(sys)$: probability of failure of the considered system sys within time interval t
- V_t: economic production value (e.g., power generation) due to the correct operation of the system within time interval t

7.2 System Life-Cycle Value

The Present Value associated to system operation and maintenance can be determined by first evaluating such present value for a single component. This Present Value associated operation and maintenance for a single component n is:

$$PV_n^{life} = C_n^{proc} + \sum_{t=1}^{T} \frac{C_{t,n}^{OM}}{(1 + ir)^t} \tag{6}$$

where:

- C_n^{proc}: procurement costs of component n (note that here more complex supply chain models can be added)
- $C_{t,n}^{OM}$: O&M costs for component n within time interval t

From PV_n^{life} it is then possible to determine the Present Value associated to operation and maintenance for the considered system PV^{life} as:

$$PV^{life} = \sum_{n=1}^{N} PV_n^{life} = \sum_{n=1}^{N} C_n^{proc} + \sum_{n=1}^{N}\sum_{t=1}^{T} \frac{C_{t,n}^{OM}}{(1 + ir)^t} \tag{7}$$

7.3 System Failure Value

The last term that needs to be included in the system Health Program economic model is the Present Value $PV^{failure}$associated to system failure. This can be determined as:

$$PV^{failure} = \sum_{t=1}^{T} R_{t-1}(sys)\frac{C_t^{failure}}{(1 + ir)^t} \tag{8}$$

where:

- $C_t^{failure}$: expected cost due to system failure
- $R_{t-1}(sys)$: reliability of the considered system sys within time interval $t - 1$

The term $C_t^{failure}$ can be defined as

$$C_t^{failure} = \sum_{n=1}^{N} p_t(n) \cdot p_t(sys|n) \cdot C_{t,n}^{failure} \tag{9}$$

where:

- $p_t(n)$: probability of failure of component n within time interval t
- $p_t(sys|n)$: probability of failure of the considered system sys within time interval t given that component n has failed
- $C_{t,n}^{failure}$: cost associated to system failure caused by failure of component n (e.g., loss of production, replacement costs, regulatory burden) within time interval t

7.4 System Operation NPV

Finally, the Net Present Value of system operation $NPV^{operation}$ can be defined as the algebraic sum of the three terms defined in Sections 7.1, 7.2 and 7.3 as follows:

$$\begin{aligned} NPV^{operation} &= PV^{operation} - PV^{life} - PV^{failure} = \\ &= \sum_{t=1}^{T} R_{t-1}(sys) \frac{\left(1 - p_t(sys)\right) \cdot V_t}{(1+ir)^t} + \\ &+ \sum_{n=1}^{N} C_n^{proc} + \sum_{n=1}^{N} \sum_{t=1}^{T} \frac{C_{t,n}^{OM}}{(1+ir)^t} + \\ &+ \sum_{t=1}^{T} R_{t-1}(sys) \frac{\sum_{n=1}^{N} p_t(n) \cdot p_t(sys|n) \cdot C_{t,n}^{failure}}{(1+ir)^t} \end{aligned} \quad (10)$$

7.5 System Reliability Model

The major obstacle in Equation (10) is the determination of the reliability models for both components and system; i.e., the determination of the variables $p_t(sys)$, $p_t(sys|s)$, $R_t(sys)$ and $p_t(s)$. Provided the definition of $p_t(sys)$ and $R_t(sys)$, it is possible to note that:

$$R_t(sys) = 1 - \sum_{\bar{t}=1}^{t} p_{\bar{t}}(sys) \quad (11)$$

The system reliability model $p_t(sys)$ is designed to create the link between system failure and component failure. For safety systems, this is already performed by plant owners which maintain their PRA models. These models are mainly based on Fault-Trees (FTs) and Event-Trees (ETs).

In our applications, since we are looking at the system level, we will mainly employ existing FTs if we are considering safety systems (see Section 8). If we are considering systems outside the regulatory jurisdiction, then new FT models for these systems might be required (see Section 9).

ETs and FTs link a set of K elemental events, i.e., basic events BE_k $(k = 1, \dots, K)$, to plant condition (e.g., Core Damage – CD – condition or Large Early Release):

$$p_t(sys) = \Psi(BE_1, \dots, BE_K) \quad (12)$$

Each basic event BE_k depicts a specific elemental event (i.e., failure or recovery events) of basic components. For each basic event BE_k, a probability value $p_t(BE_k)$ is assigned.

In our applications $p_t(BE_k)$ is not constant, but it changes with time since ageing and degradation alter the state of the component:

$$p_t(BE_k) = \Phi(ageing, degradation, O\&M) \tag{13}$$

The function Φ is obviously a non-linear function and it also depends on previous history of the component (i.e., O&M: operational condition, preventive maintenance history).

For the scope of this project, instead of reasoning in terms of failure rates and probability associated to each basic event, it is more convenient to probabilistically describe the basic events that have a time-dependent behavior (see equation above) in terms of unavailability. Section 8 presents in more detail a practical example of SSC unavailability models (see equation above) applied to maintenance optimization.

7.6 Incorporating SSC Ageing and Degradation into Reliability Models

Usually a failure rate or a probability value is associated to each basic event and these values are not time dependent. In our application, we envision that the incorporation of SSC ageing and degradation into Reliability models can be performed by:

1. Adding new basic events which model the effect of ageing (e.g., piping accelerated corrosion) of both passive and active components
2. Creating reliability models to determine temporal evolution of failure rates or failure probabilities associated to a specific set of basic events
3. Including the effect of maintenance and testing on SSC ageing and degradation
4. Including data generated from PHM methods

7.7 Mode of Operation for Decision Making

The NPV model of Section 7.4 is designed to be employed as a decision-making tool to compare and rank investment options against initial system configuration, i.e.:

$$NPV_{initial}^{operation} \text{ v.s. } NPV_{investment}^{operation}$$

In particular, the ranking criteria would be based on the relative NPV change:

$$\delta = \frac{NPV_{investment}^{operation} - NPV_{initial}^{operation}}{NPV_{initial}^{operation}} \tag{14}$$

Note that the criteria described in Equation (14) merges system/component reliability into NPV. From a decision-making perspective this would be too stringent. An alternative has been offered by [36], where system/component reliability and NPV are kept separate, i.e., we are comparing:

$$\left(NPV^{operation}, R(sys)\right)_{initial} \text{ v.s. } \left(NPV^{operation}, R(sys)\right)_{investment}$$

An important factor to consider is that some elements in Equation (11) might not be certain but they might be affected by uncertainties. Thus, it is required to propagate uncertainties throughout the model. Graphically this can be plotted in a 2-dimentional graph (see Figure 9) where each dimension corresponds to the incremental $NPV^{operation}$ and incremental $R(sys)$. Note that these two dimensions are correlated since $NPV^{operation}$ is also function of $R(sys)$. Another important feature about propagating uncertainties is that it is possible to evaluate the sensitivity of $NPV^{operation}$ and $R(sys)$ to a variation of each uncertain parameter. This sensitivity analysis might prove to be useful to rank the most relevant uncertain parameters from a decision-making standpoint.

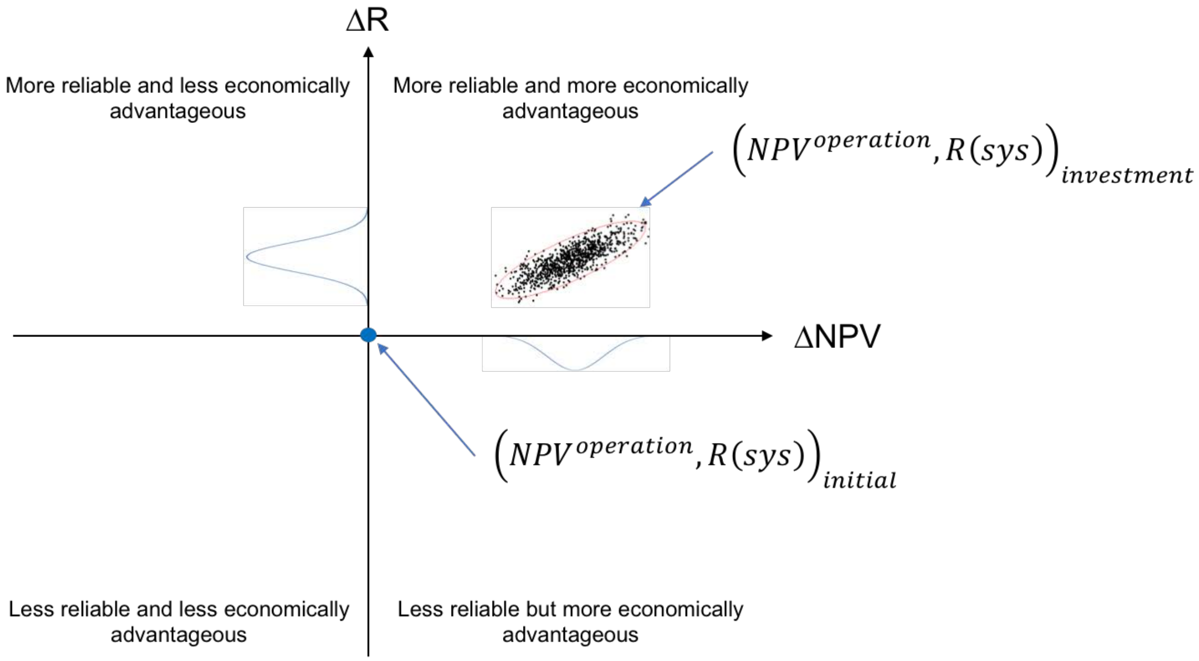

ΔR
More reliable and less economically advantageous
More reliable and more economically advantageous
$\left(NPV^{operation}, R(sys)\right)_{investment}$
ΔNPV
$\left(NPV^{operation}, R(sys)\right)_{initial}$
Less reliable and less economically advantageous
Less reliable but more economically advantageous

Figure 9. Reliability vs. NPV plot for evaluation of candidate projects.

8. RISK-INFORMED MAINTENANCE OPTIMIZATION

The objective of this section is to show a methodology and an example of a risk-informed maintenance optimization process which balances cost and risk in a unified optimization framework.

The starting point for this work is the concept of VBM as developed by NEI [13] as part of the DNP initiative. The VBM approach has the objective to change "the industry's culture of reliability at any cost and more is better to one where maintenance is treated as a highly valued and limited resource is key to advancing safety and reliability in a cost-effective manner".

Figure 5 shows, in a graphical form, how maintenance cost changes as a function of the number of PM tasks performed on a specific component. Maintenance cost is measured as the sum of the costs associated with both PM and Corrective Maintenance (CM) activities. PM tasks are designed to compensate for the ageing of the component and avoid component failure. CM tasks are uniquely performed to replace/repair such SSC as soon as practicable after its failure.

The question that arises from Figure 5 is: what is the optimal number of PM activities/tasks to perform on a SSC? The initial considerations before answering this question are the following:

- If PM activities are performed infrequently, PM costs would decrease but component ageing might increase the probability of component failure (with potential economic loss due to such failure: not only CM costs but also component unavailability related costs)
- Too frequent PM activities will increase PM costs, reduce component ageing and ageing-induced SSC failure; however, maintenance-induced component failure will increase (with potential economic loss due to such failure: not only CM costs but also component unavailability related costs)

Thus, the problem cannot be viewed and solved only in a 1-dimentional space (PM + CM costs) but it requires a second dimension: component unavailability. We are not only considering component failure probability (in terms of mean time between failure, MTBF) but we are considering also The Mean Down Time (MDT). Component unavailability is measured as the probability that the component is not operating at a specific time instant. This concept is shown in Figure 10 where the calculations of MDT and MTBF are obtained by averaging over the population of maintenance events that were performed on the particular SSC.

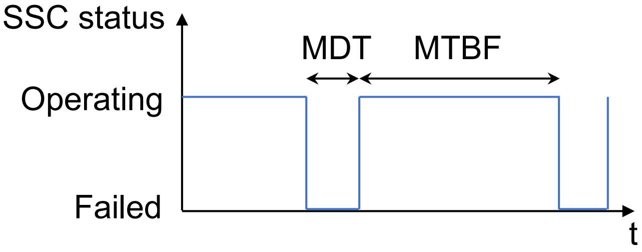
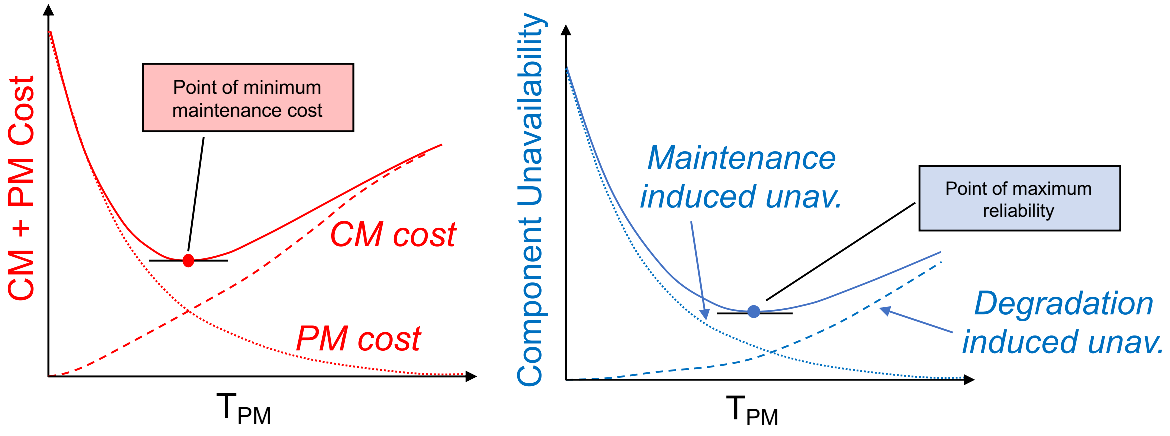


Figure 10. Grahical representation of MDT and MTBF.

An important consideration is that the balance between cost and unavailability cannot be performed solely at the component level but needs to be integrated at the system level. The goal is to balance system maintenance costs (PM and CM for all components of the system) and system availability. Instead of focusing on the number of PM tasks shown in Figure 11 we will focus on the time interval T_{PM} between two PM activities. Graphically this is shown in Figure 11:

- Small T_{PM}, i.e., high number of PM tasks
  - Maintenance costs are dominated by PM costs since it is less likely to observe component failure. PM costs grow as a higher number of PM tasks are performed while CM costs decrease since PM tasks are greatly reducing the likelihood of component failure.
  - Component unavailability is dominated by maintenance induced unavailability (e.g., human error of omission to restore component functions).
- Large T_{PM}, i.e., low number of PM tasks
  - Maintenance costs are dominated by CM costs since it is more likely to observe component failure.
  - Component unavailability is dominated by component failure due to ageing/degradation.

Note that in Figure 11 it is evident that the points of minimum total maintenance costs and maximum system reliability do not necessarily coincide. Therefore, judgment will be required to determine which of the two objectives should have greater importance when optimizing the plant system health / equipment reliability program. It also should be noted that this balancing of importance will likely lead to different outcomes for different systems that are dependent on factors such as the system's importance to plant safety or power production, system costs, previous system operating experience, etc.



(a) (b)

Figure 11. Maintenance costs (a) and component unavailability (b) as function of T_{PM}.

8.1 Generic Use Case

We consider a generic system as an ensemble of components. For each component (e.g. valves and pumps) we consider a set of PM activities designed to decrease the SSC ageing effect and improve component reliability. Each PM is characterized by:

- PM cost
- Probability of SSC unavailability due to maintenance
- Reduction of SSC ageing (i.e., measure of PM effectiveness)

The objective is to determine the optimal combination of PM interval T^{PM} for all components that maintains system unavailability below a pre-defined value and minimizes overall maintenance costs. It is here assumed that after a PM activity is performed, the component returns into operation in as good as new condition.

8.2 Mathematical Formulation

We define a system S as an ensemble of N components C_i, $S = \{C_1, \dots, C_N\}$, where each component C_i is characterized by:

- Cost of PM: $Cost_i^{PM}$
- Cost of CM: $Cost_i^{CM}$
- Failure rate: λ_i
- PM interval: T_i^{PM}
- PM downtime: T_i^{DT}
- Human error of omission (probability to fail to return to service after PM): p_i^{PM}

The mathematical formulation of risk-informed maintenance is to:

$$\begin{array}{ll} \text{Determine:} & T_i^{PM} \text{ for } i = 1, \dots, N \\ \text{Objective:} & min[Cost^{sys}] \\ \text{such that:} & U^{sys} < \tilde{u} \end{array} \qquad (15)$$

where:

- U^{sys} is system unavailability
- $Cost^{sys}$ is the complete maintenance related costs
- $Cost_i^M$ represents the maintenance costs associated to each component C_i. This variable is a function of:

$$Cost_i^M = Cost_i^M\left(Cost_i^{PM}, \tilde{u}_i, Cost_i^{CM}\right) \tag{16}$$

The last line in Equation (15) is imposing the constraint that U^{sys} must be kept below a pre-defined value $\tilde{u}$. It should be noted that imposition of such a constraint is in accordance with standard industry practice and regulatory expectations (e.g., Maintenance Rule). At this point, provided the data listed above for each component, it is needed to determine:

- $\tilde{u}_i$: component unavailability (see Section 8.2.1)
- $Cost_i^M$: costs due component maintenance (see Section 8.2.2)
- U^{sys}: system unavailability (see Section 8.2.3)
- $Cost^{sys}$: system maintenance costs (see Section 8.2.4)

and proceed to solve the optimization problem.

8.2.1 Component Unavailability Model

For the scope of this analysis we create a “first generation” unavailability model which can be written as the sum of the following terms:

- Component unavailability due to PM error of omission: p_i^{PM}
- Component unavailability due to PM operation: $\frac{T_i^{DT}}{T_i^{PM}}$
- Component unavailability due to component failure: P^F

Thus, $\tilde{u}_i$ can be written as [37]:

$$\tilde{u}_i = p_i^{PM} + \frac{T_i^{DT}}{T_i^{PM}} + P^F \tag{17}$$

where P^F is the probability of failure of a component in $\left[0, T_i^{PM}\right]$.

In order to include component ageing in this analysis, the component failure rate λ_i is not constant but can change with time, i.e., $\lambda_i = \lambda_i(t)$. The most common model that employs time-dependent failure rates is the Weibull model; for the scope of this report we will employ a simple failure model where the failure rate grows linearly in time:

$$\lambda_i = \lambda_i(t) = \lambda_{i,0} + a_i \cdot t \tag{18}$$

The reason behind this choice is that we envision that, in the near future, plant health data will be employed to determine component failure probability. In this respect, it is preferable to translate plant health data into time dependent failure rates rather than fitting such data into a pre-defined model (e.g., Weibull model). Once $\lambda_i(t)$ is determined, we can then determine the probability of failure of a component in $\left[0, T_i^{PM}\right]$ [39]:

$$P^F = \int_0^{T_i^{PM}} \lambda_i(t) \cdot e^{\int_0^t \lambda_i(\tau)\, d\tau}\, dt \tag{19}$$

8.2.2 Component Cost Model

The component cost model includes the CM and PM costs. PM costs can be considered as hard costs (i.e., real costs to the plant owners). Also CM costs are hard costs when they occur; however, because failures represent random events, these costs need to be weighted by the probability of failure. For the scope of this report we are defining $Cost_i^M$ as:

$$Cost_i^M = Cost_i^{PM} + P^F \cdot Cost_i^{CM} \tag{20}$$

As of now, in the term $Cost_i^{CM}$ we have included only procurement and installation cost. In the future, this term can be expanded to include supply-chain models and other failure-related costs (e.g., regulatory cost).

In our applications, if we want to compare maintenance strategies, it is more convenient to evaluate the costs due to maintenance (PM and CM) per unit time $\overline{Cost_i^{Maint}}$since we want to measure the normalized change of $Cost_i^M$ over a change of T_i^{PM} [38]:

$$\overline{Cost_i^{Maint}} = \frac{Cost_i^M}{T_i^{PM}} = \frac{Cost_i^{PM} + P^F \cdot Cost_i^{CM}}{T_i^{PM}} \tag{21}$$

8.2.3 System Unavailability Model

System unavailability models can be constructed using several methods. For our applications, the goal is to minimize industry efforts to construct/maintain these models and, thus, classical PRA models can be employed (Fault-Trees for example). If safety systems are considered, these models already exist and can be easily re-used for this kind of application. Fault-Trees can be easily evaluated by PRA codes like CAFTA, RiskSpectrum and SAPHIRE [158] when reliability data (failure rates, failure probabilities, unavailability values) are provided as input. Output data consists of overall system unavailability. The advantage of employing existing PRA codes is that uncertainties in input data can be propagated up to the output variables.

Thus, in our applications:

$$U^{sys} = FT(\tilde{u}_1, \dots, \tilde{u}_N) \tag{22}$$

8.2.4 System Costs Model

Given that a system S is an ensemble of N components C_i, $S = \{C_1, \dots, C_N\}$, the maintenance costs at the system level are equal to:

$$Cost^{sys} = \sum_{i=1}^{N} \overline{Cost_i^{Maint}} \tag{23}$$

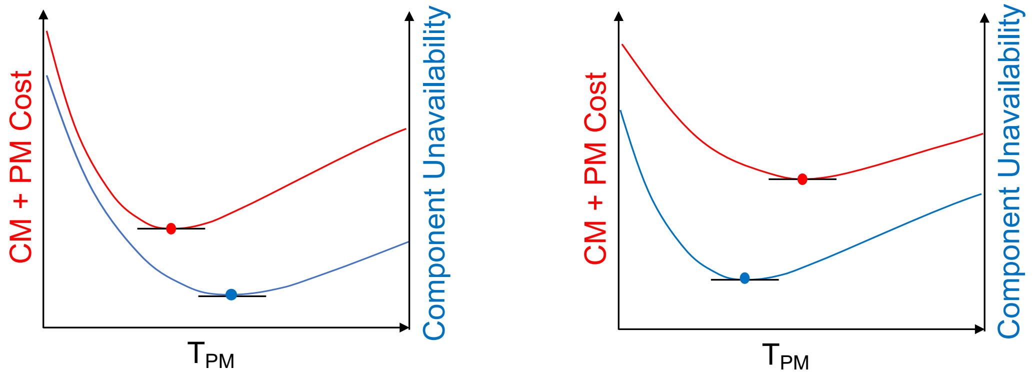
Note that here we have not included the costs associated with system failure; in such a case, we should expand Equation (9) as follows:

$$Cost^{sys} = \sum_{i=1}^{N} \overline{Cost_i^{Maint}} + U^{sys} \cdot Cost^{failure} \tag{24}$$

where $Cost^{failure}$ represents the cost associated with system failure; this term might include costs related to loss of power generation, regulatory costs, etc.

8.3 Balancing Unavailability and Costs

From Equations (17) and (21) note that component unavailability and maintenance costs are correlated variables, i.e., we cannot consider them separately when performing any type of decision. In addition, each component is part of a system which imposes its own reliability requirements. Hence, we can move from Figure 5 to a more complete set of figures which depict, at the component level, costs and unavailability as a function of frequency of PM activities (see Figure 12).



(a) (b)

Figure 12. Two possible scenarios for component mainetance cost and component unvailability as function of T_{PM}.

Note that two possible scenarios can exist depending on the locations of the costs and unavailability minima (see Figure 12):

1. Cost minima located prior to unavailability minima (see Figure 12 - a): moving away from the optimal unavailability point for higher T_{PM} values will negatively affect both costs and component unavailability. For this case, PMs should not be reduced since doing so will result in both degraded performance and higher costs; therefore, no further optimization is possible.
2. Cost minima located after unavailability minima (see Figure 12 - b): moving away from the optimal unavailability point for higher T_{PM} values will negatively affect component unavailability but will reduce maintenance costs. For this case, judgement will be required as optimization of one element (e.g., cost) can only occur at the expense of the other variable of interest (e.g., SSC unavailability).

Thus, in a mathematical form the objective to risk-informed maintenance optimization is as follows:

$$\min_{T_1^{PM},\dots,T_N^{PM}} \sum_{i=1}^{N} \overline{Cost_i^{Maint}} \qquad \text{with } T_i^{PM} > 0 \;\; \text{for } i = 1, \dots, N$$

$$\begin{aligned} s.t. \quad & FT(\tilde{u}_1, \dots, \tilde{u}_N) < \tilde{u} \\ & \overline{Cost_i^{Maint}} = \frac{Cost_i^{PM} + P^F \cdot Cost_i^{CM}}{T_i^{PM}} \\ & \tilde{u}_i = p_i^{PM} + \frac{T_i^{DT}}{T_i^{PM}} + P^F \end{aligned} \tag{25}$$

8.4 Single Component Example

An example of costs and unavailability plots are shown in Figure 14 for a component having reliability and cost data indicated in Table 44. Provided the reliability values in Table 44, probability of failure for the considered component as a function of time by employing Equations 18 and 19 is plotted in Figure 13.

Table 4. Data for the single component analysis example.

$\lambda_{i,0}$	1.0 E-8 h^{-1}
a_i	1.0 E-9 h^{-2}
p_i^{PM}	5.0 E-3
T_i^{DT}	48 h
$Cost_i^{PM}$	400 $
$Cost_i^{CM}$	30,000 $

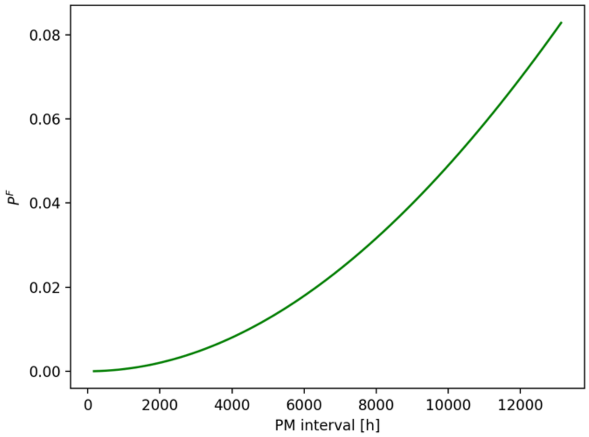


Figure 13. Component probability of failure as function of PM interval T_{PM}.

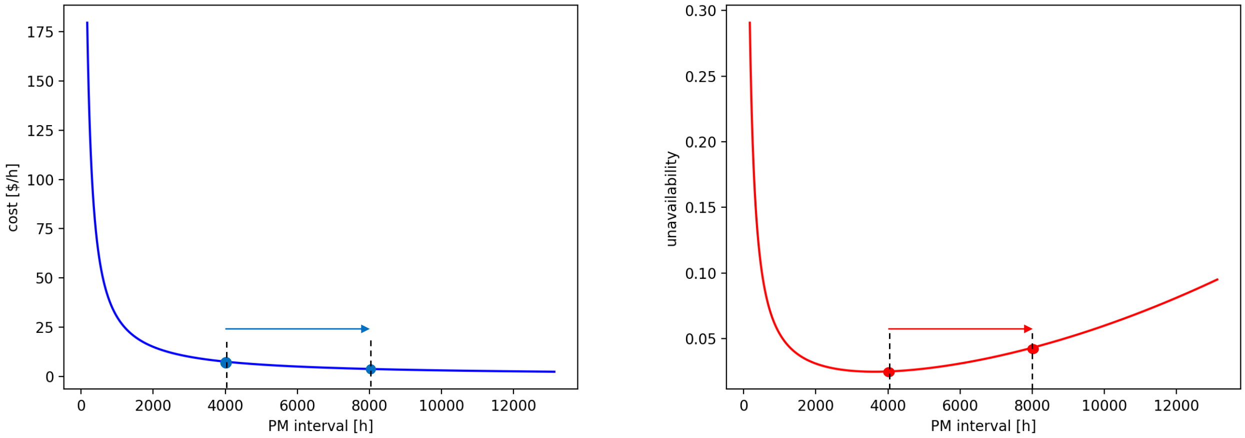


Figure 14. Cost and unavailability plot for the single component analysis example as function of PM interval T_{PM}.

In this case, note how, a change of T_{PM} from 4,000 h to 8,000 h causes a change in maintenance related costs and unavailability as shown in Table 55.

Table 5. Change in component maintenance cost and unavailability for provided data listed in Table 44.

T_{PM} [hr]	Cost [$/h]	Unavailability
4,000	7.58	2.5 E-2
8,000	3.88	4.31 E-2

In this specific example, the overall saving of maintenance costs for such a single component, considering a 10 year cost planning period, can be calculated as:

$$savings = 10 \cdot 8760 \cdot (7.58 - 3.88) = 324{,}000\ \$ \qquad (26)$$

The question now would be: is a component unavailability increase from 2.5 E-2 to 4.31 E-2 considered significant (such as evaluated by its impact in the existing plant PRA model)? The process of risk-informing plant maintenance would evaluate the overall impact of this proposed PM change on plant safety to provide information to decision-makers on the relative benefits associated with the tradeoff between cost reduction and likely increase in component availability. In achieving the objective of minimizing total maintenance costs, the additional anticipated CM costs associated with the expected increase in component unavailability needs to be evaluated and compared to the expected saving obtained from the extension in PM task frequency over the projected planning period.

8.5 Optimization Approach

The optimization problem described in Equation (11) can be numerically solved by employing gradient based optimization algorithms. Gradient based algorithms are first-order iterative optimization algorithms and they are ideal for this kind of application. The objective is to find the minimum of a function $F(\boldsymbol{x})$: starting from an initial point $\boldsymbol{x}^0$, this is performed by determining at each iteration r the gradient of $F(\boldsymbol{x})$, $\nabla F(\boldsymbol{x})$, and moving to a next point in the direction of the gradient of the function at the current point.

From a point $\boldsymbol{x}^r$ determined at iteration r, the point $\boldsymbol{x}^{r+1}$ at iteration $r+1$ is calculated as:

$$\boldsymbol{x}^{r+1} = \boldsymbol{x}^r - \boldsymbol{\gamma} \cdot \boldsymbol{\nabla F}(x) \qquad (27)$$

The sequence:

$$(\boldsymbol{x}^0, \boldsymbol{F}(\boldsymbol{x}^0)) \longrightarrow \left(\boldsymbol{x}^1, \boldsymbol{F}(\boldsymbol{x}^1)\right) \longrightarrow \left(\boldsymbol{x}^2, \boldsymbol{F}(\boldsymbol{x}^2)\right) \longrightarrow \cdots$$

converges to a local minima of $\boldsymbol{F}(\boldsymbol{x})$.

Note that the solution of Equation (1) lies in an N dimensional input space (T_i^{PM} for $i = 1, \dots, N$) while the output space is a two-dimensional space (system unavailability and system costs). In this framework the variable "system costs" is the variable to be minimized while the variable "system unavailability" imposes a constraint. For the optimization problem described in Equation (1), this constraint can be included in the gradient based optimization algorithm by adding a penalty term on the "system costs" output variable when the condition on the "system unavailability" output variable (i.e., $U^{sys} < \tilde{u}$) is not satisfied.

8.6 Optimization Tool

The optimization problem described in Equations (1) and (11) has been solved using the RAVEN code (see Appendix J) which was developed and currently is maintained by Idaho National Laboratory (INL). This choice has been driven by two factors:

1. Availability of gradient based optimization algorithms that can be applied to any type of model
2. Construction of complex models that include system reliability, component cost, and component unavailability models

Regarding the second factor, we have created the required models considered for the framework described in this report that can be applied to the example problem described here:

- Components
  - Unavailability model (see Equation 3)
  - Costs model (see Equation 7)
- System
  - Unavailability model (see Equation 8)
  - Costs model (see Equation 9)

We have then employed the EnsembleModel feature of RAVEN (see Appendix J) to link all these models together in a single model as shown in Figure 15.

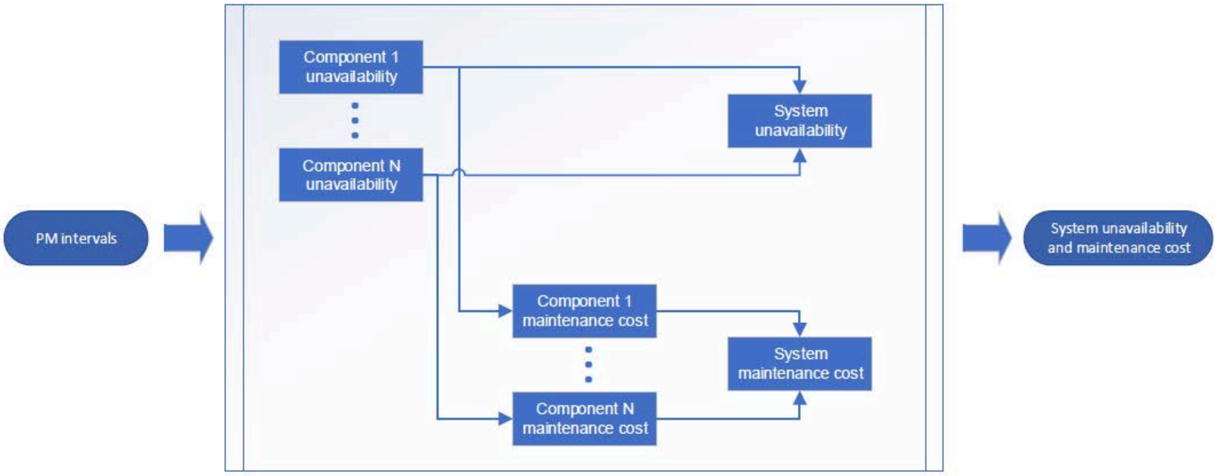

PM intervals
Component 1 unavailability
Component N unavailability
System unavailability
Component 1 maintenance cost
Component N maintenance cost
System maintenance cost
System unavailability and maintenance cost

Figure 15. Graphical representation of the RAVEN EnsembleModel for a generic system maintenance scheduling optimization problem.

8.7 Analysis Example

For this research, a proof of concept use case use case was developed that considers a Pressurized Water Reactor (PWR) High Pressure Injection (HPI) system [40-41]. As shown in Figure 16, the HPI system consists of a set of valves and pumps that are required to maintain redundancy and increase system availability. For this case, we employed the data shown in Table 66.

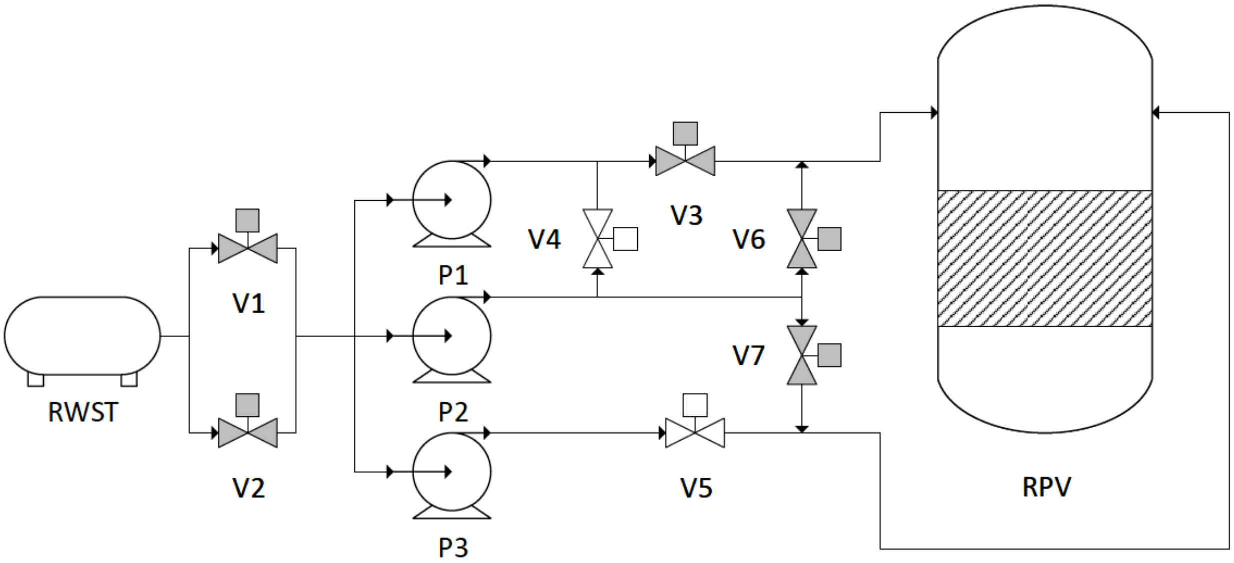


Figure 16. Graphical representation of the considered PWR HPI system.

Table 6. Reliability and cost data for the components of the HPI system of Figure 16.

	Valves	Pumps
$\lambda_{i,0}$	2.08 E-7 h^{-1}	6.05 E-8 h^{-1}
a_i	1.0 E-9 h^{-2}	1.0 E-9 h^{-2}
p_i^{PM}	1.0 E-3	1.0 E-2
T_i^{DT}	24 h	48 h
$Cost_i^{PM}$	400 $	3,000$
$Cost_i^{CM}$	30,000 $	60,000 $

The goal is to determine $T_{V_i}^{PM}$ $(i = 1, \dots, 7)$ and $T_{P_j}^{PM}$ $(j = 1, \dots, 3)$, provided the constraint:

$$P(HPI) = 1.0\,E - 3 \tag{28}$$

Appendix G provides more details about the reliability modeling of the HPI system.

With the data provided in Table 66 and the constraint shown in Equation (14) we were able to generate the optimal PM intervals for valves and pumps indicated in Table 77. As also indicated in past maintenance optimization methods [40], components with identical reliability and cost data have identical T^{PM}: valves have a PM interval of 6523 h while this value for pumps have been determined to 8242 h. These values minimize maintenance costs while maintaining system unavailability below a fixed threshold. For the calculated values for T^{PM}, the resulting system unavailability is 9.98 E-4.

Table 7. Optimal PM maintenance schedule for the components of the HPI system shown in Figure 30.

Component ID	T^{PM} [h]
P_1	8242
P_2	8242
P_3	8242
V_1	6523
V_2	6523
V_3	6523
V_4	6523
V_5	6523
V_6	6523
V_7	6523

8.8 Maintenance Optimization Under Uncertainty

The input data listed in Table 66 are point values while in real applications these values might be affected by uncertainties. In particular, this is valid for the set of SSC reliability parameters. In this situation a question may arise: how is it possible to solve this optimization problem when data are affected by uncertainties? To complete the analysis shown in Section 8.7, we have conducted an additional analysis which focuses on the propagation of uncertainties in the optimization model.

We have associated uncertainties to the parameters a_i of valves and pumps in the form of probabilistic distributions. For simplicity we have chosen an identical distribution[b] for the parameters $a_i \sim U[5.E-10,1.E-9]$. Note that these distributions are independent even thought they are identical.

In this respect we have employed again the RAVEN code (see Appendix J) and, in particular, we leveraged the RAVEN capability to run itself in a master-slave configuration:

- The RAVEN-master portion performs the stochastic sampling of the variables a_i through a Monte-Carlo sampling
- The RAVEN-slave portion performs the identical optimization shown in Section 8.7 using the values sampled by the RAVEN-master portion

When performing this Monte-Carlo sampling of an optimization process a distribution of $T_{V_i}^{PM}$ $(i = 1,\ldots,7)$ and $T_{P_j}^{PM}$ $(j = 1,\ldots,3)$ is obtained instead of point values (as shown in Table 77). Note that such distributions are correlated to each other.

Provided the set of distribution we have performed such analysis by generating 1000 Monte-Carlo samples of $\{a_i\}$ and obtained the same number of values for $\left\{T_{V_i}^{PM}, T_{P_j}^{PM}\right\}$. Since we have associated a distribution to a_i, then instead of having a single unavailability line as shown in Figure 14 (left) we have a distribution of unavailability. Figure 17 shows a distribution for component unavailability, see Equation (17), for pump P_1 (see Table 66) generated by sampling $a_{P_1} \sim U[5.E-10,1.E-9]$ using Monte-Carlo sampling.

[b] We use the notation $a_i \sim U[a,b]$ which indicates that a_i is a stochastic variable which is uniformly distributed between the values a and b.

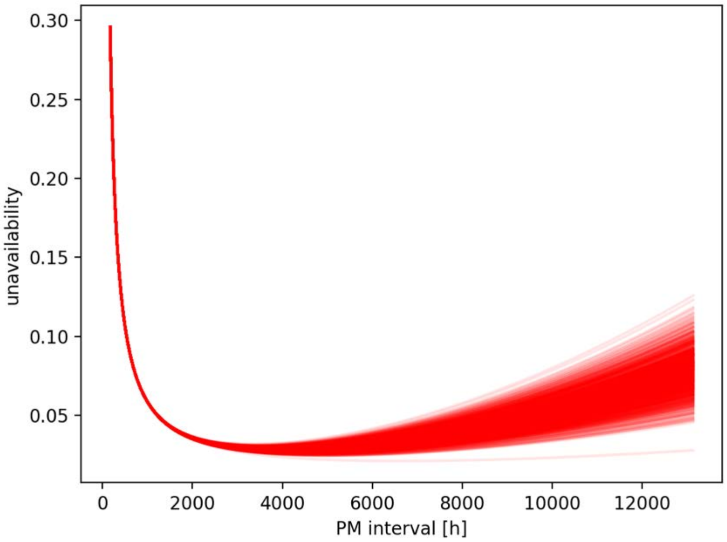


Figure 17. Density distribution for pump unavailability with $a_i \sim U[5.E-10, 1.E-9]$.

The obtained results are shown in Figure 18. Similar to the analysis of Section 8.7, the obtained distributions are identical among $T_{V_i}^{PM}$ and $T_{P_j}^{PM}$. Figure 18 shows the correlation between the distributions of $T_{V_1}^{PM}$ and $T_{P_1}^{PM}$ by plotting the full distribution in the $T_{V_1}^{PM} - T_{P_1}^{PM}$ space and the marginal distributions for $T_{V_1}^{PM}$ and $T_{P_1}^{PM}$ (top and left histograms).

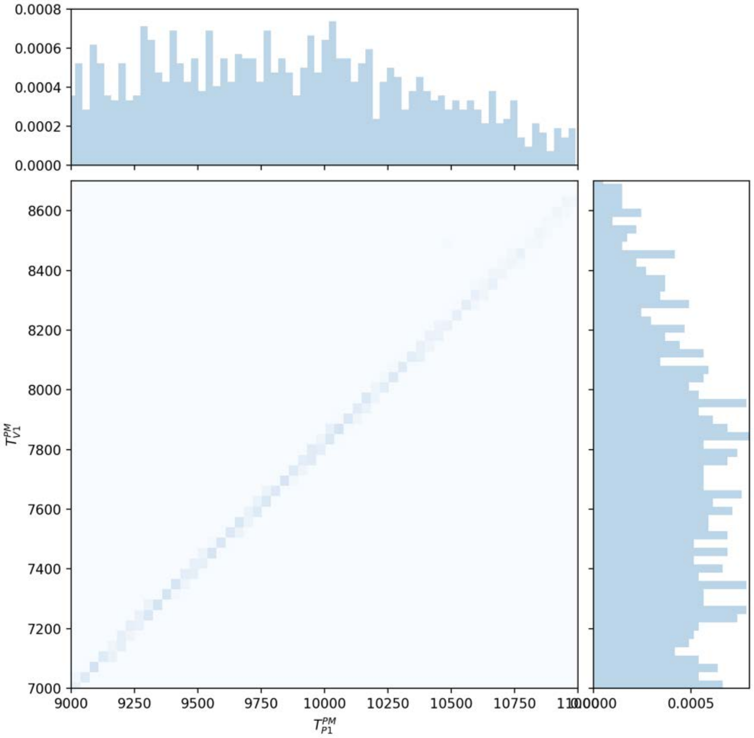


Figure 18. Density plot for T_{V1} and T_{P1}.

8.9 Model Improvements

As indicated in the previous sections, the presented optimization method employs the minimum amount of information required to perform risk-informed maintenance optimization. An important advantage of this method is that the required information can be easily retrieved by existing plant databases. In the near future we are planning to improve the presented optimization method by adding the following items:

1. **Link PHM data to reliability parameters.** Parameters such as $\lambda_{i,0}$ and a_i can be automatically calculated by existing PHM databases. This automatic link could allow plant owners to update maintenance schedules when new maintenance and failure reports (at the plant but also at the fleet level) are generated and updated in plant PHM databases.
2. **PM activities efficiency (i.e., not as good as new).** In this work we have assumed that, once a PM activity is performed, the component is considered as good as new. This may be not the case for some specific components. Depending on data availability, this assumption can be relaxed in order to get a more realistic optimal preventive maintenance solution.
3. **Adaptive (i.e., time dependent) generation of $\boldsymbol{T_i^{PM}}$.** The proposed methodology has T_i^{PM} characterized by a fixed length. This is in particular relevant when items 1 and 2 are both considered in the analysis. In this case, T_i^{PM} might change in time; i.e., large T_i^{PM} when ageing effects are negligible and smaller T_i^{PM} when component ageing is largely affecting component unavailability. Such an adaptive approach may be useful to optimize required ageing management plans for NPPs that are operating in periods of extended operation un license renewal (or second license renewal).
4. **Include supply chain models.** The term $Cost_i^{CM}$ only includes procurement and installation costs. A more detailed model could include the ability to procure the component or its associated subcomponents on the open market. This could be accomplished by developing more detailed supply chain models that could generate more realistic $Cost_i^{CM}$ values.
5. **Costs model for system failure event.** The term $Cost^{sys}$ should include the costs associated with system failure; this term might contain costs related to loss of power generation, regulatory costs, etc.
6. **Propagation of uncertainties.** As of now we have included point values for both component costs and unavailability data. In reality, these data might be affected by uncertainties that would change the optimal maintenance schedule. In the near future we will include the analysis of uncertainties on input data and how they propagate to the output variables.
7. **Sensitivity analysis of obtained solution in respect to input parameters.** This item is linked to the previous one. Even though data are affected by uncertainties, the sensitivity of the optimal maintenance schedule with respect to the input variables might change from variable to variable. Hence, a ranking of the most relevant input variables might provide guidance to the plant owner on which variable would require an uncertainty reduction to achieve improved optimizations.
8. **Extend maintenance schedule optimization from the system to the plant level.** The methodology presented in this work has focused on only a single system. However, a power plant is a network of systems and plant safety parameters such as CDF or LERF are strongly affected by unavailability of all these systems. This can be solved by linking together the full plant PRA, component unavailability models to PRA basic events, and component-system-plant cost models.

9. GENERATION RISK MODELS

The Generation Risk Assessment (GRA) model presented here centers on the main feedwater system of a generic 4-loop PWR. The development of the model supports the PHM initiative. The risk to a generic NPP associated with the Main Feed Water (MFW) system is assessed from an economic perspective. The most vulnerable aspects of the system are quantified in terms of economic loss due to equipment failure and unavailability.

NPP owner / operators are economically vulnerable due to equipment failure and unavailability. Power plants need an effective tool to evaluate these economic risks. Plants are well versed in the use of PRA to evaluate plant safety risks [51]. PRA methods can be utilized to evaluate economic loss imposed on power plants via GRA [60]. GRA is the process of predicting the risk of generation loss by estimating the probability and duration of a power plant trip or derate due to equipment unavailability.

In GRA, like PRA, the risk is defined as the product of equipment failure frequency and the associated consequence. The equipment failure frequency and the associated consequences can be derived using generic plant data in conjunction with plant response models. A GRA model is comprised of a collection of top logic representing combinations of key components whose failure can result in a plant trip or derate. The development of GRA models is similar to the development of PRA models; however, rather than estimating things like core damage frequency, the output of a GRA model is lost generation for a defined time period. The lost generation is expressed in terms of electrical megawatt hours per year not produced due to plant trips and derates. The value of megawatt hours per year can be expressed in dollars per year using an average dollar price per megawatt hour [63].

GRA modeling can provide insights to power plant health management by identifying components, trains (combinations of components), and systems (combinations of trains) susceptible to failure. The model presented in this report identifies the vulnerable equipment of a generic 4-loop pressurized water reactor's main feedwater system [56].

9.1 Generic MFW System

The MFW system provides water flow from the feedwater pumps to the steam generators in a PWR (of which there are four, on per loop, in our generic example NPP). The system consists of the piping, valves, pumps, heat exchangers, controls, instrumentation, and associated equipment that supply the steam generators with heated feedwater in a closed steam cycle using regenerative feedwater heating. Figure 19 shows a typical PWR arrangement with a dotted line outlining the feedwater system.

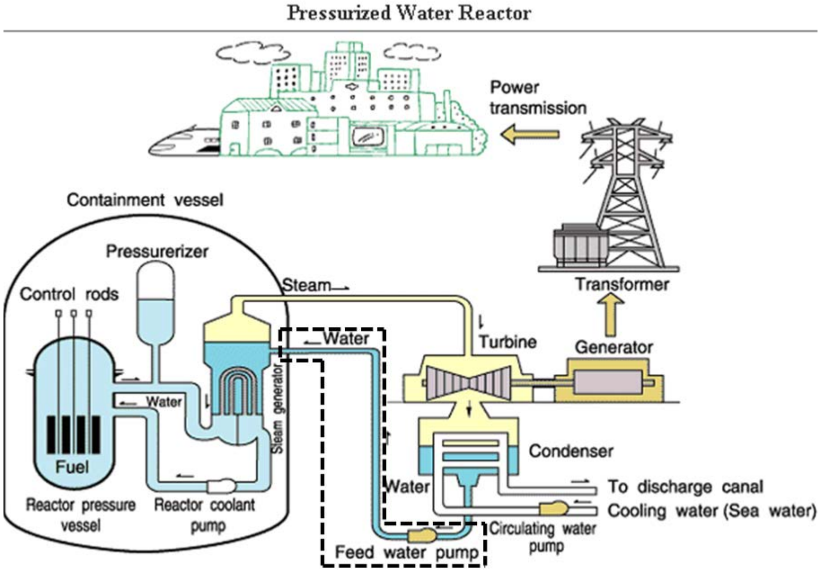


Figure 19. PWR NPP plant overview.

Figure 20 shows the simplified feedwater pathway in the system during normal operation. There are three feedwater pumps with common suction and discharge headers. Each feedwater pump provides sufficient flow to support 50% of the reactor's rated power. Two high-pressure feedwater heaters and a heater bypass are used to control feedwater temperature during normal plant operation. Each heater provides sufficient heating to support 50% of the reactor's rated power. Feedwater flow is delivered to four steam generators. Each steam generator supports 25% of the rated power.

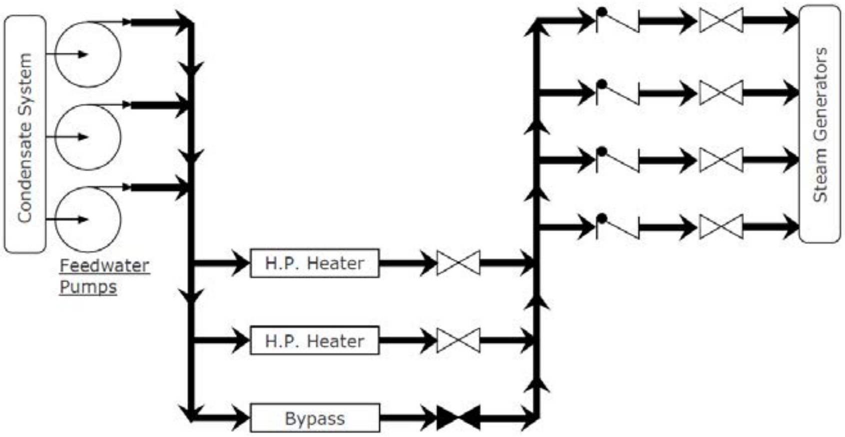


Figure 20. Feedwater system flow diagram.

The generic PWR unit we are considering is capable of an electrical output of 1000 megawatts. The preceding description provides the template for the generic feedwater system and power generating plant evaluated in this study. The model was genericized through the implementation of generic failure data, as well as generic NPP operating characteristics. The GRA model results are thus interpreted as averages over all PWR power plants in the U.S..

9.2 Modeling the Main Feedwater System

System availability models, generic feedwater schematics, Failure Modes and Effects Analyses (FMEAs), and data from the Equipment Performance and Information Exchange (EPIX) and the North American Electric Reliability Corporation Generating Availability Data System (NERC-GADS) were used to develop the model and identify contributors to lost generation. The system availability model was evaluated based on the successful transport of water from the feedwater pumps to the steam generator inlets.

An availability block diagram was created to break the modeling process into logical blocks, i.e. trains of the system, to reflect the different derate levels that could occur within the system. Figure 21 shows the availability block diagram for the feedwater system to support 100% power.

After analysis of the availability block diagram was completed, the trains of the system were broken down into the comprising components. FMEAs were conducted to identify components necessary for power generation. Each component modeled was given a conventional naming scheme for organizational purposes and a list of all the component names, the location of the components, and the purpose of the components was created. Components whose unavailability could cause plant derating were identified as key components [53].

Once the key components were found in the MFW system, the component failure modes were incorporated into fault trees. The top logic was defined by the ability of the feedwater system to support more than 0%, 50%, and 75% power. The fault trees were modeled in the SAPHIRE [158] software package using a combination of "OR" and "AND" logic gates to represent how component unavailability affects the top logic. Repair and recovery times were integrated into the model to determine the effective full power hours of lost generation due to the basic events in the fault trees. A list of minimum cut sets was generated along with the percentage of contribution to the resultant loss of generation due to the cut set.

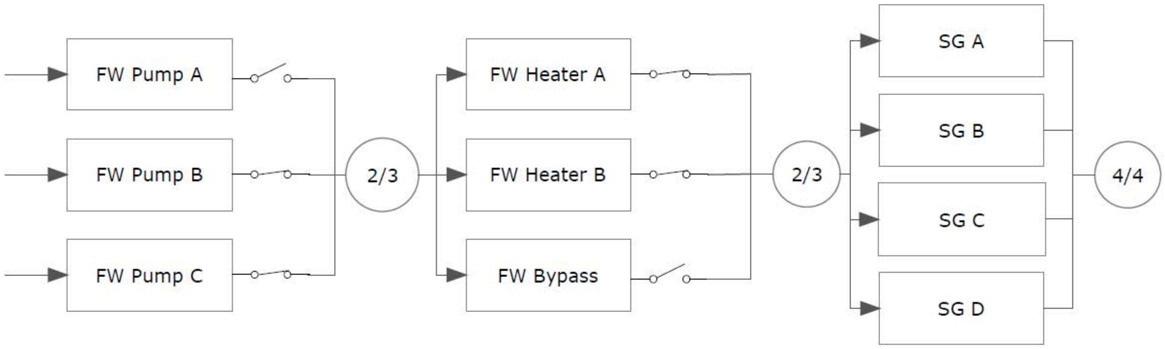


Figure 21. Feedwater system availability block diagram for 100% power.

FV and RAW importance measures were generated for each basic event evaluated in the study to obtain a four-quadrant plot comparing risk reduction and risk increase potential. Test and maintenance unavailability were not considered due to variations from plant to plant. However, human errors, random failures, common cause failures, repair times, and recovery times were accounted for in the modeling process.

The data sources were the EPIX and the NERC-GADS pc-GAR database. EPIX provides an industry average component failure distribution [59]. A majority of the failure information was found in the 2015 update of the Summary of SPAR Component Unreliability Data and Results spreadsheet; the source for developing the spreadsheet was EPIX for the years 1998 - 2015. The pc-GAR database for the years 1985 - 1990 was used for MTTR data and failure data absent from the EPIX spreadsheet [60-61]. The NERC database provides a consistent data retrieval method for a majority of the NPPs in Canada and the U.S. . The use of all of the nuclear power generating units reporting to NERC provides an average set of repair and failure data. Further details of modeling the main feedwater system are given in the appendices.

Appendices H and I provide more details about the reliability modeling of the MFW system and the obtained results which are summarized in Section 9.3.

9.3 MFW GRA Results

The results obtained through SAPHIRE identified the main contributors to economic loss in the MFW system. The GRA model determined the piping, valves, pumps, and heaters are the main contributors to lost generation in the feedwater system. Table 8 displays the estimated contribution to the lost generation. In Table 8, the "Count" column is the number of components evaluated in the study for the category. For example, 69 sections of piping were evaluated throughout the feedwater system.

The numerical results are somewhat difficult to fully gauge whether they are typical to industry experience due to the uniqueness of the model. Exclusion of testing, maintenance, and repair costs likely have led to lower than the industry average values. Nonetheless, component contributions relative to each other correlate well with previously conducted GRA results. GRA models, such as Cooper Nuclear Station's model on the main feedwater/condensate system, also imply the contribution to lost generation from high-pressure heaters for the generic model is relatively low.

Table 8. Component and system costs due to failures.

Category	Count	Lost Generation (per year)	
Pipes	69	$28,000	800 MWh
Valves	65	$110,000	3000 MWh
Pumps	3	$150,000	4000 MWh
Heaters	2	$28,000	800 MWh
Feedwater System	1	$340,000	10,000 MWh

It is worthwhile to note how a key assumption made in the development of this generic GRA model differs from the Cooper model [49]. The generic power plant model here assumes an on-line maintenance capability when the failure of one heater occurs. To see how the assumption affects the results, the 100% derate model was modified to see how the contribution to lost generation would change. Figure 22 shows the total lost generation comparison when the capability of online repair to either heater is modified.

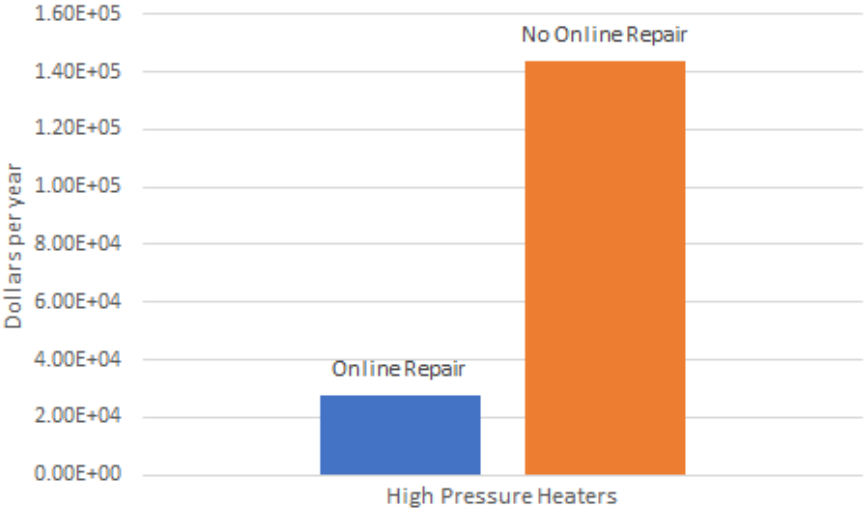


Figure 22. High-pressure heater repair assumption lost generation comparison.

When the capability of online maintenance is removed from consideration, the impact on lost generation due to the high-pressure heaters increases by a factor of five. Further financial analysis on this finding may be considered for power plants without the online repair capability of high-pressure feedwater heaters [54]. Alternatively, even for NPPs with such capability, these results indicate it may be beneficial to perform PM activities on the heater isolation valves to ensure the capability of isolating a heater if necessary. If it is determined not to perform such PMs on the isolation valves, if a failure of the respective heater should occur, the plant may no longer be capable of performing the necessary corrective maintenance while the NPP is operating, necessitating a plant shutdown, and the additional incurred costs (including lost generation costs) that would ensure.

Plotting risk increase potential and risk reduction potential importance measures for basic events supports plant health management by assisting in identifying targets for improvement. The four-quadrant plot highlights categories of basic events with the highest risk reduction and risk increase potential importance measures. The measures for each basic event category for this example are shown on a log-log plot in Figure 23.

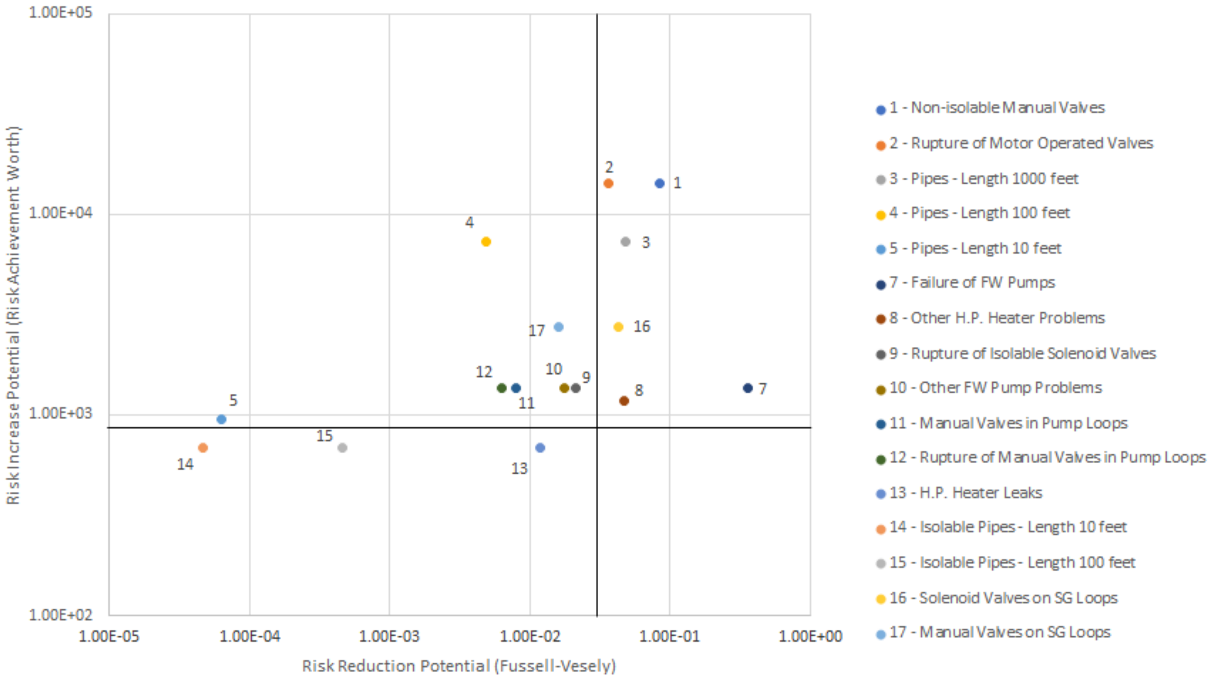


Figure 23. Feedwater system four-quadrant plot.

Plotting the two importance measures for each basic event category on a four-quadrant plot provides valuable insights for managing generation risk. The thresholds in the plot should be viewed as large bands of grey due to the current application. Threshold lines in four-quadrant plots are used to weigh cost-benefit risk-mitigating decisions for proposed component modifications [58]. The relationships of the components with one another is useful for analysis. The events furthermost to the right contribute significantly to risk. The lower the events the less additional impact on the risk the events would have if they were to degrade. Thus, components rightmost and lowest, such as the feedwater pumps, may be candidates for design modification or replacement decisions, particularly in the context of long-term asset management associated with plant life extension decisions. The location of the component failure categories for the feedwater system is comparable to the results obtained from other GRA models. A more detailed discussion of this finding is found in the appendices.

The uncertainty distributions for the component failure rates were given on the EPIX spreadsheet. The uncertainty for the rates was based on a gamma distribution. Any basic event failure rate not obtained from the EPIX spreadsheet was assigned a conservative uncertainty value. Table 9 shows data from the spreadsheet and how the uncertainty distribution was given.

SAPHIRE utilized the Monte Carlo evaluation method to obtain the uncertainty in the top event. The uncertainty evaluation was based on the probability of a plant trip or derate occurring per 24 hours due to the unavailability of equipment. Therefore, the failure rate and the mean time to repair values of the components were taken into consideration. The probability density functions, as well as a more detailed discussion, are provided in the appendices.

Appendix N provides an alternative approach to analyze GRA models by considering success path instead of Minimal Cut Sets.

Table 9. SPAR component unreliability data.

Description	Failure rate [hr^{-1}]	Distribution	α
Turbine-driven pump external leakage (small)	5.38E-07	Gamma	15.5
Motor operated valve fails to remain open	3.24E-08	Gamma	0.593
Hydraulic valve fail to control	4.57E-07	Gamma	42.5

9.4 GRA Modeling Considerations

A generic 4-loop PWR MFW system centered GRA has been performed. The GRA was performed to evaluate the utility of GRA applied to PHM. The GRA results provide an effective mechanism for justifiable identification of leading contributors to generation risks. The GRA results also provide the complementary benefit of identifying low worth contributors to generation risks. While the GRA model described here provides useful insight, several additional features can be implemented which will magnify the benefit. Key among these additional features are accommodation of degradation, testing and maintenance, and the integration of supporting and preliminary systems.

NPPs have severe environmental and operating conditions leading to a variety of degradation mechanisms [42]. Active degradation mechanisms affect GRA models through the addition of time-dependent failures [57]. Evaluating how a component failure or unavailability increases over time becomes a valuable tool in the long-term planning of a NPP. The integration of degradation to the GRA model in this report can be done through the use of time-dependent software compatible with SAPHIRE (or other similar.

Testing and maintenance also have influence on lost generation in NPPs. Degradation results in increased costs due to increased testing and maintenance requirements. Evaluating the costs associated with these time-dependent and non-time dependent activities is important in economic evaluations. The costs associated with testing and maintenance of components of the generic feedwater system can be incorporated into the GRA model developed.

Supporting systems to the generic feedwater system must be operable for the feedwater flow to be successfully transported to the steam generator inlets. Although supporting systems are subject to an entirely new degradation model in themselves, the results can provide helpful insights. Incorporating supporting system GRA models with the model in this report highlights the interdependencies of components at a larger power plant level. Important economic decisions may be based on the findings of the interdependencies and the values of generation loss.

The feedwater system has preliminary processes that must occur to effectively deliver heated water to the steam generators. The condensate system must successfully perform its design functions for the feedwater system to operate correctly. The addition of the condensate system in the generic plant evaluated in this study can also be incorporated directly into the GRA model. Economic decisions are often made on the main feedwater and condensate systems collectively. Evaluation of the condensate system in conjunction with the feedwater system would provide insights into additional plant health management decisions.

It is noted here that, to date, although the technology to develop and apply GRA models is straightforward; the technology has not been widely applied at NPPs. This is predominantly due to the costs (or perceived costs) associated with developing GRA models. Industry experience has shown that PRA-type models are labor intensive and expensive to develop and maintain. As a result, if the GRA techniques described in this section are to achieve widespread adoption to support system health management programs, techniques will need to be developed to substantially reduce these costs. Since all U.S. NPPs have full plant PRA models, one such option is to modify these models so as to permit them to evaluate the impact on plant production and economics related to system health and asset management decisions. Development of such methods (and supporting tools) represents an area for research.

10. SSC MAINTENANCE AND MONITORING

As a result of intense global competition, companies are considering novel approaches to enhance the operational efficiency of their products. For some products, high in-service reliability can be a means to ensure customer satisfaction. For other products, increased warranties, or at least reduced warranty costs, and a reduction in liability due to product failures, are incentives for manufacturers to improve field reliability and operational availability.

PHM is a multi-faceted discipline for the assessment of product degradation and reliability. The purpose is to protect the integrity of the product and avoid unanticipated operational problems leading to mission performance deficiencies, degradation, and adverse effects on mission safety. More specifically, prognostics is the process of predicting a system's Remaining Useful Life (RUL) by estimating the progression of a fault given the current degree of degradation, the load history, and the anticipated future operational and environmental conditions. Health management is the process of decision-making and implementing actions based on the estimate of the state of health derived from health monitoring and expected future use of the product.

In general, PHM consists of sensing, anomaly detection, diagnostics, prognostics, and decision support, as shown in Figure 24. The objective of sensing is to collect a history of time-dependent operation of a product, the degradation of materials, and / or the environmental loads on the components of a product or the total product.

The primary purpose of anomaly detection is to identify strange or unusual or unexpected (anomalous) behavior of the product by identifying deviations from nominally healthy behavior of the product. The results from anomaly detection can provide advanced warnings of failure, often referred to as failure precursors. Note that anomalies do not necessarily indicate a failure because changes in operating and environmental conditions can influence sensor data to show anomalous behavior. However, even this type of anomaly information is valuable to product health management, because it can indicate an unexpected use.

Diagnostics enables the extraction of fault-related information, such as failure modes, failure mechanisms, quantify of damage, and so forth, from sensor data caused by anomalies in the products health. This is a key piece of information that feeds into maintenance planning and logistics.

Prognostics refers to predicting a product's RUL within appropriate confidence intervals, which often requires additional information not traditionally provided by sensors, such as maintenance history, past and future operating profiles, and environmental factors. Based on predictions, the goal is to inform decision makers of potential cost avoidance activities, and to ensure safe operation. That is, the aspects of PHM are to effect appropriate decision making; to prevent system's catastrophic failures; to increase system availability by reducing downtime; to expend maintenance cycles; to execute timely repair actions; to lower life-cycle costs from reductions in inspection and repair; and to improve system qualification, design, and logistical support. In Appendix L we summarize in more details the most advanced PHM methods that are currently available. In Appendix K we provide a summary of methods for supply-chain surveillance for PHM systems. In Appendix O we provide a summary of condition assessment approaches for both active and passive components.

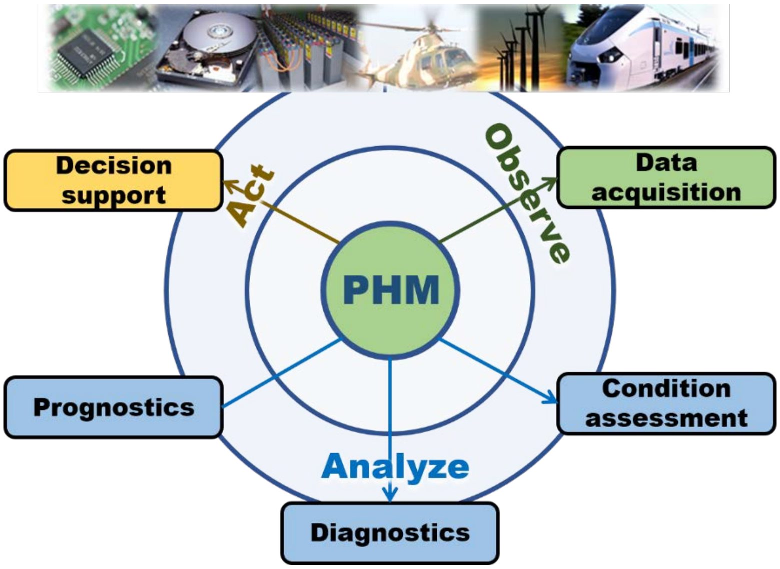


Figure 24. Framework for prognostics and health management.

11. LINK WITH RIAM PROJECT

The Use Case related to development of a modern, integrated, risk-informed system health program has significant commonalities to the Use Case that is developing a RIAM program. Although these two Use Cases are similar in that they focus on plant equipment and system performance, they possess different emphases in objectives and timeframes. This is characterized in Table 10.

Table 10. Emphases and timeframes for system health and asset management Use Cases.

Program	Primary Timeframe	Primary Focus
System Health	Short to Intermediate Term	Engineering
Asset Management	Intermediate to Long Term	Financial

As described in Section 7 of this report, the conduct of NPP ER programs are developed and implemented in accordance with INPO AP-913 [5]. Additionally, as described in Section 7 of this report, regulatory focus via the Maintenance Rule as implemented by the industry in NEI 93-01 [2] focuses, to a large extent, on the reliability and availability of plant SSCs [2]. As a result, plant system health programs have tended to focus predominantly on the engineering aspects related to ER. Additionally, focus on items such as Maintenance Rule performance, in particular addressing performance deficiencies associated with plant SSCs classified as (a)(1) or for SSCs which possess small amounts of margin for the MSPI program [4], has focused attention on issues that are short to intermediate term in nature. One indicator of this focus can be seen in the content of industry sponsored research to support plant ER programs. This research typically is sponsored by the EPRI under the Plant Engineering Program. The results of this research are used by operating NPPs around the world to support plant ER programs. To support widespread adoption of the outcomes of this research EPRI periodically publishes a report (which is publicly available) that lists all of the products developed from this research. A review of the most recent of these reports [42] indicates a large portion of the research focuses on the engineering aspects of plant ER and also focuses on the short and intermediate term needs of the operating NPPs.

In contrast, RIAM applies a combination of financial and engineering evaluation methods to apply risk management technology to support plant long-term planning and investment. RIAM is intended to provide decision makers with both qualitative and quantitative information related to investments in asset management with an objective of optimizing long-term economic value while effectively identifying and controlling enterprise risks. As a result, RIAM is most closely aligned with the Life Cycle Management (LCM) portion of AP-913 which has a longer-term focus than the other portions of that industry guidance document.

An important set of methods and tools to support NPP LCM efforts and, in particular, their application to NPPs that are anticipating operating during extended periods of operation (i.e., periods of license renewal) is Integrated Life Cycle Management (ILCM) developed by EPRI. The ILCM method [43] addresses the management and optimization of large capital projects for the purposes of extended plant operation. The ILCM approach is an evaluation method that consists of a sequence of structured evaluations. ILCM methods and accompanying software are available to EPRI member utilities; it should be noted that since all U.S. NPP owner / operators are EPRI members, ILCM is available to all operating U.S. NPPs. Important elements of ILCM are described in the LWRS RIAM Use Case report that is being published simultaneously with this report [44].

Although the two Use Cases have different emphases, it is evident that they are closely related. For example, development of long-term asset management plans related to plant life extension will be dependent upon the effectiveness of the management of the health of plant SSCs achieved by the plant ER program. Conversely, anticipated financial restraints related to either current ER programs or for future investments can have an impact on decisions related to the reliability and performance of plant SSCs. As a result, as the two Use Cases related to system health and risk-informed asset management progress, the LWRS collaboration is planning to work with both host utilities to coordinate activities to more fully integrate the approaches to the greatest extent practicable. Some key areas where these collaborations are anticipated to occur are the following:

- Evaluation of the impact of short to intermediate term investments on long-term system performance including potential impacts on plant risk (both safety and economic) and impacts on long term capital investment needs.
- Evaluation of the impact of long-term investment alternatives system performance, particularly with respect to the impacts of investment limitations and deferrals on plant risk (both safety and economic).

12. ARCHITECTURE FOR RI-PSH

The objective of this section is to present an architecture to manage and control plant risk, efficiency and operations. The material presented here looks more in the near future when the PHM project and the RIAM project will converge on the same tracks. This will happen when we will integrate PHM data and models to inform and update RIAM models for optimization of plant resources. In addition, we are planning to integrate several other plant structures such as supply chain and plant safety to permit achieving an integrated framework to address both short and long-term asset management decisions.

The idea behind the term "architecture" is that several plant activities are strictly/loosely depending on each other and on external factors (e.g., power demand and energy price). In addition, these plant activities are also heterogenous in nature, i.e., they control different aspects of the plant (e.g., plant operation, plant finance, plant risk, etc.).

In a NPP these activity dependencies are more or less considered and controlled by "passing data" from one activity to the other. This process of "passing data" is not always automatized and plant benefits likely would emerge from the creation of this automatization. As an example, the PHM project has focused during this past year on the integration of risk-informed applications with plant health management. An application is the optimization on plant maintenance schedules based on plant heath data and system risk models. Another example is the RIAM project were plant resources and plant health data are employed to identify an optimal schedule for replacement/refurbishment of capital component, with particular emphasis to support plant life extension activities (including second license renewal).

Note that for both of these examples, there is a direct connection between plant operations, economics and safety. The objective of this architecture is to create these automatized links between these entities, and we will employ a Model Based System Engineering (MBSE) approach to create such automatized linking.

MBSE is an emerging approach in the discipline of System Engineering (SE) which can be described as "the formalized application of modeling principles, methods, languages and tools to the entire lifecycle of large complex, interdisciplinary, sociotechnical systems" [151]. Compared to classical SE approaches which are based on the *system-as-machine paradigm*, MBSE is based on *system-as-organism paradigm*. In other words, MBSE evolves SE approaches to explicitly consider large highly complex, adaptive and human-interactive systems. The artifact generated by a MBSE approach is a *system model* developed in a pre-defined modeling language and appropriate tools.

The main computational languages currently employed for MBSE practices are the: Unified Modeling Language (UML) and the System Modeling Language (SysML). Both of these are highly object-oriented graphical modeling languages designed to support SE activities. SysML evolved from UML to supplement UML with additional capabilities: requirements and parametric modeling.

While these approaches and languages have been employed in SE applications for the design and analysis of complex systems, in recent years MBSE has been employed to perform safety analysis [152]. Such a modeling approach contrasts with the currently employed safety and PRA approaches which are based on much simpler graphical languages such as Event-Trees, Fault-Trees and Reliability Block Diagrams. The advantage of employing a MBSE approach is the higher level of abstraction and detail that can be reached when performing system modeling.

When looking at NPP activities we observe several entities (e.g., equipment reliability, PRA) that are coupled to each other (with different degree of coupling). This coupling can be synthesized by the passage of shared models (e.g., reliability models) and data (e.g., maintenance reports). In this report, we have focused on the development of a risk-informed system health program (see Section 4) which links equipment reliability with risk-informed applications. We have shown how these entities are linked to other plant activities (e.g., supply chain and long-term panning); from here, the following inquiries are suggested: can we extend MBSE modeling and languages approaches to integrate into a single analysis framework all plant activities? In other terms, can we automatize as much as possible the interactions among plant activities?

We are proposing a MBSE approach to answer these questions, i.e., we aim to extend capabilities to system design, system safety, and system operation. Figure 25 represents in graphical form how the proposed MBSE-based architecture could be used to support engineering, science, operations and management activities of a NPP. Each plant activity is composed of models, requirements, functions and organization structures which can be translated into MBSE models and then linked to the MBSE models of other plant activities. The objective is to monitor continuously: risk (economic and safety related), costs and efficiency.

These MBSE models will be integrated with risk and reliability models of SSCs which will be continuously updated once new data (e.g., maintenance report or failure data) is generated. Once the MBSE models have been created and linked, the internal analysis engines will:

1. Employ system dynamics models (e.g., economic models, structural models, thermal-hydraulic models, ageing/degradation models) to perform time dependent analysis to forecast future trends
2. Propagate data uncertainties and perform sensitivity analyses

3. Include data analytics methods to identify and analyze patterns

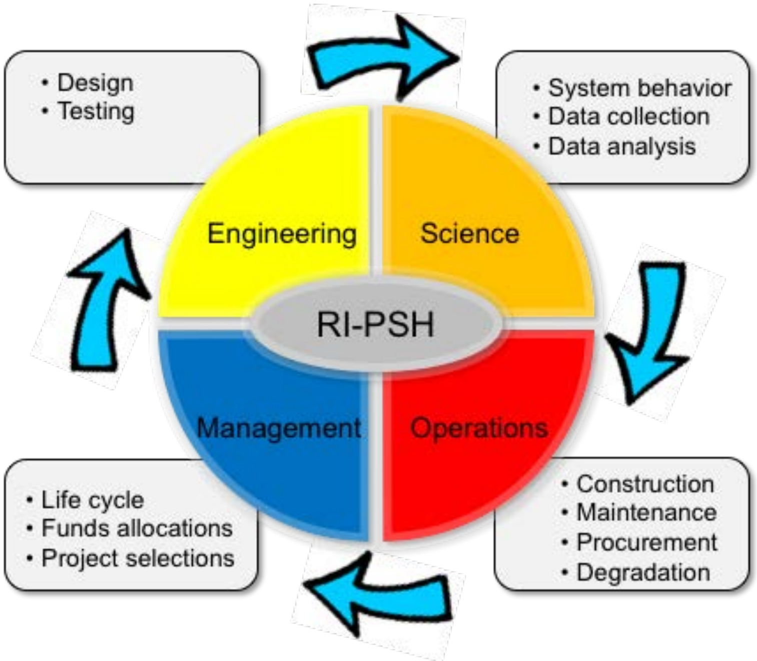
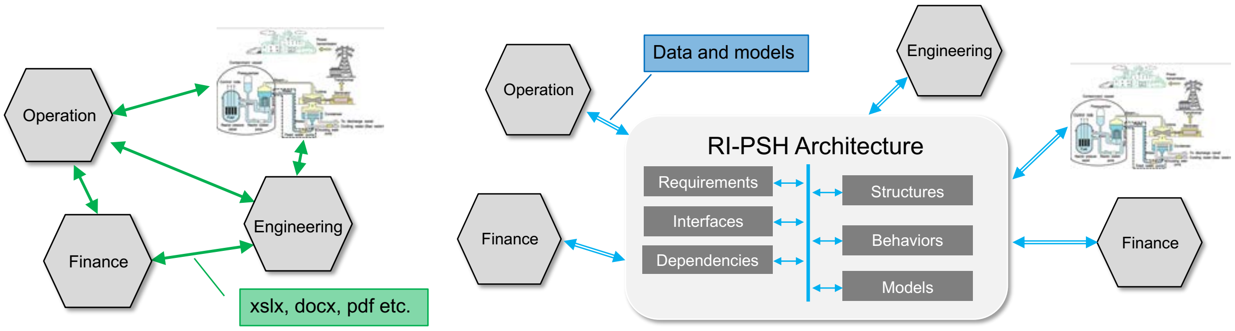


Figure 25. Functionalities of a RI-PSH architecture.

In a graphical form we are aiming to transform plant operation and management from the paradigm shown in Figure 26(a) to that in Figure 26(b). Figure 26(a) depicts the current current state of practice typical for most existing NPPs where several plant activities (i.e., finance, engineering, operations) continuously pass data in different formats across different organizations. This passing of data is not always automatized, and the structure of the data may vary depending on the requested activity or function. Again, the issue is not related to passing data, the issue we are aiming to solve is: can we structure this "passing data interaction" in a more structured, automatized, efficient,, timely, and effective manner?



(a) (b)

Figure 26. Comparison between currently and proposed RI-PSH architecture.

We envision to answer this question by proposing a MBSE approach as shown in Figure 26 (b) where each plant activity provides to the plant MBSE architecture not only data and models but also its structure and behavior, its interfaces and dependencies with other activities, and its requirements. The advantage of such an approach is that the interactions between plant activities are well defined and bounded which allow a well-structured automation. Appendix M shows in more detail how the initial design of the RI-PSH architecture has been performed using MBSE tools.

13. CONCLUSIONS AND NEXT STEPS

This report has summarized the research activities conducted during FY19 for the PHM Use Case project. With the goal to start the development of a RI-PSH program we have begun by 1) identifying its major components and 2) by evaluating which and how risk-informed applications are linked to it. We have identified how plant information can be employed to evaluate safety and economic risk of a NPP. We then applied such information for two types of applications: maintenance optimization and GRA. By doing this we were able to provide an initial set of tools to better support risk-informed decisions.

As shown in Figure 2, in this report we touched upon the main structural elements of an envisioned RI-PSH framework and proposed a possible architecture framework which would greatly automatize data and model sharing among plant organizational structures by including:

1. *Data* generated that provides information related to the performance and health of plant SSCs
2. *Models* and data pre-processing functions
3. *Algorithms* which employs data and models to provide services.

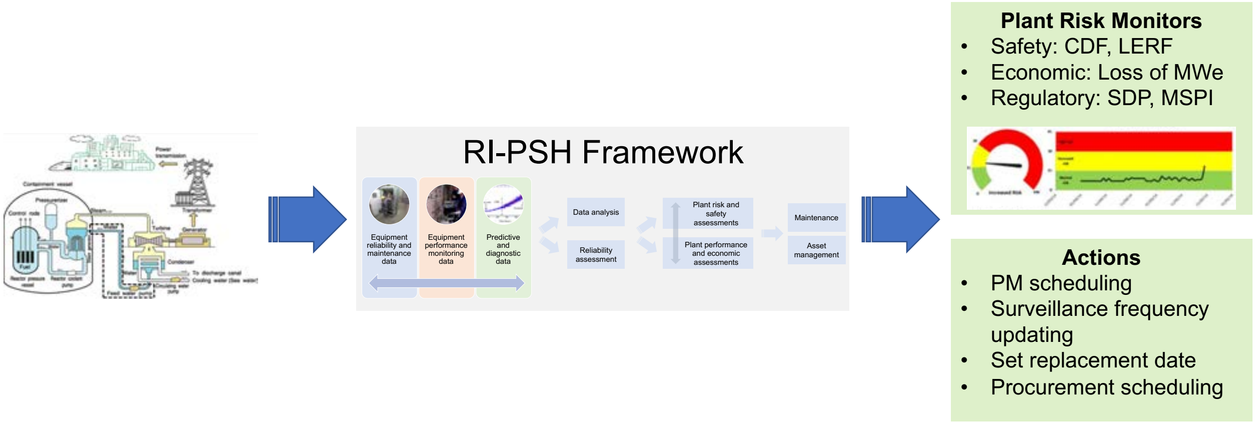


Figure 27. RI-PSH from a decision-making perspective.

These services are shown in Figure 27: from plant data, the RI-PSH framework will provide risk-informed information from the safety, regulatory, and economical perspectives. In addition, it will provide a set of suggested actions such as optimal PM/surveillance frequency and replacement/procurement scheduling.

As a result of the work performed during this first year and in accordance with our industry partner, we have identified the initial stage of the RI-PSH framework as target for the R&D work for the next fiscal year. For FY20, we are the process of planning to extensively develop data analytics methods to quantify component degradation. The goal is to identify situations within the ER system of a chosen operating plant (in collaboration with the utility partner) that would benefit the deployment of methods/algorithms to more accurately determine SSC condition and predict SSC remaining useful life. In particular, we are focusing on the three directions shown in Table 11 where for each of them we have the corresponding impact time scale.

Table 11. RI-PSH research directions for FY20.

Research directions	Impact time scale
Analysis of temporal events such as failure and events reports, maintenance history, SSC conditions	Short
Integration of SSC online data with physical models (e.g., codes)	Medium
Progress on the development of a MBSE architecture for the RI-PSH	Long

REFERENCES

[1] United States Nuclear Regulatory Commission (NRC), "10CFR 50.65 Requirements for monitoring the effectiveness of maintenance at nuclear power plants," Washington, DC. [https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0065.html].

[2] Nuclear Energy Institute (NEI), "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Revision 4b", NEI Report NEI 93-01, Washington, DC (2015).

[3] United States Nuclear Regulatory Commission (NRC), "Regulatory Guide 1.160 - Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Revision 4," Washington, DC (2018). [https://www.federalregister.gov/documents/2018/09/26/2018-20864/monitoring-the-effectiveness-of-maintenance-at-nuclear-power-plants].

[4] Nuclear Energy Institute (NEI), "Regulatory Assessment Performance Indicator Guideline, Revision 7," NEI Report 99-02 Washington, DC (2013). [https://www.nrc.gov/docs/ML1326/ML13261A116.pdf].

[5] Institute of Nuclear Power Operations (INPO), "AP-913 - Equipment Reliability Process Description, Revision 6," Washington, DC (2018) (limited distribution).

[6] M. Gluhak, "Equipment Reliability Process in Krško NPP," *Journal of Energy*, **65** , no. 3-4 (2016). [http://journalofenergy.com/index.php/joe/issue/view/95/88 Accessed 6 August 2019].

[7] Electric Power Research Institute (EPRI), "Demonstration of Reliability Centered Maintenance," EPRI Report EPRI-NP-6152 vol.2, Palo Alto, CA (1991).

[8] Electric Power Research Institute (EPRI), "Comprehensive Low-Cost Reliability Centered Maintenance," EPRI Report EPRI-TR-105365, Palo Alto, CA (1995).

[9] Nuclear Energy Institute (NEI), "Efficiency Bulletin 16-25; Critical Component Reduction," Washington, DC (2016).

[10] Electric Power Research Institute (EPRI), *EPRI Preventive Maintenance Basis Database (PMBD)*, Palo Alto, CA (2015).

[11] Electric Power Research Institute (EPRI), "Preventive Maintenance Basis Database (PMBD): Quick Reference Guide," Palo Alto, CA (2018).

[12] Electric Power Research Institute (EPRI), "Insights on Risk Margins at Nuclear Power Plants: A Technical Evaluation of Margins in Relation to Quantitative Health Objectives and Subsidiary Risk Goals in the United States," Palo Alto, CA (2018). [https://rtoinsider.com/wp-content/uploads/Insights-on-Risk-Margins-at-Nuclear-Power-Plants-EPRI-document-3002012967.pdf].

[13] Nuclear Energy Institute (NEI), "Efficiency Bulletin 17-03a; Value Based Maintenance," Washington, DC (2017).

[14] Nuclear Energy Institute (NEI), "Efficiency Bulletin 16-33; System Health Reporting Efficiencies," Washington, DC (2016).

[15] Nuclear Energy Institute (NEI), "Efficiency Bulletin 16-34; Streamline Program Health Reporting," Washington, DC (2016).

[16] Nuclear Energy Institute (NEI), "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NEI Report NUMARC 93-01, Rev. 4F, Washington, DC (2018).

[17] D. Blanchard and R. Youngblood, “Risk Informed Safety Margin Characterization Case Study: Selection of Electrical Equipment to Be Subjected to Environmental Qualification,” INL Technical Report INL/EXT-11-23479 (2011).

[18] Nuclear Energy Institute (NEI), “An Alternate Approach to NUMARC 93-01,” Washington, DC, June 20, 2018. [Draft Publication– available to NEI members].

[19] United States Nuclear Regulatory Commission (NRC), Inspection Manual Chapter (IMC) 0305, “Operating Reactor Assessment Program,” (2018).

[20] United States Nuclear Regulatory Commission (NRC), “Independent Verification of the Mitigating Systems Performance Index (MSPI) Results for the Pilot Plants,” NUREG-1816, Washington, DC (2005).

[21] Nuclear Energy Institute (NEI), “Regulatory Assessment Performance Indicator Program,” NEI Report 99-02, Revision 7, Washington, DC (2013).

[22] United States Nuclear Regulatory Commission (NRC), Inspection Manual Chapters 0609, “Significance Determination Process,” Washington, DC (2015).

[23] United States Nuclear Regulatory Commission (NRC), Management Directive 8.3, “NRC Incident Investigation Program,” Washington, DC (2014).

[24] D. E. True, “The Value of Risk-Informed Regulation – Safety and Economic Perspective,” Asia Nuclear Business Platform (2016).

[25] United States Nuclear Regulatory Commission (NRC), “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 3, Washington, DC (2018).

[26] United States Nuclear Regulatory Commission (NRC), “An Approach for Plant-Specific Risk-Informed Decision making for Inservice Inspection of Piping,” Regulatory Guide 1.178, Revision 1, Washington, DC (2003).

[27] Nuclear Energy Institute (NEI), “Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines,” NEI Report 06-09, Revision 0 - A, Washington, DC (2006).

[28] Nuclear Energy Institute (NEI), “Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies,” NEI Report 04-10, Revision 1, Washington, DC (2007).

[29] Nuclear Energy Institute (NEI), “10 CFR 50.69 SSC Categorization Guideline,” NEI Report 00-04, Revision 0, Washington, DC (2005).

[30] National Fire Protection Association, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” NFPA 805 (2015).

[31] United States Nuclear Regulatory Commission (NRC), “10 CFR 50.61a Alternate Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events,” 75 FR 23 (2010), as amended.

[32] D. A. Dube et al., “Exelon Economic Enterprise Risk Modeling of a BWR,” *Proceeding of PSA 2017,* Pittsburgh, PA (2017).

[33] Electric Power Research Institute (EPRI), “Generation Risk Assessment (GRA) Plant Implementation Guide,” EPRI Report 1008121, Palo Alto, CA (2004).

[34] Electric Power Research Institute (EPRI), “Risk-Informed Asset Management (RIAM) Development Plan,” EPRI Report 1006268, Palo Alto, CA (2002).

[35] United States Nuclear Regulatory Commission (NRC), “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 3, Washington, DC (2018).

[36] J. H. Saleh, K. Marais, “Reliability: How much is it worth? Beyond its estimation or prediction, the (net) present value of reliability,” *Reliability Engineering & System Safety*, **91**, no. 6, pp. 665-673 (2006).

[37] J. K. Vaurio, “Optimization of Test and Maintenance Intervals Based on Risk and Cost,” *Reliability Engineering & System Safety*, **49**, no. 1, pp. 23-36 (1995).

[38] T. Teresa, I. Singh, E. Popova, E. J. Kee, “Risk-Informed Preventive Maintenance Optimization,” in *Proceedings of Annual Reliability and Maintainability Symposium* (2012).

[39] J. Lee and N. McCormick, *Risk and Safety Analysis of Nuclear Systems*, John Wiley and Sons (2011).

[40] I. Martón, P. Martorell, R. Mullor, A.I. Sánchez, S. Martorell, “Optimization of Test and Maintenance of Ageing Components Consisting of Multiple Items and Addressing Effectiveness,” *Reliability Engineering & System Safety*, **153**, pp. 151-158 (2016).

[41] M. Harunuzzaman, T. Aldemir, “Optimization of Standby Safety System Maintenance Schedules in Nuclear Power Plants,” *Nuclear Technology*, **113**, pp. 354-367 (1996).

[42] Electric Power Research Institute (EPRI), “Plant Engineering: 2018 Complete Product List,” EPRI Report 3002007859 Palo Alto, CA (2019).

[43] Electric Power Research Institute (EPRI), “Integrated Life Cycle Management: Status Report,” EPRI Report 1021188 Palo Alto, CA (2010).

[44] D. Mandelli, C. Wang, D. Morton, I. Popova, S. Hess, S. St Germain, “Combined Data Analytics and Risk Analysis Tool for Long Term Capital SSC Refurbishment and Replacement,” INL Technical Report (2019).

[45] United States Nuclear Regulatory Commission (NRC), “Glossary of Risk-Related Terms in Support of Risk- Informed Decision Making,” NUREG-2122, Washington, DC (2013).

[46] United States Nuclear Regulatory Commission (NRC), “Fault Tree Handbook,” NUREG-0492, Washington, DC (1981).

[47] J. C. Lee, N. J. McCormick, *Risk and Safety Analysis of Nuclear Systems*, Wiley Publishing Company, Hoboken, NJ (2011).

[48] G. Sliter, “Generation Risk Assessment (GRA) Plant Implementation Guide,” EPRI Report 1008121, Palo Alto, CA (2004).

[49] G. Sliter, “Generation Risk Assessment (GRA) at Cooper Nuclear Station,” EPRI Report 1011924, Palo Alto, CA (2005).

[50] G. Sliter, “Introduction to Simplified Generation Risk Assessment Modeling,” EPRI Report 1007386, Palo Alto, CA (2004).

[51] R. J. Breeding, T. J. Leahy, J. Young, W. R. Cramond, “Probabilistic Risk Assessment Course Documentation,” U.S. Nuclear Regulatory Commission, NUREG/CR-4350 (1985).

[52] M. I. Jyrkama, M. D. Pandey, S. M. Hess, “Integration of Degradation Models into Generation Risk Assessment: Challenges and Modeling Approaches,” *Journal of Engineering for Gas Turbines and Power*, **132** (2010).

[53] N. Wilmshurst, “Critical Component Identification Process – Licensee Examples,” EPRI Report 1007935, Palo Alto, CA (2003).

[54] D. Dube, G. Parry, S. Lewis, D. True, F. Ferrante, J. Chapman, “Enhanced Guidance on Integrated Risk-Informed Decision-Making,” *Proceedings of Probability Safety Assessment Conference (PSA)* Pittsburgh, PA (2017).

[55] D. Dube, B. Albinson, R. Wolfgang, M. Saunders, G. Krueger, “Exelon Economic Enterprise Risk Modeling of a BWR,” Exelon Generation, Kenneth Square, PA.

[56] D. Blanchard, W. Brinsfield, P. Szetu, G. Sliter, “Power Plant Generation Risk Assessment (GRA),” Applied Reliability Engineering, Inc.

[57] D. Sanzo, P. Kvam, G. Apostolakis, J. Wu, T. Milici, N. Ghoniem, S. Guarro, “Survey and Evaluation of Ageing Risk Assessment Methods and Applications,” Los Alamos National Laboratory (1994).

[58] B. Fischhoff, “The Realities of Risk-Cost-Benefit Analysis,” *Science*, **350**, no. 6260 (2015).

[59] S. A. Eide, T. E. Wierman, C. D. Gentillon, D. M. Rasmuson, C. L. Atwood, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, NUREG/CR-6928 (2007).

[60] North American Electric Reliability Council (NERC), “pc-GAR for Windows,” Demo Release 4.1.15 (2008).

[61] Summary of SPAR Component Unreliability Data and Results, 2015 Parameter Estimation Update.

[62] U.S. Atomic Energy Commission, “Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants,” NUREG-75/014 (WASH-1400) (1974).

[63] Nuclear Energy Institute (NEI), “Nuclear Costs in Context,” NEI (2018). [https://www.nei.org/resources/reports-briefs/nuclear-costs-in-context].

[64] A. Jayakumar, S. Asgarpoor, “A Markov Method for the Optimum Preventive Maintenance of a Component,” *Proceedings of the IASTED International Conference Power and Energy Systems*, Palm Springs, CA (2003).

[65] D. Yaga, P. Mell, N. Roby and K. Scarfone, “Blockchain Technology Overview,” Gaithersburg, MD, (2018).

[66] P. Soni, “Why Blockchain for the Supply Chain,” EBN, 25 June 2018. [https://www.ebnonline.com/why-blockchain-for-the-supply-chain/].

[67] R. Narasimhan, S. Talluri, D. Méndez, “Supplier Evaluation and Rationalization via Data Envelopment Analysis: An Empirical Examination,” *Journal of Supply Chain Management*, **37**, no.2, pp. 28-37 (2006).

[68] A. Azadeh, S. M. Alem, “A Flexible Deterministic, Stochastic and Fuzzy Data Envelopment Analysis Approach for Supply Chain Risk and Vendor Selection Problem: Simulation Analysis,” *Expert Systems with Applications*, **37**, no. 12, pp. 7438-7448 (2010).

[69] “Social Accountability International | SA8000® Standard,” Social Accountability International, [http://www.sa-intl.org/index.cfm?fuseaction=Page.ViewPage&PageID=1689].

[70] M. Burkhart, “5 Different types of audits to evaluate your supplier,” China Quality Focus, (2019). [https://www.intouch-quality.com/blog/the-3-most-common-types-of-factory-audits].

[71] S. Tiku, M. Pecht, J. E. Strutt, “Organizational Reliability Capability,” *IEEE Transactions on Components and Packageing Technologies*, **29**, no. 2, pp. 425 - 428 (2006).

[72] S. Tiku, M. Pecht, “Reliability Capability Assessment Methodology,” *in Proceedings of Canadian Reliability and Maintainability Symposium*,Ottawa, ON, Canada (2003).

[73] S. Tiku, M. Azarian, M. Pecht, “Using a Reliability Capability Maturity Model to Benchmark Electronics Companies,” *International Journal of Quality and Reliability Management*, **24**, no. 5, pp. 547-563 (2007).

[74] T. Working Group, “IECEE Operational Document TRF-Development, Maintenance and Use IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System),” 2020.

[75] J. Niggl, “How to Verify Critical Components with a Construction Data Form,” China Quality Focus, (2019). [https://www.intouch-quality.com/blog/always-verify-cdf.].

[76] B. Sood, D. Das, M. Pecht, “Screening for Counterfeit Electronic Parts,” *Journal of Materials Science: Materials in Electronics*, **22**, no. 10, pp. 1511-1522 (2011).

[77] A. Shrivastava, M. H. Azarian, C. Morillo, B. Sood, M. Pecht, “Detection and Reliability Risks of Counterfeit Electrolytic Capacitors,” *IEEE Transactions on Reliability*, **63**, no. 2, pp. 468-479 (2014).

[78] U. Guin, K. Huang, D. Dimase, J. M. Carulli, M. Tehranipoor, Y. Makris, “Counterfeit Integrated Circuits: a Rising Threat in the Global Semiconductor Supply Chain,” *Proceedings of the IEEE*, **102**, no. 8, pp. 1207-1228 (2014).

[79] K. Chatterjee, D. Das, M. Pecht, C. Ricci, P. Suorsa, “Solving the Counterfeit Electronics Problem,” SMTA Pan Pacific Conference (2007).

[80] M. Partridge, R. A. Calvo, “Fast Dimensionality Reduction and Simple PCA,” *Intelligent Data Analysis*, **2,** no. 3, pp. 203–214 (1998).

[81] B. Scholkopf, A. Smola, K.-R. Muller, “Kernel Principal Component Analysis,” in *Artificial Networks*, Springer, Berlin, Germany (1997).

[82] J. Yang, J.-Y. Yang, “Why can LDA be Performed in PCA Transformed Space?” *Pattern Recognition*, **36**, no. 2, pp. 563–566 (2003).

[83] K.-R. Muller, S. Mika, G. Ratsch, K. Tsuda, B. Scholkopf, “An Introduction to Kernel-Based Learning Algorithm,” *IEEE Transactions on Neural Networks*, **12**, no. 2, pp. 181–201 (2001).

[84] G. Baudat, F. Anouar, “Generalized Discriminant Analysis Using a Kernel Approach,” *Neural Computation*, **12**, no. 10, pp. 2385–2404 (2000).

[85] P. Comon, “Independent Component Analysis, a New Concept?” *Signal Processing*, **36**, no. 3, pp. 287–314 (1994).

[86] L. Van der Maaten, G. Hinton, “Visualizing Data Using t-SNE,” *Journal of Machine Learning Research*, **9**, pp. 2579–2605 (2008).

[87] R. Schumacker, S. Tomek, “Chi-Square Test,” *Understanding Statistics Using R*, pp. 169–175 (2012).

[88] J. T. Kent, “Information Gain and A General Measure of Correlation,” *Biometrika*, **70**, no. 1, pp. 163–173 (1983).

[89] J. L. Rodgers, and W. A. Nicewander, “Thirteen Ways to Look at The Correlation Coefficient,” *The American Statistician*, **42**, no. 1, pp. 59–66 (1988).

[90] C. Furlanello, M. Serafini, S. Merler, G. Jurman, “An Accelerated Procedure for Recursive Feature Ranking on Microarray Data,” *Neural Networks*, **16**, no. 5, pp. 641–648 (2003).

[91] V. Roth, “The Generalized LASSO,” *IEEE Transactions on Neural Networks*, **15**, no. 1, pp. 16–28 (2004).

[92] Q. Li, N. Lin, “The Bayesian Elastic Net,” *Bayesian Analysis*, **15**, no. 1, pp. 151–170 (2010).

[93] S. Le Cessie, J. C. Van Houwelingen, “Ridge Estimators in Logistic Regression,” *Journal of the Royal Statistical Society*, **41**, no. 1, pp. 191–201(1992).

[94] W. Yan, L. Yu, “On Accurate and Reliable Anomaly Detection for Gas Turbine Combustors: A Deep Learning Approach,” *Proceedings of Annual Conference of the Prognostics and Health Management Society*, Coronado, CA, USA (2015).

[95] M. Zhao, M. Kang, B. Tang, M. Pecht, “Deep Residual Networks with Dynamically Weighted Wavelet Coefficients for Fault Diagnosis of Planetary Gearboxes,” *IEEE Transactions on Industrial Electronics*, **65**, no. 5, pp. 4290–4300 (2018).

[96] H. Shao, H. Jiang, H. Zhang, T. Liang, “Electric Locomotive Bearing Fault Diagnosis Using a Novel Convolutional Deep Belief Network,” *IEEE Transactions on Industrial Electronics*, **65**, no. 3, pp. 2727–2736 (2018).

[97] Z. Liu, Z. Jia, C.-M. Vong, S. Bu, J. Han, X. Tang, “Capturing High-Discriminative Fault Features for Electronics-Rich Analog System Via Deep Learning,” *IEEE Transactions on Industrial Informatics*, **13**, no. 3, pp. 1213–1226 (2017).

[98] J. Tian, C. Morillo, M. H. Azarian, M. Pecht, “Motor Bearing Fault Detection Using Spectral Kurtosis-Based Feature Extraction Coupled with K-Nearest Neighbor Distance Analysis,” *IEEE Transactions on Industrial Electronics*, **63**, no. 3, pp. 1793–1803 (2016).

[99] M. Kang, G. Krishnan Ramaswami, M. Hodkiewicz, E. Cripps, J.-M. Kim, M. Pecht, “A Sequential *K*-Nearest Neighbor Classification Approach for Data-Driven Fault Diagnosis Using Distance- and Density-Based Affinity Measures,” in *Data Mining and Big Data*, Springer (2016).

[100] M. Kang, J. Kim, J. -M. Kim, A. C. C. Tan, E. Y. Kim, B.-K. Choi, “Reliable Fault Diagnosis for Low-Speed Bearings Using Individually Trained Support Vector Machines with Kernel Discriminative Feature Analysis,” *IEEE Transactions on Power Electronics*, **30**, no. 5, pp. 2786–2797 (2015).

[101] A. S. Vasan, B. Long, M. Pecht, “Experimental Validation of LS-SVM Based Fault Identification in Analog Circuits Using Frequency Features,” *Proceedings of the World Congress on Engineering Asset Management*, Cincinnati, OH, USA (2011).

[102] Y. Cui, J. Shi, Z. Wang, “Analog Circuit Fault Diagnosis Based On Quantum Clustering Based Multi-Valued Quantum Fuzzification Decision Tree (QC-MQFDT),” *Measurement*, **93**, pp. 421–434 (2016).

[103] F. Ye, Z. Zhang, K. Chakrabarty, X. Gu, “Adaptive Diagnosis Using Decision Trees (DT),” Knowledge-*Driven Board-Level Functional Fault Diagnosis*, pp. 61–78 (2016).

[104] A. Zou, R. Deng, Q. Mei, L. Zou, “Fault Diagnosis of a Transformer Based on Polynomial Neural Networks,” *Cluster Computing*, 1–9 (2017).

[105] L. Wen, X. Li, L. Gao, Y. Zhang, “A New Convolutional Neural Network-Based Data-Driven Fault Diagnosis Method,” *IEEE Transactions on Industrial Electronics*, (2018). [https://dx.doi.org/10.1109/TIE.2017.2774777].

[106] H. Hu, B. Tang, X. Gong, W. Wei, H. Wang, “Intelligent Fault Diagnosis of The High-Speed Train with Big Data Based on Deep Neural Networks,” *IEEE Transactions on Industrial Informatics*, **13**, no. 4, pp. 2106–2116 (2017).

[107] J. Tian, M. Azarian, M. Pecht, G. Niu, C. Li, “An Ensemble Learning-Based Fault Diagnosis Method for Rotating Machinery,” *Proceedings of the 2017 Prognostics and System Health Management Conference*, Harbin, China (2017).

[108] R. Xiong, Y. Zhang, H. He, X. Zhou, M. Pecht, "A Double-Scale, Particle-Filtering, Energy State Prediction Algorithm for Lithium-Ion Batteries," *IEEE Transitions on Industrial Electronics*, **65**, no. 2, pp. 1526–1538 (2018).

[109] M. -H. Chang, M. Kang, M. Pecht, "Prognostics-Based LED Qualification Using Similarity-Based Statistical Measure with RVM Regression Model," *IEEE Transactions on Industrial Electronics*, **64**, no. 7, pp. 5667–5677 (2017).

[110] N. Montgomery, D. Banjevic, A. K. S. Jardine, "Minor Maintenance Actions and Their Impact on Diagnostic and Prognostic CBM Models," *Journal of Intelligent Manufacturing*, **23**, no. 2, pp. 303-311 (2012).

[111] M. Pecht, T. Shibutani, M. Kang, M. Hodkiewicz, E. Cripps, "A Fusion Prognostics-Based Qualification Test Methodology for Microelectronic Products," *Microelectronics Reliability*, **63**, pp. 320–324 (2016).

[112] S. Kumar, N. Vichare, E. Dolev, M. Pecht, "A Health Indicator Method for Degradation Detection of Electronic Products," *Microelectronics Reliability*, **52**, pp. 439–445 (2012).

[113] S. Cheng, M. Pecht, "Using Cross-Validation for Model Parameter Selection of Sequential Probability Ratio Test," *Expert Systems with Applications*, **39**, pp. 8467–8473 (2012).

[114] J. Tian, M. H. Azarian, M. Pecht, "Anomaly Detection Using Self-Organizing Maps-Based K-Nearest Neighbor Algorithm," *Proceedings of the European Conference of the Prognostics and Health Management Society*, (2014).

[115] Q. Jiang, X. Yan, W. Zhao, "Fault Detection and Diagnosis In Chemical Processes Using Sensitive Principal Component Analysis," *Industrial & Engineering Chemistry Research*, **52** (4), pp. 1635–1644 (2013).

[116] X. Jin, W. M. Ma, L. L. Cheng, M. Pecht, "Health Monitoring of Cooling Fans Based On Mahalanobis Distance With Mrmr Feature Selection," *IEEE Transactions on Instrumentation and Measurement*, **61**, no. 8, pp. 2222–2229 (2012).

[117] J. Qu, "Support-Vector-Machine-Based Diagnostics and Prognostics for Rotating Systems," Ph.D. dissertation, University of Alberta, Canada (2013).

[118] M. E. Tipping, "Sparse Bayesian Learning and the Relevance Vector Machine," *Journal of Machine Learning Research*, **1**, pp. 211–244 (2001).

[119] W. Wang, and M. Carr, "A Stochastic Filtering Based Data Driven Approach for Residual Life Prediction and Condition Based Maintenance Decision Making Support," *Proceedings of 2010 Prognostics and Health Management Conference*, Macao, China (2010).

[120] P. Baraldi, F. Mangili, E. Zio, "A Kalman Filter-Based Ensemble Approach with Application to Turbine Creep Prognostics," *IEEE Transactions on Reliability*, **61**, no. 4, pp. 966–977 (2012).

[121] J. Fan, K.-C. Yung, M. Pecht, "Predicting Long-Term Lumen Maintenance Life of LED Light Sources Using a Particle Filter-Based Prognostic Approach," *Expert Systems with Applications*, **42**, no. 5, pp. 2411–2420 (2015).

[122] S. Cheng, M. Pecht, "A Fusion Prognostics Method for Remaining Useful Life Prediction of Electronic Products," *Proceedings of IEEE International Conference on Automation Science and Engineering*, Bangalore, India (2009).

[123] J. Xu, L. Xu, "Health Management Based on Fusion Prognostics for Avionics Systems," *Journal of Systems Engineering and Electronics*, **22**, pp. 428–436 (2011).

[124] N. Patil, D. Das, C. Yin, C. Bailey, M. Pecht, "A Fusion Approach to IGBT Power Module Prognostics," *Proceedings of the 10th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems*, Delft, Netherlands, (2009).

[125] M. Chookah, M. Nuhi, M. Modarres, "A probabilistic physics-of-failure model for prognostic health management of structures subject to pitting and corrosion-fatigue," *Reliability Engineering & System Safety*, **96**, pp. 1601–1610 (2011).

[126] M. Pecht, R. Radojcic, G. Rao, *Guidebook for Manageing Silicon Chip Reliability*, CRC Press, Boca Raton, FL, USA (1999).

[127] M. E. Porter, J. E. Heppelmann, "How smart, connected products are transforming companies," *Harvard Business Review*, **93**, pp. 97–114 (2015).

[128] R. Drath, A. Horch, "Industrie 4.0: Hit or hype?", *IEEE Industrial Electronics Magazine*, **8**, no. 2, pp. 56–58 (2014).

[129] J. Bruner, *The Machines are Talking*, O'Reilly Media, Sebastopol, CA, USA (2013).

[130] F. Farber, N. May, W. Lehner, P. Grobe, I. Muller, H. Rauhe, J. Dees, "The SAP HANA Database – an Architecture Overview," *IEEE Data Engineering Bulletin*, **35**, no. 1, pp. 28–33 (2012).

[131] Energy Agency, Key World Energy Statistics (2015).

[132] D. S. Markovic, D. Zivkovic, I. Branovic, R. Popovic, D. Cvetkovic, "Smart Power Grid and Cloud Computing," *Renewable and Sustainable Energy Reviews*, **24**, pp. 566–577 (2013).

[133] W. Zhixin, J. Chuanwen, A. Qian, W. Chengmin, "The Key Technology of Offshore Wind Farm and Its New Development in China," *Renewable and Sustainable Energy Reviews*, **13**, no. 1, pp. 216–222 (2009).

[134] G. Cros, "Industry Trends Maintenance Cost," *Proceedings of the IATA 3rd Airline Cost Conference*, Geneva, Switzerland (2015).

[135] Z. Williams, "Benefits of IVHM: An Analytical Approach," *Proceedings of 2006 IEEE Aerospace Conference*, Big Sky, MT, USA (2006).

[136] P. Smith, D. Campbell, "Practical Implementation of BICs for Safety-Critical Applications," *Proceedings of 2000 IEEE International Workshop on Defect Based Testing*, Montreal, Quebec, Canada (2000).

[137] I. Pecuh, M. Margala, V. Stopjakova, "1.5 volts Iddq/Iddt Current Monitor," *Proceedings of 1999 IEEE Canadian Conference on Electrical and Computer Engineering*, Edmonton, Alberta, Canada (1999).

[138] B. Xue, D. Walker, "Built-In Current Sensor for IDDQ Test," *Proceedings of 2004 IEEE International Workshop on Current and Defect Based Testing*, Napa Valley, CA, USA (2004).

[139] R. Wright, L. Kirkland, "Nano-Scaled Electrical Sensor Devices for Integrated Circuit Diagnostics," *Proceedings of 2003 IEEE Aerospace Conference*, Big Sky, MT, USA (2003).

[140] R. Wright, M. Zgol, D. Adebimpe, L. Kirkland, "Functional Circuit Board Testing Using Nanoscale Sensors," *Proceedings of IEEE Systems Readiness Technology Conference*, Anaheim, CA, USA (2003).

[141] R. Wright, M. Zgol, S. Keeton, L. Kirkland, "Nanotechnology-Based Molecular Test Equipment (MTE)," *IEEE Aerospace and Electronic Systems Magazine*, **16**, no. 6, pp. 15–19 (2001).

[142] M Kanniche, M. Mamat-Ibrahim, "Wavelet Based Fuzzy Algorithm for Condition Monitoring Of Voltage Source Inverters," Electronic Letters, **40**, no. 4, pp. 1–2 (2004).

[143] G. Hughes, J. Murray, K. Kreutz-Delgado, C. Elkan, "Improved Disk-Drive Failure Warnings," *IEEE Transactions on Reliability*, **51**, no. 3, pp. 350–357 (2002).

[144] K. Whisnant, K. Gross, N. Lingurovska, "Proactive Fault Monitoring in Enterprise Servers," *Proceedings of the 2005 IEEE International Multiconference in Computer Science & Computer Engineering*, Las Vegas, NV, USA (2005).

[145] K. Mishra, K. Gross, "Dynamic Stimulation Tool for Improved Performance Modeling and Resource Provisioning of Enterprise Servers," *Proceedings of the 14th IEEE International Symposium on Software Reliability Engineering*, Denver, CO, USA (2003).

[146] K. Cassiday, K. Gross, A. Malekpour, "Advanced Pattern Recognition for Detection of Complex Software Ageing Phenomena in Online Transaction Processing Servers," *Proceedings of the International Performance and Dependability Symposium*, Washington, D.C., USA (2002).

[147] K. Vaidyanathan, K. Gross, "MSET Performance Optimization for Detection of Software Ageing," *Proceedings of the 14th IEEE International Symposium on Software Reliability Engineering*, Denver, CO, USA (2003).

[148] D. W. Brown, P. W. Kalgren, C. S. Byington, M. J. Roemer, "Electronic Prognostics – A Case Study Using Global Positioning System (GPS)," *Microelectronics Reliability*, **47**, no. 12, pp. 1874–1881 (2005).

[149] M. H. Azarian, D. Kwon, M. Pecht, "Use of The Skin Effect For Detection Of Interconnect Degradation," in *IMAPS 42nd International Symposium on Microelectronics* (2009).

[150] N. J. Jameson, M. H. Azarian, M. Pecht, "Impedance-Based Health Monitoring of Electromagnetic Coil Insulation Subjected to Corrosive Deterioration," In *Proceedings of the Annual Conference of the Prognostics and Health Management Society 2016* (2016).

[151] A. Ramos, J. Ferreira, J. Barcelo, "Model-Based Systems Engineering: An Emerging Approach for Modern Systems," *IEEE Transactions on Systems Man and Cybernetics*, **42**, no. 1, pp. 101-111 (2011).

[152] A. B. Rauzy, C. Haskins, "Foundations for Model-Based Systems Engineering and Model-Based Safety Assessment," *System Engineering*, **22**, no. 2, pp.146-155 (2019).

[153] M. Hause, "The SysML Modelling Language," *Fifteenth European Systems Engineering Conference* (2006). [http://www.omgsysml.org/The_SysML_Modelling_Language.pdf].

[154] C. L. Smith, V. N. Shah, T. Kao, G. Apostolakis, "Incorporating Ageing Effects into Probabilistic Risk Assessment - A Feasibility Study Utilizing Reliability Physics Models," U.S. Nuclear Regulatory Commission NUREG/CR-5632 (2001).

[155] T. Dumargue, J.-R. Pougeon, and J.-R. Massé, "An Approach to Designing PHM Systems with Systems Engineering," *in Proceedings of Third European Conference of the Prognostics and Health Management Society 2016* (2016).

[156] E. Borgonovo, G. E. Apostolakis, "A New Importance Measure for Risk-Informed Decision Making," *Reliability Engineering & System Safety*, **72**, no. 2, pp. 193-212 (2001).

[157] Electric Power Research Institute (EPRI), "Introduction to Simplified Generation Risk Assessment Modeling," EPRI Report 1007386 Palo Alto, CA (2004).

[158] C. L. Smith, S.T. Wood, D. O'Neal, "Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Version 8," NUREG/CR-7039, vol. 3 (2011).

[159] R. C. Kryter, H. D. Haynes, *Condition monitoring of machinery using motor current signature analysis*," No. CONF-890555-3, Oak Ridge National Laboratory (1989).

[160] W.T. Thomson, M. Fenger, "Current Signature Analysis to Detect Induction Motor Faults," *IEEE Industry Applications Magazine*, **7**, no. 4, pp. 26–34 (2001).

[161] W. T. Thomson, R. J. Gilmore, "Motor Current Signature Analysis To Detect Faults in Induction Motor Drives-Fundamentals, Data Interpretation, and Industrial Case Histories," in *Proceedings of the 32nd turbomachinery Symposium*, Texas A&M University Turbomachinery Laboratories (2003).

[162] K. M. Siddiqui, K. Sahay, and V. K. Giri, "Health Monitoring and Fault Diagnosis in Induction Motor - A Review," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, **3**, no. 1, pp. 6549-6565 (2014).

[163] D. Z. Li, W. Wang, F. Ismail, "A Spectrum Synch Technique for Induction Motor Health Condition Monitoring," *IEEE Transactions on Energy Conversion*, **30**, no. 4, pp. 1348-1355 (2015).

[164] D. Z. Li, W. Wang, F. Ismail, W. Wang, "An Enhanced Bispectrum Technique with Auxiliary Frequency Injection for Induction Motor Health Condition Monitoring," *IEEE Transactions on Instrumentation and Measurement*, **64**, no. 10, pp. 2679-2687 (2015).

[165] C.-Y., Eduardo, et al., "Real-Time Condition Monitoring on VSD-Fed Induction Motors Through Statistical Analysis and Synchronous Speed Observation," *International Transactions on Electrical Energy Systems*, **25**, no. 8, pp. 1657-1672 (2015).

[166] J. P. Peck, J. Burrows, "On-Line Condition Monitoring of Rotating Equipment Using Neural Networks," *ISA Transactions*, **33**, no. 2, pp. 159-164 (1994).

[167] D. K. Martin, J. VanDyke, "Integrating Vibration, Motor Current, And Wear Particle Analysis with Machine Operating State for On-Line Machinery Prognostics/Diagnostics Systems (MPROS)," *Proceedings of the 1997 ASME International Mechanical Engineering Congress and Exposition, Dallas, Texas*, vol. 7, (1997).

[168] Y. Zhongming, W. Bin, "A Review on Induction Motor Online Fault Diagnosis," in *Proceedings IPEMC 2000, Third International Power Electronics and Motion Control Conference (IEEE Cat. No. 00EX435)*, vol. 3, IEEE (2000).

[169] R. Yan, R. X. Gao, "Approximate Entropy as a Diagnostic Tool for Machine Health Monitoring," *Mechanical Systems and Signal Processing*, **21**, no. 2, pp. 824-839 (2007).

[170] H. Zhao, et al., "A New Feature Extraction Method Based on EEMD and Multi-Scale Fuzzy Entropy for Motor Bearing," *Entropy*, **19**, no. 1 (2016).

[171] D. Casada, *Using the Motor to Monitor Pump Conditions*, NUREG/CP-0152; CONF-9607103-. American Society of Mechanical Engineers, New York, NY (1996).

[172] G. D. Neill, et al., "Detection of Incipient Cavitation in Pumps Using Acoustic Emission," *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering*, **211**, no. 4, pp. 267–277 (1997).

[173] J. Yan, et al., "Nondestructive Detection of Valves Using Acoustic Emission Technique," *Advances in Materials Science and Engineering* 2015 (2015).

[174] L. Dong, Y. Zhao, C. Dai, "Detection of Inception Cavitation In Centrifugal Pump By Fluid-Borne Noise Diagnostic," *Shock and Vibration* 2019 (2019).

[175] G. Geiger, "Monitoring of an Electrical Driven Pump Using Continuous-Time Parameter Estimation Methods," *IFAC Proceedings Volumes*, **15**, no. 4, pp. 603-608 (1982).

[176] I. S. Koo, W. W. Kim, "The Development of Reactor Coolant Pump Vibration Monitoring and a Diagnostic System in the Nuclear Power Plant," *ISA transactions*, **39**, no. 3, pp. 309-316 (2000).

[177] E. Egusquiza, "Condition Monitoring of Pump-Turbines. New Challenges," *Measurement*, **67**, pp. 151-163 (2015).

[178] S. Mukhopadhyay, S. Chaudhuri, "A Feature-Based Approach to Monitor Motor-Operated Valves Used in Nuclear Power Plants," *IEEE Transactions on Nuclear Science*, **42**, no. 6, pp. 2209-2220(1995).

[179] H. D. Haynes, "Aging And Service Wear of Electric Motor-Operated Valves Used in Engineered Safety-Feature Systems of Nuclear Power Plants", No. NUREG/CR-4234, vol. 2. Nuclear Regulatory Commission (1989).

[180] P. Granjon, "Condition Monitoring of Motor-Operated Valves in Nuclear Power Plants," *The Eighth International Conference on Condition Monitoring and Machinery Failure Prevention Technologies CM/MFPT 2011* (2011).

[181] S.-C. Kang, et al., "Motor Control Center (MCC) Based Technology Study for Safety-Related Motor Operated Valves," *Nuclear Engineering and Technology*, **38**, no. 2, pp. 155-162 (2006).

[182] S. Kang, et al., "A Study on The Actuator Efficiency Behavior of Safety-Related Motor Operated Gate and Globe Valves," *Nuclear Engineering and Design*, **239**, 12, pp. 2705-2712 (2009).

[183] A. R. Bhende, et al., "Detection of Incipient Failure in Nuclear Reactor Pressure Systems Using Acoustic Emission," *Jurnal Tribologi*, **2**, pp. 1-30 (2014).

[184] F. Elasha, et al. "Application of Acoustic Emission in Diagnostic of Bearing Faults within a Helicopter Gearbox," *Procedia CIRP*, **38**, pp. 30–36 (2015).

[185] C. J. Li, S. Y. Li, "Acoustic Emission Analysis for Bearing Condition Monitoring," *Wear*, **185**, no. 1, pp. 67-74 (1995).

[186] D. Mba, "Acoustic Emissions and Monitoring Bearing Health," *Tribology Transactions*, **46**, no. 3, pp. 447-451(2003).

[187] D. F. Shi, F. Tsung, P. J. Unsworth, "Adaptive Time–Frequency Decomposition for Transient Vibration Monitoring of Rotating Machinery," *Mechanical Systems and Signal Processing*, **18**, no. 1, pp. 127-141 (2004).

[188] S. Seker, E. Ayaz, "Feature Extraction Related to Bearing Damage in Electric Motors by Wavelet Analysis," *Journal of the Franklin Institute*, **340**, no. 2, pp. 125-134 (2003).

[189] A. K. Nandi, C. Liu, D. Wong, "Intelligent Vibration Signal Processing for Condition Monitoring," *Proceedings of the International Conference Surveillance*, vol. 7 (2013).

[190] R. Yan, R. X. Gao, "Machine Health Diagnosis Based on Approximate Entropy," *Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference (IEEE Cat. No. 04CH37510)*. vol. 3. IEEE (2004).

[191] M. A. S. Jeronimo, et al., "Monitoring the Thermal Efficiency of Fouled Heat Exchangers: A Simplified Method," *Experimental Thermal and Fluid Science*, **14**, no. 4, pp. 455-463 (1997).

[192] C. M. Astorga-Zaragoza, et al., "Observer-Based monitoring of Heat Exchangers," *ISA transactions*, **47**, no. 1, pp. 15-24 (2008).

[193] C. Ennaceur, et al., "Monitoring Crack Growth in Pressure Vessel Steels by the Acoustic Emission Technique and the Method of Potential Difference," *International Journal of Pressure Vessels and Piping*, **83**, no. 3, pp. 197-204 (2006).

[194] M. Niffenegger, H. J. Leber, "Monitoring the Embrittlement of Reactor Pressure Vessel Steels by Using the Seebeck Coefficient," *Journal of Nuclear Materials*, **389**, no. 1, pp. 62-67 (2009).

[195] V. Giurgiutiu, A. Zagrai, J. Bao, "Embedded Active Sensors for In-Situ Structural Health Monitoring of Thin-Wall Structures," *Journal of Pressure Vessel Technology*, **124**, no. 3, pp. 293-302 (2002).

[196] J. Degrieck, W. Waele, P. Verleysen, "Monitoring of Fibre Reinforced Composites with Embedded Optical Fibre Bragg Sensors, with Application to Filament Wound Pressure Vessels," *NDT & E International*, **34**, no. 4, pp. 289-296 (2001).

[197] X. F. Yao, et al., "Full-Field Deformation Measurement of Fiber Composite Pressure Vessel Using Digital Speckle Correlation Method," *Polymer Testing*, **24**, no. 2, pp. 245-251 (2005).

[198] M. Kunzler, et al., "Use of Multidimensional Fiber Grating Strain Sensors for Damage Detection in Composite Pressure Vessels," *Smart Structures and Materials 2005: Smart Sensor Technology and Measurement Systems*, vol. 5758, International Society for Optics and Photonics (2005).

[199] C. B. Scruby, H. N. G. Wadley, "An assessment of acoustic emission for nuclear pressure vessel monitoring," *Progress in Nuclear Energy*, **11**, no. 3, pp. 275-297 (1983).

[200] B. Trujillo, A. Zagrai, "Embedded and Conventional Ultrasonic Sensors for Monitoring Acoustic Emission During Thermal Fatigue," *Health Monitoring of Structural and Biological Systems 2016*, vol. 9805, International Society for Optics and Photonics (2016).

[201] P. Tscheliesnig, G. Lackner, A. Jagenbrein, "Corrosion detection by means of acoustic emission (AE) monitoring," *Proceedings of the 19th World Conference on Non-Destructive Testing (WCNDT 2016), Munich, Germany* (2016).

[202] L. B. Sipahi, M. R. Govindaraju, D. C. Jiles, "Monitoring Neutron Embrittlement in Nuclear Pressure Vessel Steels using Micromagnetic Barkhausen Emissions," *Journal of Applied Physics*, **75**, no. 10, pp. 6981-6983 (1994).

[203] C. Li, et al., "Effects of neutron irradiation on magnetic properties of reactor pressure vessel steel," *Nuclear Engineering and Design*, **342**, pp. 128-132 (2019).

[204] B. Fekete, P. Trampus, "Acoustic Barkhausen Effect Observed in Various Steels," *Materials Science Forum*, **885**, Trans Tech Publications (2017).

[205] P Ramuhalli, et al., *Experimental Design for Evaluating Selected Nondestructive Measurement Technologies-Advanced Reactor Technology Milestone: M3AT-16PN2301043*, No. PNNL-25561 Rev. 0, Pacific Northwest National Laboratory (PNNL), Richland, WA (2016).

[206] F. Li, et al., "Propagation of Guided Waves in Pressure Vessel," *Wave Motion*, **52**, pp. 216-228 (2015).

[207] Y. Lugovtsova, J. Prager, "Structural Health Monitoring of Composite Pressure Vessels Using Guided Ultrasonic Waves," *Insight-Non-Destructive Testing and Condition Monitoring*, **60**, no. 3, pp. 139-144 (2018).

[208] B. Trujillo, A. Zagrai, "Embedded and Conventional Ultrasonic Sensors for Monitoring Acoustic Emission During Thermal Fatigue," *Health Monitoring of Structural and Biological Systems 2016*, vol. 9805, International Society for Optics and Photonics (2016).

[209] J. M. Muggleton, et al., "A Theoretical Study of the Fundamental Torsional Wave in Buried Pipes for Pipeline Condition Assessment and Monitoring," *Journal of Sound and Vibration*, **374**, pp. 155-171 (2016).

[210] Z. Liu, Zheng, Y. Kleiner, "State-of-the-Art Review of Technologies for Pipe Structural Health Monitoring," *IEEE Sensors Journal*, **12**, no. 6, pp. 1987-1992 (2012).

[211] A. Smith, N. Dixon, G. Fowmes, "Monitoring Buried Pipe Deformation Using Acoustic Emission: Quantification of Attenuation," *International Journal of Geotechnical Engineering*, **11**, no. 4, pp. 418-430 (2017).

[212] H. J. Heather-Smith, et al., "Monitoring Buried Infrastructure Deformation Using Acoustic Emissions," *International Journal of Geotechnical Engineering*, **11**, no. 4 (2017).

[213] A. Smith, I. D. Moore, N. Dixon, "Acoustic Emission Sensing of Pipe-Soil Interaction: Development of an Early Warning System for Buried Pipe Deformation," *International Conference on Smart Infrastructure and Construction 2019* (2019).

[214] A. Smith, N. Dixon, G. Fowmes, "Monitoring buried pipe deformation using acoustic emission: quantification of attenuation," *International Journal of Geotechnical Engineering*, **11**, no. 4, pp. 418-430 (2017).

[215] Y.-J. Shin, et al,, "Application of Time-Frequency Domain Reflectometry for Detection and Localization of a Fault on a Coaxial Cable," *IEEE Transactions on Instrumentation and Measurement*, **54**, no. 6, pp. 2493-2500 (2005).

[216] P. Smith, C. Furse, J. Gunther, "Analysis of spread spectrum time domain reflectometry for wire fault location," *IEEE sensors journal*, **5**, no. 6, pp. 1469-1478 (2005).

[217] R. Papazyan, R. Eriksson, "Calibration for time domain propagation constant measurements on power cables," *IEEE Transactions on Instrumentation and Measurement*, **52**, no. 2, pp. 415-418 (2003).

[218] M. K. Smail, et al., "Detection of Defects in Wiring Networks Using Time Domain Reflectometry," *IEEE Transactions on Magnetics*, **46**, no. 8, pp. 2998-3001 (2010).

[219] C. Furse, et al., "Frequency-Domain Reflectometry for On-Board Testing of Aging Aircraft Wiring," *IEEE Transactions on Electromagnetic Compatibility*, **45**, no. 2, pp. 306-315 (2003).

[220] Y. J. Chung, C. Furse, J. Pruitt, "Application of Phase Detection Frequency Domain Reflectometry for Locating Faults in an F-18 Flight Control Harness," *IEEE Transactions on Electromagnetic Compatibility*, **47**, no. 2, pp. 327-334 (2005).

[221] E. Song, et al., "Detection and Location of Multiple Wiring Faults Via Time–Frequency-Domain Reflectometry," *IEEE Transactions on Electromagnetic Compatibility*, **51**, no. 1, pp. 131-138 (2009).

[222] J. Wang, et al., "Application of Joint Time–Frequency Domain Reflectometry for Electric Power Cable Diagnostics," *IET Signal Processing*, **4**, no. 4, pp. 395-405 (2010).

[223] J. Wang, et al., "Health Monitoring of Power Cable Via Joint Time-Frequency Domain Reflectometry," *IEEE transactions on Instrumentation and Measurement*, **60**, no. 3, pp. 1047-1053 (2010).

[224] E. Song, et al., "Detection and Location of Multiple Wiring Faults Via Time–Frequency-Domain Reflectometry," *IEEE Transactions on Electromagnetic Compatibility*, **51**, no. 1, pp. 131-138 (2009).

[225] P. F. Fantoni, "Condition Monitoring of Electrical Cables Using Line Resonance Analysis (LIRA)," *17th International Conference on Nuclear Engineering*, American Society of Mechanical Engineers Digital Collection (2010).

[226] M. Ekelund, P. F. Fantoni, U. W. Gedde, "Thermal Ageing Assessment Of EPDM-Chlorosulfonated Polyethylene Insulated Cables Using Line Resonance Analysis (LIRA)," *Polymer testing*, **30**, no. 1, pp. 86-93 (2011).

[227] G. J. Toman, P. F. Fantoni, "Cable Aging Assessment and Condition Monitoring Using Line Resonance Analysis (LIRA)," *16th International Conference on Nuclear Engineering*, American Society of Mechanical Engineers Digital Collection (2009).

[228] P. F. Fantoni, *Wire System Aging Assessment and Condition Monitoring: The Line Resonance Analysis Method (LIRA)*, no. HWR-788, Institutt for Energiteknikk (2005).

[229] K. T. Gillen, R. A. Assink, R. Bernstein, "Condition monitoring approaches applied to a polychloroprene cable jacketing material," *Polymer Degradation and Stability*, **84**, no. 3, pp. 419-431 (2004).

[230] K. Anandakumaran, "Aging and Condition Monitoring Studies of Composite Insulation Cables Used in Nuclear Power Plants," *IEEE Transactions on Dielectrics and Electrical Insulation*, **14**, no. 1, pp. 227-237 (2007).

[231] Y. T. Hsu, et al., "Correlation Between Mechanical and Electrical Properties for Assessing the Degradation of Ethylene Propylene Rubber Cables Used in Nuclear Power Plants," *Polymer Degradation and Stability*, **92**, no. 7, pp. 1297-1303 (2007).

[232] J.-S. Kim, "Evaluation of Cable Aging Degradation Based on Plant Operating Condition," *Journal of Nuclear Science and Technology*, **42**, no. 8, pp. 745-753 (2005).

[233] D. McCarter, et al., "Nuclear power plant instrumentation and control cable prognostics using indenter modulus measurements," *International Journal of Prognostics and Health Management*, **16**, no. 5, pp. 1-10 (2014).

[234] V.A. Sotiris, W.T. Peter, and M. Pecht, "Anomaly detection through a Bayesian support vector machine." *IEEE Transactions on Reliability*, **59**, no. 2, pp.277-286 (2010).

[235] N. Gang, L. Xiong, X. Qin, M. Pecht, "Fault Detection Isolation and Diagnosis of Multi-Axle Speed Sensors for High-Speed Trains," *Mechanical Systems and Signal Processing*, **131**, pp. 183-198 (2019).

[236] M. Zhao, M. Kang, B. Tang, M. Pecht, "Multiple Wavelet Coefficients Fusion in Deep Residual Networks for Fault Diagnosis," *IEEE Transactions on Industrial Electronics*, **66**, no. 6, pp. 4696-4706 (2018).

[237] Y. Zhang, X. Rui, H. Hongwen, M. Pecht, "Long Short-Term Memory Recurrent Neural Network for Remaining Useful Life Prediction of Lithium-Ion Batteries," *IEEE Transactions on Vehicular Technology*, **67**, no. 7, pp. 5695-5705 (2018).

[238] J. Liu, J. Liu, D. Yu, M. Kang, W. Yan, Z. Wang, M. Pecht, "Fault Detection for Gas Turbine Hot Components Based on a Convolutional Neural Network," *Energies*, **11**, no. 8, pp. 2149 (2018).

[239] W. Yu, K. L. Tsui, W.M. Eden, M. Pecht, "A fusion approach for anomaly detection in hard disk drives," in *Proceedings of the IEEE 2012 Prognostics and System Health Management Conference (PHM-2012 Beijing)*, pp. 1-5. IEEE (2012).

[240] D. Enkhjargal, C. Chen, and M. Pecht, "A Bayesian Hidden Markov Model-based approach for anomaly detection in electronic systems," in *2013 IEEE Aerospace Conference*, pp. 1-10. IEEE, (2013).

[241] X. Jin, M. Zhao, T. Chow, and M. Pecht, "Motor Bearing Fault Diagnosis Using Trace Ratio Linear Discriminant Analysis," *IEEE Transactions on Industrial Electronics*, **61**, no. 5, pp. 2441–2451 (2014).

[242] S. Choi, E. Pazouki, J. Baek, and H. R. Bahrami, "Iterative Condition Monitoring and Fault Diagnosis Scheme of Electric Motor for Harsh Industrial Application," *IEEE Transactions on Industrial Electronics*, **62**, no. 3, pp. 1760–1769 (2015).

[243] H. Oh, T. Shibutani, and M. Pecht, "Precursor monitoring approach for reliability assessment of cooling fans," *Journal of Intelligent Manufacturing*, **23**, no. 2, pp. 173–178 (2012).

[244] M. Kang, J. Kim, In-Kyu Jeong, Jong-Myon Kim, and M. Pecht, "A Massively Parallel Approach to Real-Time Bearing Fault Detection Using Sub-Band Analysis on an FPGA-Based Multicore System," *IEEE Transactions on Industrial Electronics,* **63**, no. 10, pp. 6325-6335 (2016).

[245] W. He, Q. Miao, M. Azarian, and M. Pecht, "Health monitoring of cooling fan bearings based on wavelet filter," *Mechanical Systems and Signal Processing*, **64**, pp. 149-161 (2015).

[246] N. Lee, M. Azarian, M. Pecht, J. Kim, and J. Im, "A Comparative Study of Deep Learning-Based Diagnostics for Automotive Safety Components Using a Raspberry Pi," in *2019 IEEE International Conference on Prognostics and Health Management (ICPHM)*, pp. 1-7. IEEE (2019).

[247] A. Vasan, B. Long, and M. Pecht, "Diagnostics and prognostics method for analog electronic circuits," *IEEE Transactions on Industrial Electronics*, **60**, no. 11, pp. 5277-5291 (2012).

[248] V. Khemani, M. Azarian, and M. Pecht, "Electronic Circuit Diagnosis with No Data," in *2019 IEEE International Conference on Prognostics and Health Management (ICPHM)*, pp. 1-7. IEEE (2019).

Appendix A

CHARACTERIZATION OF PILOT SYSTEMS

This appendix provides a complete characterization (see Table 12) of the EHC, RCIC and HPCI systems from a risk-informed perspective.

Table 12. Characterization of EHC, RCIC and HPCI systems.

System Characterization	EHC System	RCIC and HPCI Systems
Key functions	Provide normal reactor pressure control by controlling steam flow consistent with reactor power, Control reactor pressure during startup, heatup, and cooldown evolutions, Control the speed and electrical load on the turbine generator, and Provide protection for the main turbine, main generator and main condenser.	The major functions include: Reactor vessel coolant inventory control, Reactor vessel pressure control. Additional functions may be specified but they are generally of lower safety importance and typically not modeled in the PRA.
Key Risk-Informed Applications		
50.65 Maintenance Rule	SSCs is within the rule scope because of potential to scram reactor or cause an engineered safety feature (ESF) actuation	Typically, SSCs are within scope due to being classified as safety related and also based on several risk importance criteria for RCIC and HPCI
50.69 – NEI 00-04 SSC Characterization & Treatment	In general, SSCs not categorized	The SSCs in these systems may be chosen for characterization and treatment
TSTF-425, NEI 04-10, SFCP	TSV and TCV testing frequency may be within scope but in many cases there are limitations on frequency adjustment because of concerns with main turbine missile generation analysis	Various surveillances have been extended (e.g., HPCI/RCIC Low Steam Supply Pressure Test, HPCI/RCIC Fill & Vent)

System Characterization	EHC System	RCIC and HPCI Systems
TSTF-505, NEI 06-09, RMTS	EHC may be indirectly in RMTS (i.e., risk-informed completion times) because the main turbine bypass valves (BPVs) typically are in scope as well as the closure of the TSVs and TCVs (which provide reactor protection system (RPS) input)	Typically, RCIC and HPCI are within scope of RMTS program
RG 1.178 Inservice Inspection of Piping	Generally, not in-scope	Typically, RCIC and HPCI are within scope of the RI-ISI program
Potential Impacts on Generation		
Direct loss of generation due to equipment reliability and availability issues	Performance of the EHC directly impacts plant thermal efficiency and electrical generation. System failure can directly cause a turbine trip and subsequent reactor scram.	RCIC and HPCI are standby only and their performance does not directly affect electrical power generation.
Indirect impacts (e.g., Tech Specs limiting condition for operation)	Generally, the steam cycle aspects of the turbine typically are not within Technical Specifications (TS). However, the BPVs are within TS as well as inputs to the RPS including: TSV Closure, Trip Oil Pressure – Low Function TCV Fast Closure Trip Oil Pressure – Low Function when thermal power is greater than a specified percentage.	RCIC and HPCI are subject to Technical Specifications. The allowed outage times (AOTs) are plant-specific with limits on the time that these systems may be inoperable before action up to and including plant shutdown is necessitated.
Potential Impacts of Off-normal Transients and Accidents		

System Characterization	EHC System	RCIC and HPCI Systems
With no physical damage to equipment	The vast majority of off-normal transients (e.g., turbine trip/reactor trip) involve no major damage to equipment necessitating more than a few days of assessment or repair.	The vast majority of RCIC and HPCI performance issues can be readily addressed (within the allowed outage times prescribed in the plant Technical Specifications) and do not require long repair times or large capital expenditures.
With physical damage to equipment	Incidents involving turbine overspeed precursors or actual events can result in root cause analysis and in some cases extensive repair resulting in weeks of outage. In a worst-case scenario, the turbo-generator could be catastrophically damaged potentially resulting in several months of lost generation and extensive repair/replacement costs.	Hazards such as internal flooding of the RCIC and HPCI compartments or fire in those compartments can have major impacts necessitating significant repair and in extreme cases replacement of key components.
Potential Regulatory Impacts		
MD 8.3 Incident Investigation	Incidents involving turbine overspeed precursors or actual events could result in NRC investigation such as special inspection (or greater) depending on the risk significance of the event.	Risk-significant failures of RCIC or HPCI could prompt NRC investigation. The NRC will typically review the sequence of events, and the licensee's root cause analysis, determine the probable causes, and assess the corrective actions to address the RCIC/HPCI inoperability.
Significance Determination Process (SDP) for inspection finding	The risk significance of a performance deficiency involving EHC-related off-normal transients or accidents with failures of mitigating equipment is evaluated and used to establish whether and to what extent NRC applies additional inspections.	The risk significance of a performance deficiency involving RCIC or HPCI is evaluated and used to establish whether and to what extent NRC applies additional inspections.
Reactor Oversight Process performance indicators (e.g., MSPI)	Initiating events such as unplanned scrams (per 7000 critical hours) or unplanned scrams with complications will impact performance indicators (initiating events). However, EHC performance is not assessed by the MSPI.	The risk impacts of RCIC or HPCI reliability and availability departures from established baselines are assessed in the MSPI. RCIC/HPCI failures may also factor into the safety system functional failure (SSFF) performance indicator.

Appendix B

SUMMARY OF RI APPLICATIONS

Table 13 summarizes the most relevant RI applications from a decision-making perspective (e.g., cost vs. savings) while Table 14 links specific SSC parameters to RI applications.

Table 13. RI applications impact on plant decisions.

RI application	Complexity	Implementation	PRA input	Cost (upfront)	Cost (subsequent)	Roadblocks	Savings (hard/soft $)
RMTS, 4(b), RICT	H	Moderate	H	H	L	PRA quality- CC II with closure of peer review findings; Regulatory uncertainty,	Hard: Allows maintenance at power thus shortening refueling outage; avoid forced shutdown
SFCP, 5(b)	L	Easy	M	M	L	Some PRA quality issues; also, heavily dependent on Engineering Department staff availability and participation	Hard: Reduced testing of equipment and costs, avoidance of power reduction and/or reduced refuel outage duration. Reduced worker exposure. Soft: Reduction of high-risk evolutions leading to reactor scram.
50.69	categ. = H treat. = M	Hard	M	M	H	PRA quality- CC II with closure of peer review findings; also, seismic issues.	Hard: Reduced procurement costs, as well as reduced testing and inspection
RI-ISI	M	Moderate	M	L	L	None. Has been implemented across nearly the entire U.S. fleet	Hard: Direct savings in terms of reduced inspections and reduced worker radiation exposure

Table 14. Links between RI applications and SSC parameters.

RI application	Affected SSC parameters
RMTS	In-scope SSCs, specific Technical Specifications LCOs affected
SFCP	Specific Technical Specifications Surveillance Requirements affected and associated frequency change, impact on time-related failure probability
10CFR50.69	Replacement cost savings, maintenance and testing cost savings, new reliability data
RI-ISI	In-scope ASME piping Classes and segments/elements, associated risk metrics

Appendix C

MAPPING OF NPP EVENTS TO PLANT IMPACT STATES

Table 15 provides a summary of events which may occur in a NPP and their relative cost impact binned in ranges listed in Table 16.

Table 15. NPP event vs. cost impact.

Event	Nominal Outage Duration	Median Impact	Uncertainty Range	Comment
Minor equipment issue	None	C0	C0-C1	Plant-specific data
Minor equipment repair	None	C1	C0-C2	Plant-specific data
Equivalent of several hours of lost generation due to equipment problems	2 hours	C2	C1-C3	Plant-specific data
Equivalent of one shift of lost generation due to equipment problems	8 hours	C3	C2-C4	Plant-specific data
Equivalent of one day of lost generation due to equipment problems	1 day	C4	C3-C5	Plant-specific data
Equivalent of several days of lost generation due to equipment problems	3 days	C5	C4-C6	Plant-specific data
Uncomplicated reactor trip or manual shutdown	Days to 1 week	C6	C5-C7	Industry event data
Complicated reactor trip with minimal physical damage	1 week	C6	C5-C7	River Bend electrical fault causing loss of normal service water, circulating water, and feedwater (May 2012)
Internal flooding – spray event on key equipment	1 week	C6	C5-C7	Judgment, pairwise comparison
Fire to one key component	1 week	C6	C5-C7	Waterford feedwater pump fire (June 1985)
Inadvertent/stuck-open primary SRV (BWR only)	1 week	C6	C5-C7	Judgment, pairwise comparison

Event	Nominal Outage Duration	Median Impact	Uncertainty Range	Comment
Loss of offsite power	1 to 2 weeks	C7	C6-C8	Industry event data, potential for accident sequence precursor or special inspection per MD 8.3 (e.g., Browns Ferry-3 LOOP, May 2012)
ECCS suction from suppression pool (BWR)	2 weeks	C7	C6-C8	Judgment, pairwise comparison
Complicated reactor trip with some physical damage	2 to 4 weeks	C7	C6-C8	Byron-2 (Jan 2012) electrical fault
Tornado through site – some damage to non-safety SSCs	4 weeks	C7	C6-C8	Browns Ferry, impact per unit (April 2011)
General internal flooding - early termination	4 weeks	C7	C6-C8	Millstone-3 MSR drain line ruptures (Dec 1990), Oconee-2 FW heater extraction line rupture (June 1982)
Turbine building or switchgear room fire with some physical damage	4 weeks	C7	C6-C8	Quad Cities-2 (April 2014), Oconee-1 (Jan 1989)
Fire in main transformer	10 weeks	C8	C7-C9	STP-2 fire (Jan 2013)
BWR emergency depressurization / blowdown	10 weeks	C8	C7-C9	Judgment, pairwise comparison, Regulatory impact
Complicated reactor trip with significant physical damage	10 weeks	C8	C7-C9	Wolf Creek (Jan 2012)
BWR containment venting	10 weeks	C8	C7-C9	Judgment, pairwise comparison, Regulatory impact
PWR feed & bleed – short duration	10 weeks	C8	C7-C9	Judgment, pairwise comparison, Regulatory impact
Extended Station Blackout	10 weeks	C8	C7-C9	Judgment, pairwise comparison, Regulatory impact
Major feed line/steam line break outside containment with significant physical damage (PWR)	10 weeks	C8	C7-C9	Judgment, pairwise comparison
Major internal flooding – early termination	10 weeks	C8	C7-C9	Judgment, pairwise comparison
Seismic event at or beyond design basis	10 weeks	C8	C7-C9	North Anna seismic inspection & analysis, per unit (Aug 2011)

Event	Nominal Outage Duration	Median Impact	Uncertainty Range	Comment
Switchgear room fire with some damage	10 weeks	C8	C7-C9	Robinson (March 2010), Waterford (June 1995)
Turbine building fire with moderate physical damage	10 weeks	C8	C7-C9	Salem-2 (Nov 1991)
Stuck-open primary PORV/SRV – short duration up to point of sump recirculation (PWR)	10 weeks	C8	C7-C9	Judgment, pairwise comparison
Stuck-open primary PORV/SRV – long duration through sump recirculation (PWR)	1 year	C9	C8-C10	Judgment, pairwise comparison
Switchgear room fire with significant damage	1 year	C9	C8-C10	Judgment, pairwise comparison (several significant fires in the former Soviet Union and Eastern Europe, see NUREG/CR-6738)
Major external flooding	1 year	C9	C8-C10	Ft. Calhoun (June 2011), judgment, pairwise comparison
Major feed line/steam line break inside containment (BWR)	1 year	C9	C8-C10	Judgment, pairwise comparison
Catastrophic turbine-generator fire	1 year	C9	C8-C10	Maanshan-1 (July 1985)
Reactor coolant pump seal LOCA	1 year	C9	C8-C10	Judgment, pairwise comparison
Small pipe-break LOCA	1 year	C9	C8-C10	Judgment, pairwise comparison, Regulatory impact
Steam generator tube rupture	1 year	C9	C8-C10	Indian Point-2 (Feb 2000), Regulatory impact
PWR feed & bleed – long duration through recirculation	1 year	C9	C8-C10	Judgment, pairwise comparison, Regulatory impact
ATWS at high power – BWR or PWR	1 year	C9	C8-C10	Judgment, pairwise comparison, Regulatory impact (1983 Salem events were at low power)
Raw (fresh) water injection into steam generator(s)	1 year	C9	C8-C10	Judgment, pairwise comparison
General or major internal flooding – no termination	1 year	C9	C8-C10	Judgment, pairwise comparison

Event	Nominal Outage Duration	Median Impact	Uncertainty Range	Comment
Major feed line/steam line break inside containment (PWR)	1 year	C9	C8-C10	Judgment, pairwise comparison
BWR alternate RPV injection with alternate water source (raw but fresh water)	1 year	C9	C8-C10	Judgment, pairwise comparison
Switchgear room or cable spreading room fire with catastrophic damage	> 1 year	C10	C9-C11	Browns Ferry (March 1975), see also NUREG/CR-6738
Salt water injection into steam generator(s)	> 1 year	C10	C9-C11	Cost data, judgment, pairwise comparison
Medium LOCA	> 1 year	C10	C9-C11	Judgment, pairwise comparison, Regulatory impact, near-miss 2002 Davis-Besse vessel head degradation
Short-duration core uncovery and fuel temperature excursion	> 1 year	C10	C9-C11	Judgment, pairwise comparison, Regulatory impact
BWR RPV injection after containment failure but no CD	terminal	C11	C10 up to loss of plant	Judgment, pairwise comparison, Regulatory impact
Large LOCA	terminal	C11	C10 up to loss of plant	Judgment, pairwise comparison, Regulatory impact
ISLOCA – major leakage/rupture outside containment but no CD	terminal	C11	C10 up to loss of plant	Judgment, pairwise comparison, Regulatory impact
Pressurized thermal shock of reactor pressure vessel	terminal	C11	C10 up to loss of plant	Judgment, pairwise comparison, Regulatory impact
Contained core damage event, minimal to small release	terminal	C12	C11 up to C13	TMI-2 accident costs adjusted to current dollars (rounded), e.g., NUREG/BR-0058 and 0184
Core damage event, large release	terminal	C13	C12 up to 3x C13	Estimated Fukushima accident costs (rounded)

Table 16. Cost associated to each impact bin.

Impact Bin	Value
C0	$0
C1	$30,000
C2	$100,000
C3	$300,000
C4	$1 million
C5	$3 million
C6	$10 million
C7	$30 million
C8	$100 million
C9	$300 million
C10	$600 million
C11	$1 billion
C12	$10 billion
C13	$100 billion

Appendix D

STANDBY FAILURE MODEL

Reliability is the likelihood that a SSC performs its required function(s) for a specified period of time [45]. Unreliability is the mathematical complement of reliability and is the likelihood that an SSC does not operate for its mission time when required.

Availability represents the degree to which an SSC is operational and accessible when required for use, with no reference to a mission time [45]. Unavailability is the mathematical complement of availability. Unavailability modeling in plant PRAs generally is with regard to testing and maintenance of the SSC.

The standby failure rate model is a simplified means of representing a state of failure of an SSC. In this model, the failure rate is given by λ which we take to be a constant failure rate with time, T, the time period during which the SSC is "ready" for actual operation [46]. For SSCs that are not continuously monitored but for which periodic surveillance is performed, the probability that the SSC will be in a failed state when demanded is given by the well-known expression:

$$Q = \tfrac{1}{2}\lambda T + \lambda T_R \qquad \text{(D-1)}$$

where T is the time between STs or PM, and T_R is the repair time. Here it is assumed that the SSC is fully renewed following the ST or PM (i.e., the SSC is in "a good as new" condition). Often it is also assumed that the repair time, typically hours or days, is small in comparison to the test interval, one month to 24 months (typical BWR refueling cycle). For this situation of small repair time, Equation D-1 can be simplified by:

$$Q \approx \tfrac{1}{2}\lambda T \qquad \text{(D-2)}$$

Plant-specific data on unavailability are collected at the component, train, or system level by a number of risk-informed programs and processes as described in greater detail in Section 5 of this report.

If θ represents the mean time that an SSC is unavailable due to test and maintenance, then to Equation D-2 we can include the contribution of that unavailability to give the total as:

$$Q_t = \tfrac{1}{2}\lambda T + \theta/T \qquad \text{(D-3)}$$

In theory, the test interval, T, can be optimized (from the perspective of SSC reliability and availability) by finding the value that minimizes Q_t. Differentiating Equation D-3 with respect to T gives:

$$dQ_t/dT = \tfrac{1}{2}\lambda - \theta/T^2 \qquad \text{(D-4)}$$

Setting Equation D-4 to zero and re-arranging to find the optimum test interval, T_{opt}, gives the well-known expression:

$$T_{opt} = \sqrt{2\theta/\lambda} \qquad \text{(D-5)}$$

For most mechanical equipment including pumps, valves, and emergency diesel generators, the actual test intervals specified in the plant TS is found to be not too far off from the optimum. There are exceptions, of course, for SSCs that cannot be tested during power operation or would result in unnecessary radiological exposure to workers. Additionally, too frequent testing can result in "wear-out" which has the effect of increasing the failure rate λ with time, thus negating the assumption of constant failure rate.

The reliability principles expressed by Equations D-3 and D-5 are illustrated in Figure 28 where we represent the x-axisby *frequency* of performing the PM or ST (i.e., $1/T$, the reciprocal of the test period).

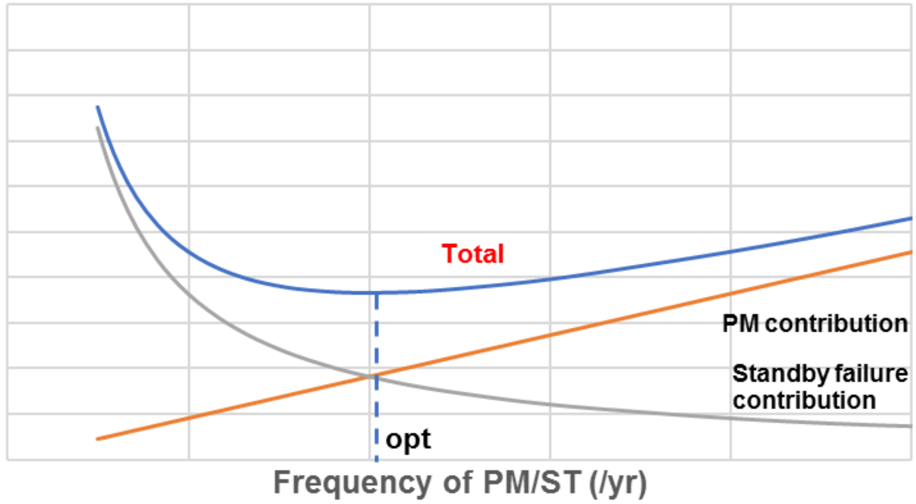


Figure 28. Total probability that SSC is in a failed state Q_t.

A shortcoming of this standby model is that it simplifies the treatment of real-world failure mechanisms by aggregating all degradations and failure mechanisms into one constant rate parameter, λ. Also, while optimizing reliability, the approach does not necessarily optimize total testing and maintenance costs.

In reality, SSCs can degrade or fail by a number of vastly different mechanisms, each with its own rate of failure/degradation, repair time, contribution to train/system unavailability, and repair cost. If N represents the total number of degradation and failure mechanisms for which plant-specific data can be collected, then Equation D-3 can be expanded to give:

$$Q_t = (\tfrac{1}{2}\, \lambda_1 T + \theta_1/T) + \ldots + (\tfrac{1}{2}\, \lambda_N T + \theta_N/T) \qquad \text{(D-6)}$$

The "optimum" test interval is thus no longer clear. Each degradation or failure mechanism will have its individual optimum interval for ST and PM depending on the relative magnitudes of λ_N and θ_N. In practice, plant-specific programs account for this observation (at least qualitatively) and have implemented ST and PM procedures at differing frequencies, although these have not necessarily been optimized from the perspective of cost.

Cost considerations can be factored into Equation D-6 by including plant-specific repair and testing/maintenance costs for each of the degradation/failure mechanisms, N. If C_R represents the generalized repair cost, and C_{TM} the generalized cost of the ST or PM, then Equation D-6 can be modified to give the total annual testing, maintenance, and repair cost for a particular SSC as:

$$C_t = \lambda_1\, C_{R1} + C_{TM1}\, /T + \ldots + \lambda_N\, C_{RN} + C_{TMN}\, /T \quad (\$/\text{yr}) \qquad \text{(D-7)}$$

It can be demonstrated that for typical component failure rates and PM/ST frequencies that costs are usually dominated by the ST and PM costs. For example, assume the following:

- $\lambda = 10^{-5}$ /hr
- $T = 720$ hr (monthly testing)
- $C_R = \$4{,}000$ (nominal 40 labor hours @ $100 /hr for most small repairs)
- $C_{TM} = \$200$ (nominal 1 hr ST duration assuming 2 personnel).

Repair cost would thus be: (10^{-5} /hr) (8760 hr/yr) (\$4,000) = \$350 /yr

Testing cost would be: (\$200) (8760 hr/yr) /720 hr = \$2400 /yr

Thus, test and maintenance costs are found in this example to totally dominate overall costs.

Care must be taken not to generalize this observation for one particular failure mode to all possible degradation and failure mechanisms. A catastrophic failure mode that is one to two orders of magnitude lower in frequency but results in the need to completely overhaul or replace the SSC (e.g., emergency diesel generator) could be the overall dominant contributor to SSC costs if a plant forced shutdown is also the consequence of the assumed failure.

The costs represented by routine PM/ST and small-to moderate scope SSC repair are often referred to as *hard* costs shown on the balance sheet. Additional *soft* costs that potentially lead to regulatory impact as well as lost power generation need to be considered as well.

For example, an SSC failure mechanism that is the result on a licensee performance deficiency and leads to an increase in core damage frequency of greater than 1.E-5 yr^{-1} and a Yellow inspection finding under the NRC's Reactor Oversight Process (ROP) may have associated costs (NRC inspection time, plant staff support, plant modifications, program impacts) of some \$30 million. Concern over potential regulatory impact could be reason enough to perform more frequent testing than the "optimum" might indicate. The framework in this project must therefore factor in conditional probabilities that various failure mechanisms result in regulatory impact in addition to the potential for forced plant shutdown.

Appendix E

MARKOV METHOD

Given some of the shortcomings of the Standby Failure Model, an alternate approach to applying plant-specific data in this project is the use of the Markov Method. A full discussion of this approach is beyond the scope of this report and the reader is referred to Lee and McCormick [47] or any number of other publications on reliability theory.

Figure 29 shows a Markov Model for a simple generalized SSC. In this illustration, three general states are indicated:

- State S: fully functional (i.e., Success)
- State D: degraded
- State F: failed

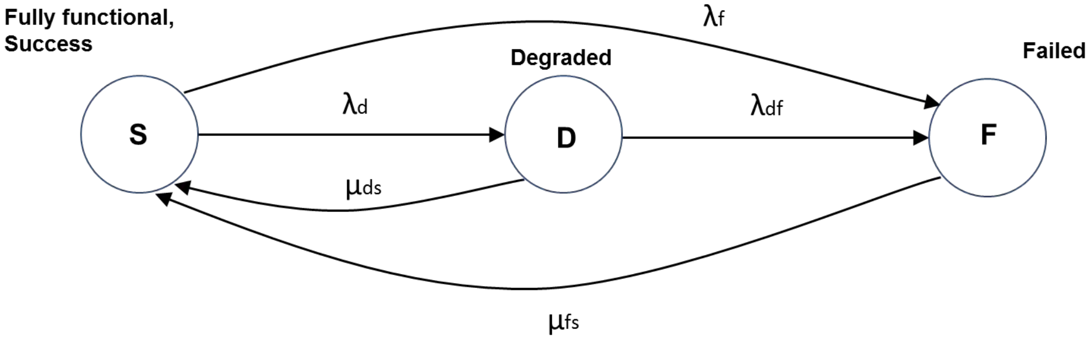


Figure 29. Markov model example.

A degraded state might be a condition requiring attention such as a pump vibration alarm in the alert condition. In this state there is an increased probability that if no action is taken the SSC would eventually fail. Therefore, planned maintenance would be scheduled and performed to restore the SSC to a fully functional condition. Also shown are transition rates, *λ*, from Success to Degraded, Degraded to Failed, and Success directly to Failed. These rates can be derived from the plant performance data corresponding to the reciprocals of Mean-Time-To-Degradation (MTTD) and Mean-Time-To-Failure (MTTF).

Repair rates are given by *μ*. For SSCs that are continuously monitored such as many electronic circuits, the various values of *μ* represent strictly the repair time. For many SSCs such as mechanical equipment, the degraded or failed state may be found only during ST, PM, or upon occurrence of an actual demand. In these cases, the values of *μ* need to reflect detection time as well. Variations of the Markov diagram could decompose such rates into detection and repair.

From the transition rates illustrated in Figure 29 a set of coupled linear differential equations can be written as follows:

$$dS/dt = -\lambda_d S - \lambda_f S + \mu_{ds} D + \mu_{fs} F \tag{E-8a}$$

$$dD/dt = \lambda_d S - \lambda_{df} D - \mu_{ds} D \tag{E-8b}$$

$$dF/dt = \lambda_f S + \lambda_{df} D - \mu_{fs} F \tag{E-8c}$$

In this simple model it is assumed that all of the transition rates, λ and μ, are constant with time. The above differential equations can be solved using Laplace transforms and linear algebra akin to solutions for radioactive decay chains. The results are exponential functions for the various states from which the probabilities of the various states also can be derived.

As is the case for the Standby Failure Model, SSCs can degrade or fail by a number of vastly different mechanisms, each with its own rate of failure/degradation, repair time, contribution to train/system unavailability, and repair cost. Thus, Equations E-8a through c can be modified to include more states of degradation and failure to the degree that the plant-specific SSC performance data support the added complexity.

Appendix F

DATA ANALYSIS EXAMPLES

Example 1: Small Motor Replacement in RCIC System

On-going PMs identify the need to replace all or portions of the vacuum pump motor that is part of the RCIC system. A WO is generated and some 30 tasks are specified as part of the WO. These include tasks such as:

- Disassemble, clean and inspect pump
- Repair minor wiring
- Adjust motor resistor
- Inspect and clean discharge check valve on RCIC pump
- Clean gasket surfaces
- Reassemble pump with new gaskets
- Install the proper amount of shims to set the correct impeller gap
- Install new packing
- Fill lantern ring with specified grease.

During the work, the on-line risk monitor transitioned from GREEN to YELLOW per the Operations Log. The System Unavailability file lists a nominal 60 hours of unavailability that were accrued due to this planned maintenance.

A summation of the individual WO tasks gives total labor as 135 hours. At an assumed nominal fully-loaded cost plus unspecified overhead (e.g., engineering resources, operations resources, etc.) of $100 per hour, nominal cost of this task is about $13k plus materials (therefore it is presumed that this task incurred under $50k in total costs).

The integrated plant PRA model (full-power internal events plus fire) has CDF of 8.E-6/yr and large early release frequency (LERF) of 3.E-7/yr. The associated risk achievement worth (RAW) for CDF has a nominal value of about 3 for RCIC. The ICCDP of the PM, taking no credit for any compensatory measures that may have been implemented during the RCIC outage is thus:

ICCDP ~ (3 - 1) (8.E-6/yr) (60/8760) ~ 1.E-7

This is a small but not insignificant fraction of the plant annual core damage probability of 8.E-6.

Economic risks consist of:

- Regulatory impact
- Lost generation
- Economic damages from potential accidents.

The RCIC system has a 14-day (336 hr) AOT per the plant Technical Specifications, so there is little risk of exceeding this limit and entering a forced plant shutdown.

The MSPI uses a 3-year moving time period for the system performance, so the incremental contribution to the MSPI from this activity to refurbish the motor is about 3.E-8 compared to the White threshold at 1.E-6. So, there is little impact on the MSPI.

From these results it is concluded that there is very low adverse regulatory impact from carrying out this WO. Additionally, it can be concluded that the improvement in system reliability and performance more than compensates for the unavailability that was incurred on the system as a result of performing the maintenance.

Since the RCIC system is a standby system and not used for power generation, there is no possibility of reactor trip and lost generation from this activity. As discussed above, the risk of unplanned plant shutdown due to exceeding the AOT is low for this activity.

The unavailability of the RCIC system for the nominal 60 hours of outage time is estimated above as contributing to a theoretical increase in core damage probability of ~1.E-7. Appendix C of this report gives a categorization of C12 and $10 billion for the plant impact vector resulting from core damage. The associated contribution to economic risk thus is estimated to be a nominal value of

$$(10^{-7})\ (\$10^{10})\text{ or} \sim \$1000$$

Similar calculations for the contribution to large early release probability using appropriate plant risk metrics gives an additional economic risk contribution of ~$100.

In summary, the economic risk contribution from regulatory impact, lost generation potential, and potential accident damages is a small fraction of the total cost of this PM task.

The benefits of refurbishing the motor are more difficult to ascertain using strictly the plant data that has been provided for this project. If operation of the vacuum pump motor was absolutely necessary for Operability of RCIC then allowing the motor to further degrade would adversely impact RCIC failure probability and overall system unavailability.

The plant 10 CFR 50.69 documentation describes the vacuum pump as non-safety, RISC-4 and LSS. Hence, the immediate risk impact of vacuum pump degradation/failure is evaluated to be low. However, the vacuum pump serves to condense steam that leaks from the RCIC turbine seals to limit radioactivity levels in the RCIC room. Thus, failure of this SSC would have a worker radiological exposure impact. A water spray condenses the steam which is then dumped into the RCIC pump discharge and the non-condensibles go to the suppression pool. Therefore, long-term impacts of this function of the vacuum pump need to be assessed to further quantify the benefits of this motor refurbishment. This is beyond the scope of the current effort; however, such evaluation would be appropriate for inclusion in LTAM plan for the RCIC system. Almost any measurable contribution to RCIC failure probability would have regulatory impact, with the nominal cost of a White inspection finding or White MSPI estimated at about $10 million. Hence, PM activity that averts even a few percent increase in the probability of a White Regulatory finding (probability of a $10 million impact versus total cost of repair at under $50k when materials are included) would clearly tilt the Cost-Benefit equation in favor of motor replacement and continuation of performance of this PM.

Example 2: RCIC System MOV Switch Failure

During a surveillance test an MOV in the RCIC system failed to open. This valve needs to be open to provide RCIC pump suction from the suppression pool. The system is designed that normal pump suction is from the CST until a low tank level is reached, at which time automatic switchover to the suction from the suppression pool occurs. For this event, an IR was generated, and a WO was created. The failure was due to an auxiliary contactor for a hand switch which was then replaced. The System Unavailability file gives a nominal 5 hours of RCIC system unavailability during the work.

Because of multiple suction sources, the PRA identifies the RAW for the valve in question as having only a nominal 1.4 value. The ICCDP estimate using the mathematical approach as for Example #1 gives about 3.E-8, a very low value. Review of the MSPI for the corresponding calendar quarter showed an

Unavailability Index (UAI) increase from the previous quarter for the High Pressure Injection function of an amount comparable to the 3.E-8 increment.

Without further detailed review of the historical MSPI worksheets, it is unclear from the plant data that was provided whether a functional failure was counted in the MSPI program. However, it can be illustrated that one additional MOV failure within the RCIC system over a 3-year period would have no impact. Specifically, the performance data are pooled for MOVs in the RCIC system resulting in several hundred demands, and because of the Bayesian process for determining a change in MOV failure probability from the baseline, one additional MOV failure within the system would have no measurable impact on the Unreliability Index in the MSPI. This was confirmed by a review of the MSPI for the calendar quarter in question. Hence it was concluded that the MOV failure (i.e., auxiliary contactor failure in a hand switch) has no regulatory impact.

Based on the quantification in Example #1, it also can be concluded that economic risk contribution from lost generation and the potential to affect accident damage costs are insignificant.

Labor hours for the switch repair were recorded as 35. Hence, repair costs are under $10k. Regardless of the potential benefits of the repair, these costs under $10k would appear to be at a level *below concern* and the repair is justified simply on the basis of maintaining the plant in good working order for routine operations. In fact, many operating NPPs have instituted “Fix it Now” (FIN) teams that are specifically tasked with addressing such minor maintenance activities as they arise. As a result, the marginal costs associated with addressing this type of failure are likely to have been conservatively estimated in this analysis. Because the required surveillance performed its objective of identifying failures or degraded system performance, it is concluded that the ST provides a valuable contribution to maintaining adequate system availability, reliability, and performance.

Example 3: HPCI Turbine Bearing Oil Leak

A significant oil leak was identified on the HPCI turbine following turbine shutdown from scheduled pump valve and flow testing. An IR was generated, and a WO was processed. Investigation of the source of the oil leak identified that the pressure retaining portion of the pressure switch failed allowing oil to enter the switch housing. Oil was found leaking from the switch housing and an unsealed intermediate junction box where the pressure switch flexible conduit terminated. The oil leak rate was estimated to be about one liter per minute with the auxiliary oil pump operating. This leak was classified as a Maintenance Rule Functional Failure, as well as a failure of the HPCI turbine as a monitored component in the MSPI program. This was confirmed by observing an incremental change in UAI and step change in Unreliability Index (URI) under the MSPI program for the High Pressure Injection function.

As a result of this failure, HPCI unavailability of about 15 hours was accrued. Labor hours for repair amounted to about 40. The PRA gives a RAW for the HPCI system of about 4.

In comparison to Example #1, the RAW for HPCI is slightly higher than for RCIC (4 versus 3) while the hours of unavailability are substantially less (15 hr versus 60) in this example. Simply by inspection of the ratios of RAW and hours of unavailability the risk impact of the unavailability of HPCI in this example is bounded by the RCIC Example #1. Reactor risk and economic risk are low due to unavailability alone.

However, there still remains the matter of the effect of the HPCI pump failure on unreliability and its impact on ICCDP. The plant PRA database for HPCI indicates HPCI functional failures are rare, with few recorded failures over the previous 10-year observation period. Therefore, any one additional failure may have a small but noticeable impact on calculated risk.

For example, the Birnbaum importance measure for HPCI is approximated by:

$B \sim (RAW - 1) * CDF$

B ~ (4 - 1) * 8.E-6/yr

B ~ 2.4E-5/yr

Nominal failure to start (FTS) probability for the HPCI pump is approximately 0.01, while failure to run (FTR) for a 4-hour mission is approximately 0.002. Doubling of the FTS probability results in a nominal 2.E-7/yr increase in CDF (B * 0.01), which is small but not insignificant. Like Example #1, ensuring that these types of failures are not repeated is clearly cost effective.

Appendix G

HPI RELIABILITY MODELING

For the HPI system scheme shown in Figure 16, we have constructed the FT for the HPI system as shown in Figure 30, Figure 31 and Figure 32. In our application some of the failure rates and failure probabilities in Figure 30, Figure 31 and Figure 32 were updated with the values generated by the unavailability models described in Section 8.2.1. The corresponding list of Minimal Cut Sets (MCSs) is shown in Table 17. In particular, the unavailability models for pumps and valves of the HPI system scheme shown in Figure 16 were linked to the Basic Events as indicated in Table 18 and Table 19.

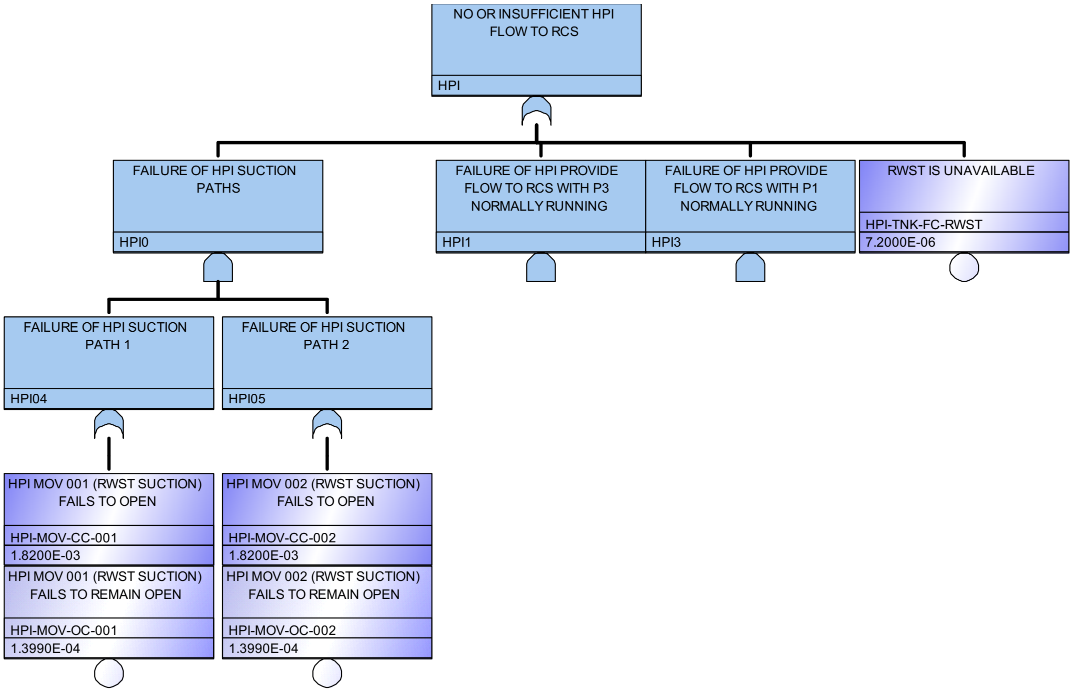

NO OR INSUFFICIENT HPI FLOW TO RCS
HPI
FAILURE OF HPI SUCTION PATHS
HPI0
FAILURE OF HPI PROVIDE FLOW TO RCS WITH P3 NORMALLY RUNNING
HPI1
FAILURE OF HPI PROVIDE FLOW TO RCS WITH P1 NORMALLY RUNNING
HPI3
RWST IS UNAVAILABLE
HPI-TNK-FC-RWST
7.2000E-06
FAILURE OF HPI SUCTION PATH 1
HPI04
FAILURE OF HPI SUCTION PATH 2
HPI05
HPI MOV 001 (RWST SUCTION) FAILS TO OPEN
HPI-MOV-CC-001
1.8200E-03
HPI MOV 001 (RWST SUCTION) FAILS TO REMAIN OPEN
HPI-MOV-OC-001
1.3990E-04
HPI MOV 002 (RWST SUCTION) FAILS TO OPEN
HPI-MOV-CC-002
1.8200E-03
HPI MOV 002 (RWST SUCTION) FAILS TO REMAIN OPEN
HPI-MOV-OC-002
1.3990E-04

Figure 30. HPI system fault tree.

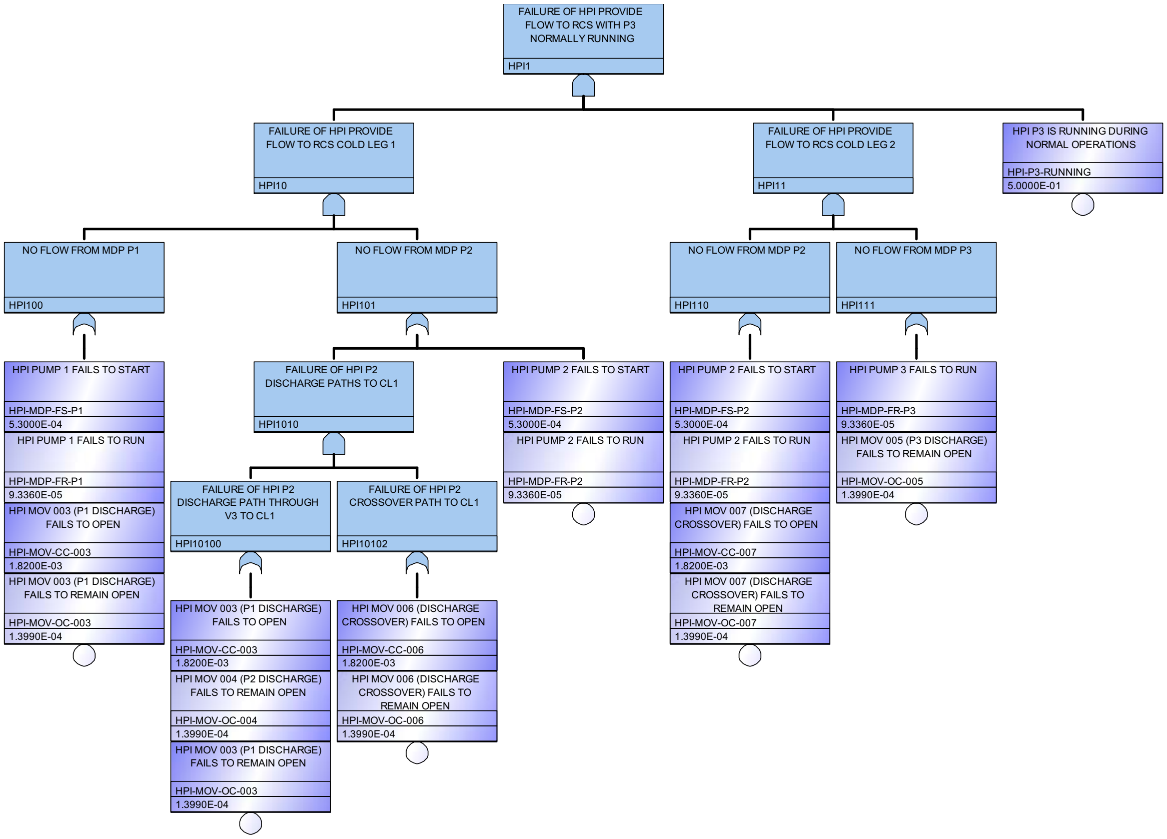

FAILURE OF HPI PROVIDE FLOW TO RCS WITH P3 NORMALLY RUNNING
HPI1
FAILURE OF HPI PROVIDE FLOW TO RCS COLD LEG 1
HPI10
FAILURE OF HPI PROVIDE FLOW TO RCS COLD LEG 2
HPI11
HPI P3 IS RUNNING DURING NORMAL OPERATIONS
HPI-P3-RUNNING
5.0000E-01
NO FLOW FROM MDP P1
HPI100
NO FLOW FROM MDP P2
HPI101
NO FLOW FROM MDP P2
HPI110
NO FLOW FROM MDP P3
HPI111
HPI PUMP 1 FAILS TO START
HPI-MDP-FS-P1
5.3000E-04
HPI PUMP 1 FAILS TO RUN
HPI-MDP-FR-P1
9.3360E-05
HPI MOV 003 (P1 DISCHARGE) FAILS TO OPEN
HPI-MOV-CC-003
1.8200E-03
HPI MOV 003 (P1 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-003
1.3990E-04
FAILURE OF HPI P2 DISCHARGE PATHS TO CL1
HPI1010
HPI PUMP 2 FAILS TO START
HPI-MDP-FS-P2
5.3000E-04
HPI PUMP 2 FAILS TO RUN
HPI-MDP-FR-P2
9.3360E-05
FAILURE OF HPI P2 DISCHARGE PATH THROUGH V3 TO CL1
HPI10100
FAILURE OF HPI P2 CROSSOVER PATH TO CL1
HPI10102
HPI MOV 003 (P1 DISCHARGE) FAILS TO OPEN
HPI-MOV-CC-003
1.8200E-03
HPI MOV 004 (P2 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-004
1.3990E-04
HPI MOV 003 (P1 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-003
1.3990E-04
HPI MOV 006 (DISCHARGE CROSSOVER) FAILS TO OPEN
HPI-MOV-CC-006
1.8200E-03
HPI MOV 006 (DISCHARGE CROSSOVER) FAILS TO REMAIN OPEN
HPI-MOV-OC-006
1.3990E-04
HPI PUMP 2 FAILS TO START
HPI-MDP-FS-P2
5.3000E-04
HPI PUMP 2 FAILS TO RUN
HPI-MDP-FR-P2
9.3360E-05
HPI MOV 007 (DISCHARGE CROSSOVER) FAILS TO OPEN
HPI-MOV-CC-007
1.8200E-03
HPI MOV 007 (DISCHARGE CROSSOVER) FAILS TO REMAIN OPEN
HPI-MOV-OC-007
1.3990E-04
HPI PUMP 3 FAILS TO RUN
HPI-MDP-FR-P3
9.3360E-05
HPI MOV 005 (P3 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-005
1.3990E-04

Figure 31. HPI1 gate with P3 normally running.

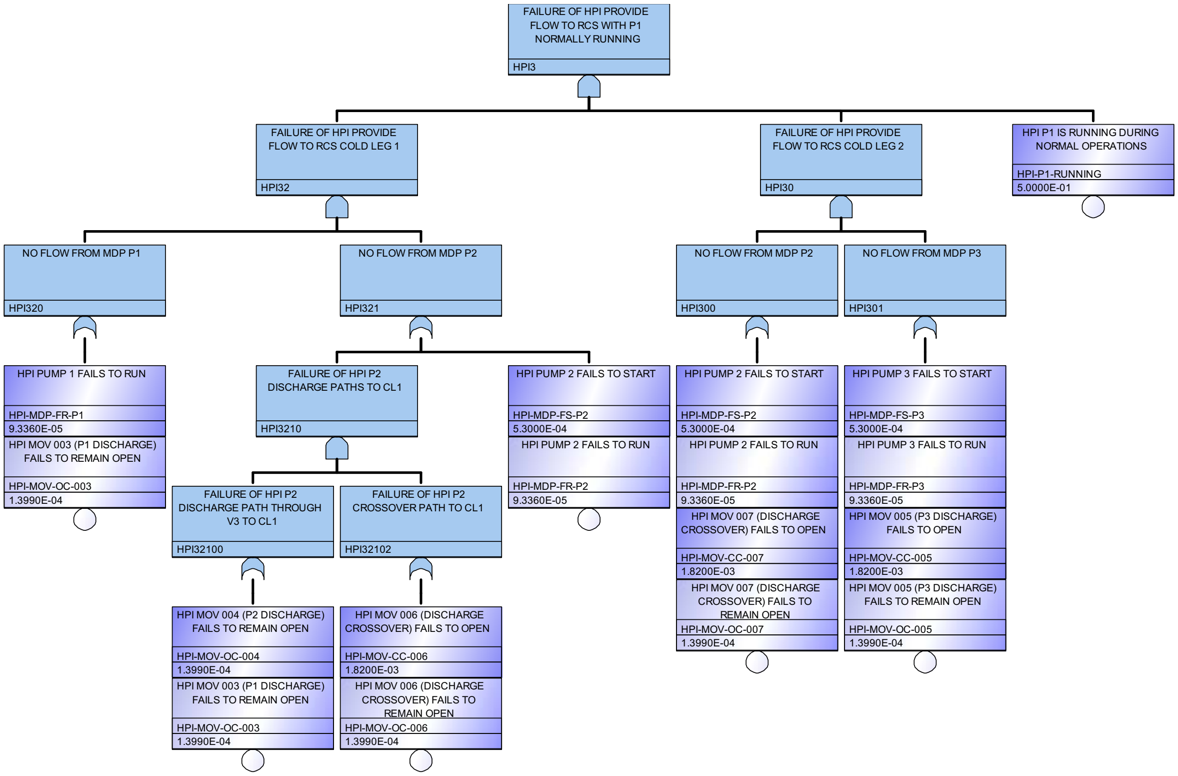

FAILURE OF HPI PROVIDE FLOW TO RCS WITH P1 NORMALLY RUNNING
HPI3
FAILURE OF HPI PROVIDE FLOW TO RCS COLD LEG 1
HPI32
FAILURE OF HPI PROVIDE FLOW TO RCS COLD LEG 2
HPI30
HPI P1 IS RUNNING DURING NORMAL OPERATIONS
HPI-P1-RUNNING
5.0000E-01
NO FLOW FROM MDP P1
HPI320
NO FLOW FROM MDP P2
HPI321
NO FLOW FROM MDP P2
HPI300
NO FLOW FROM MDP P3
HPI301
HPI PUMP 1 FAILS TO RUN
HPI-MDP-FR-P1
9.3360E-05
HPI MOV 003 (P1 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-003
1.3990E-04
FAILURE OF HPI P2 DISCHARGE PATHS TO CL1
HPI3210
HPI PUMP 2 FAILS TO START
HPI-MDP-FS-P2
5.3000E-04
HPI PUMP 2 FAILS TO RUN
HPI-MDP-FR-P2
9.3360E-05
FAILURE OF HPI P2 DISCHARGE PATH THROUGH V3 TO CL1
HPI32100
FAILURE OF HPI P2 CROSSOVER PATH TO CL1
HPI32102
HPI MOV 004 (P2 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-004
1.3990E-04
HPI MOV 003 (P1 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-003
1.3990E-04
HPI MOV 006 (DISCHARGE CROSSOVER) FAILS TO OPEN
HPI-MOV-CC-006
1.8200E-03
HPI MOV 006 (DISCHARGE CROSSOVER) FAILS TO REMAIN OPEN
HPI-MOV-OC-006
1.3990E-04
HPI PUMP 2 FAILS TO START
HPI-MDP-FS-P2
5.3000E-04
HPI PUMP 2 FAILS TO RUN
HPI-MDP-FR-P2
9.3360E-05
HPI MOV 007 (DISCHARGE CROSSOVER) FAILS TO OPEN
HPI-MOV-CC-007
1.8200E-03
HPI MOV 007 (DISCHARGE CROSSOVER) FAILS TO REMAIN OPEN
HPI-MOV-OC-007
1.3990E-04
HPI PUMP 3 FAILS TO START
HPI-MDP-FS-P3
5.3000E-04
HPI PUMP 3 FAILS TO RUN
HPI-MDP-FR-P3
9.3360E-05
HPI MOV 005 (P3 DISCHARGE) FAILS TO OPEN
HPI-MOV-CC-005
1.8200E-03
HPI MOV 005 (P3 DISCHARGE) FAILS TO REMAIN OPEN
HPI-MOV-OC-005
1.3990E-04

Figure 32. HPI3 gate with P1 normally running.

Table 17. List of the first 101 MCSs for the HPI system of Figure 16.

#	Prob/Freq	Total %	Cut Set
Total	**1.104E-5**	**100**	
1	7.200E-6	65.21	HPI-TNK-FC-RWST
2	3.312E-6	30.00	HPI-MOV-CC-001,HPI-MOV-CC-002
3	2.546E-7	2.31	HPI-MOV-CC-001,HPI-MOV-OC-002
4	2.546E-7	2.31	HPI-MOV-CC-002,HPI-MOV-OC-001
5	1.957E-8	0.18	HPI-MOV-OC-001,HPI-MOV-OC-002
6	6.748E-11	< 0.01	HPI-MDP-FS-P2,HPI-MOV-CC-003,HPI-MOV-OC-005,HPI-P3-RUNNING
7	6.748E-11	< 0.01	HPI-MDP-FS-P2,HPI-MOV-CC-005,HPI-MOV-OC-003,HPI-P1-RUNNING
8	4.503E-11	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P2,HPI-MOV-CC-003,HPI-P3-RUNNING
9	4.503E-11	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P2,HPI-MOV-CC-005,HPI-P1-RUNNING
10	1.965E-11	< 0.01	HPI-MDP-FS-P2,HPI-MDP-FS-P3,HPI-MOV-OC-003,HPI-P1-RUNNING
11	1.965E-11	< 0.01	HPI-MDP-FS-P1,HPI-MDP-FS-P2,HPI-MOV-OC-005,HPI-P3-RUNNING
12	1.311E-11	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-MDP-FS-P2,HPI-P3-RUNNING
13	1.311E-11	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P2,HPI-MDP-FS-P3,HPI-P1-RUNNING
14	1.189E-11	< 0.01	HPI-MDP-FR-P2,HPI-MOV-CC-003,HPI-MOV-OC-005,HPI-P3-RUNNING
15	1.189E-11	< 0.01	HPI-MDP-FR-P2,HPI-MOV-CC-005,HPI-MOV-OC-003,HPI-P1-RUNNING
16	7.931E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MOV-CC-005,HPI-P1-RUNNING
17	7.931E-12	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-MOV-CC-003,HPI-P3-RUNNING
18	5.187E-12	< 0.01	HPI-MDP-FS-P2,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P3-RUNNING
19	5.187E-12	< 0.01	HPI-MDP-FS-P2,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P1-RUNNING
20	3.461E-12	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FS-P1,HPI-MOV-OC-005,HPI-P3-RUNNING
21	3.461E-12	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FS-P3,HPI-MOV-OC-003,HPI-P1-RUNNING
22	3.461E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P2,HPI-MOV-OC-005,HPI-P3-RUNNING
23	3.461E-12	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P2,HPI-MOV-OC-003,HPI-P1-RUNNING
24	3.461E-12	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P2,HPI-MOV-OC-003,HPI-P3-RUNNING
25	3.461E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P2,HPI-MOV-OC-005,HPI-P1-RUNNING
26	2.310E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MDP-FS-P3,HPI-P1-RUNNING
27	2.310E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MDP-FS-P2,HPI-P3-RUNNING
28	2.310E-12	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-P3-RUNNING
29	2.310E-12	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MDP-FS-P2,HPI-P1-RUNNING
30	9.137E-13	< 0.01	HPI-MDP-FR-P2,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P1-RUNNING
31	9.137E-13	< 0.01	HPI-MDP-FR-P2,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P3-RUNNING
32	6.097E-13	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MOV-OC-005,HPI-P3-RUNNING
33	6.097E-13	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MOV-OC-005,HPI-P1-RUNNING
34	6.097E-13	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-MOV-OC-003,HPI-P1-RUNNING
35	6.097E-13	< 0.01	HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-MOV-OC-003,HPI-P3-RUNNING
36	4.217E-13	< 0.01	HPI-MOV-CC-005,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-P1-RUNNING
37	4.217E-13	< 0.01	HPI-MOV-CC-003,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-005,HPI-P3-RUNNING
38	4.068E-13	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-P3-RUNNING
39	4.068E-13	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P2,HPI-MDP-FR-P3,HPI-P1-RUNNING
40	2.814E-13	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-003,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-P3-RUNNING
41	1.228E-13	< 0.01	HPI-MDP-FS-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-P1-RUNNING
42	3.242E-14	< 0.01	HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P3-RUNNING

#	Prob/Freq	Total %	Cut Set
43	3.242E-14	< 0.01	HPI-MOV-CC-005,HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-007,HPI-P1-RUNNING
44	3.242E-14	< 0.01	HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-P1-RUNNING
45	3.242E-14	< 0.01	HPI-MOV-CC-005,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-P1-RUNNING
46	3.242E-14	< 0.01	HPI-MOV-CC-003,HPI-MOV-CC-007,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P3-RUNNING
47	3.242E-14	< 0.01	HPI-MOV-CC-003,HPI-MOV-CC-006,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P3-RUNNING
48	2.163E-14	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-003,HPI-MOV-CC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
49	2.163E-14	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-003,HPI-MOV-CC-007,HPI-MOV-OC-006,HPI-P3-RUNNING
50	2.163E-14	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-P1-RUNNING
51	2.163E-14	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-P3-RUNNING
52	9.441E-15	< 0.01	HPI-MDP-FS-P3,HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-007,HPI-P1-RUNNING
53	9.441E-15	< 0.01	HPI-MDP-FS-P3,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-P1-RUNNING
54	2.492E-15	< 0.01	HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P3-RUNNING
55	2.492E-15	< 0.01	HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P3-RUNNING
56	2.492E-15	< 0.01	HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P1-RUNNING
57	2.492E-15	< 0.01	HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P1-RUNNING
58	2.492E-15	< 0.01	HPI-MOV-CC-003,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
59	2.492E-15	< 0.01	HPI-MOV-CC-005,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
60	1.663E-15	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-007,HPI-P1-RUNNING
61	1.663E-15	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-P3-RUNNING
62	1.663E-15	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-OC-003,HPI-MOV-OC-007,HPI-P3-RUNNING
63	1.663E-15	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-007,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-P1-RUNNING
64	1.663E-15	< 0.01	HPI-MDP-FR-P3,HPI-MOV-CC-003,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
65	7.258E-16	< 0.01	HPI-MDP-FS-P3,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
66	1.916E-16	< 0.01	HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
67	1.916E-16	< 0.01	HPI-MOV-OC-003,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
68	1.278E-16	< 0.01	HPI-MDP-FR-P3,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
69	1.278E-16	< 0.01	HPI-MDP-FR-P3,HPI-MOV-OC-003,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
70	3.937E-17	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-005,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-P1-RUNNING
71	1.718E-17	< 0.01	HPI-MDP-FS-P1,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-P3-RUNNING

#	Prob/Freq	Total %	Cut Set
72	1.147E-17	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-P1-RUNNING
73	1.147E-17	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-P3-RUNNING
74	3.027E-18	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-P3-RUNNING
75	3.027E-18	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-005,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-007,HPI-P1-RUNNING
76	3.027E-18	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-P1-RUNNING
77	3.027E-18	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-005,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-P1-RUNNING
78	2.019E-18	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-P1-RUNNING
79	2.019E-18	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-P3-RUNNING
80	1.321E-18	< 0.01	HPI-MDP-FS-P1,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P3-RUNNING
81	1.321E-18	< 0.01	HPI-MDP-FS-P1,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P3-RUNNING
82	8.814E-19	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-P3-RUNNING
83	8.814E-19	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-007,HPI-P3-RUNNING
84	8.814E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P3,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-007,HPI-P1-RUNNING
85	8.814E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P3,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-P1-RUNNING
86	2.327E-19	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P1-RUNNING
87	2.327E-19	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P1-RUNNING
88	2.327E-19	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-P3-RUNNING
89	2.327E-19	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-007,HPI-P3-RUNNING
90	2.327E-19	< 0.01	HPI-MDP-FR-P1,HPI-MOV-CC-005,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
91	1.552E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-P3-RUNNING
92	1.552E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-007,HPI-P1-RUNNING
93	1.552E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-007,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-P1-RUNNING
94	1.552E-19	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-CC-006,HPI-MOV-OC-004,HPI-MOV-OC-007,HPI-P3-RUNNING
95	1.015E-19	< 0.01	HPI-MDP-FS-P1,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
96	6.775E-20	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FS-P3,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
97	6.775E-20	< 0.01	HPI-MDP-FR-P3,HPI-MDP-FS-P1,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
98	1.789E-20	< 0.01	HPI-MDP-FR-P1,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING
99	1.789E-20	< 0.01	HPI-MDP-FR-P1,HPI-MOV-OC-004,HPI-MOV-OC-005,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING
100	1.193E-20	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P1-RUNNING

#	Prob/Freq	Total %	Cut Set
101	1.193E-20	< 0.01	HPI-MDP-FR-P1,HPI-MDP-FR-P3,HPI-MOV-OC-004,HPI-MOV-OC-006,HPI-MOV-OC-007,HPI-P3-RUNNING

Table 18. Link between valves for the system shown in Figure 30 and basic events of the FT of Figure 30, Figure 31 and Figure 32.

Valve ID	Basic Event ID
V_1	HPI-MOV-CC-001
V_2	HPI-MOV-CC-001
V_3	HPI-MOV-CC-003
V_4	HPI-MOV-CC-004
V_5	HPI-MOV-CC-005
V_6	HPI-MOV-CC-006
V_7	HPI-MOV-CC-007

Table 19. Link between pumps for the system shown in Figure 30 and basic events of the FT of Figure 30, Figure 31 and Figure 32.

Pump ID	Basic Event ID
P_1	HPI-MDP-FS-P1
P_2	HPI-MDP-FS-P2
P_3	HPI-MDP-FS-P3

Appendix H

PWR FEEDWATER SYSTEM

The generic simplified feedwater system analyzed provides heated feedwater from the feedwater pumps to the steam generators. The feedwater system consists of the piping, valves, pumps, heat exchangers, controls, instrumentation, and the associated equipment that supply the steam generators with feedwater in a closed steam cycle using regenerative feedwater heating. Adequate flow from the condensate system to the feedwater pumps was assumed for the modeling process.

The feedwater system is of the closed type, with deaerating accomplished in the condenser. The water discharge from the feedwater pumps flows through one stage of high-pressure heating into the steam generators. There are two strings of high-pressure feedwater heaters. Each string is capable of supporting 50% of the plants rated power output. Each string is provided with motor-operated isolation valves with an operator override switch in the control room. A single bypass line, sized to handle the flow through one heater, is provided. The two strings of high-pressure feedwater heaters and the bypass line have a common discharge header.

Feedwater line isolation is provided by a hydraulically-operated gate valve and a check valve outside the containment. The hydraulically-operated gate valve has an operator override switch in the control room. Feedwater line isolation is also provided at the steam generator inlet in the case where the hydraulically-operated valve and check valve fail.

The system is composed of three feedwater pumps capable of supporting 50% of the plant's rated power output. Two of the pumps are turbine-driven and are used during normal operation. The third pump is used as a reserve or standby pump in situations where one of the turbine-driven pumps fails to run. The pumps have common suction and discharge headers.

Discharge from the pumps is automatically recirculated back to the condenser whenever flow to the high-pressure feedwater heaters falls below a predetermined point. Pump starting circuits are interlocked to prevent starting unless the recirculation control valves are open. Minimum feedwater pump suction pressure protection is assured through the heater drain pump control system and the automatic starting of a condensate pump and/or condensate booster pump.

Figure 33 shows the feedwater system beginning at the feedwater pumps up to the high-pressure heater discharge. A symbol identification table is provided at the end of this appendix. Feedwater pump discharge from pumps B and C are represented by blocks for simplification. The feedwater pump loops for B and C are designed the same as pump loop A. Pump A is the standby motor-driven pump. Symbols are described in Figure 38.

Feedwater flow from the high-pressure heater discharge to each steam generator is controlled by a feedwater regulator valve in each feedwater line. The regulator valve is controlled by steam generator level, steam flow, and feedwater flow. A signal from the feedwater control system also sets the speed of the turbine-driven feedwater pumps and the position of the motor-driven pump discharge control valve to maintain the main feedwater regulator valves within their control range. This allows the system to accommodate all operating conditions automatically and provides a control margin to accommodate load transients. During startup, a feedwater regulator bypass valve is controlled by steam generator liquid level and reactor power level. Each one of the four steam generators is capable of supporting 25% of the plant's rated power output.

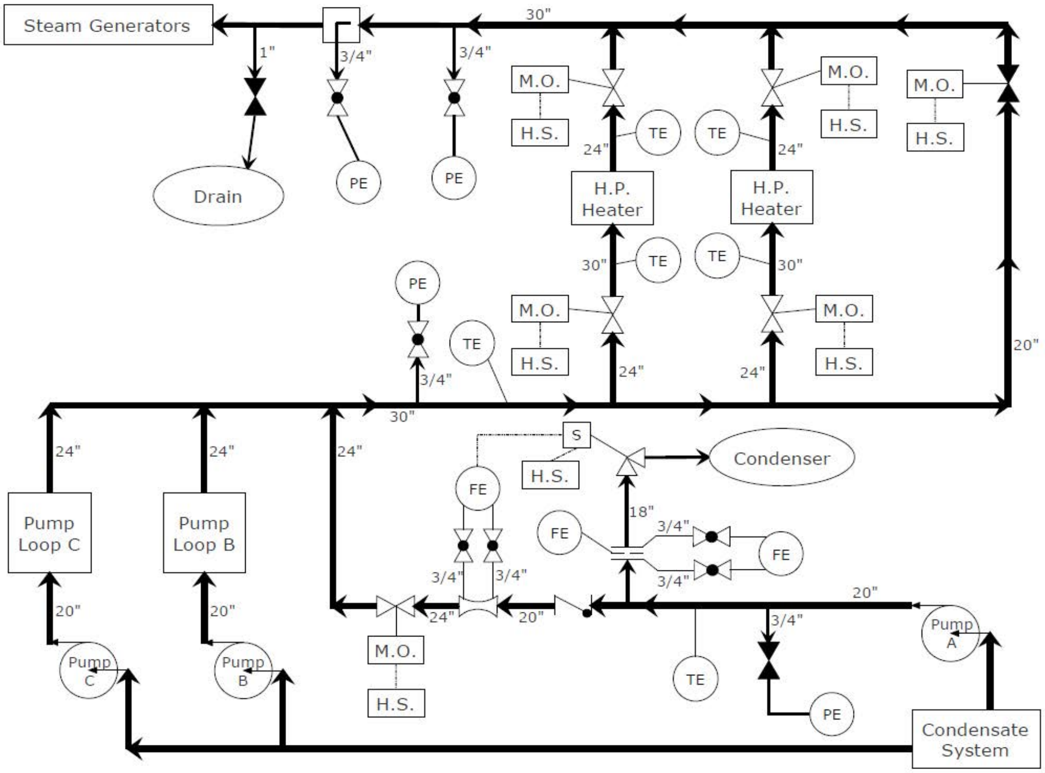


Figure 33. Feedwater system

Figure 34 shows the feedwater system beginning at the high-pressure heater discharge and up to the steam generator inlets. Steam generator loops B, C, and D are simplified in the figure because they are designed the same as loop A.

Heater drain flow into the condensate header is normally controlled as a fixed ratio of total feedwater flow, thereby maintaining Net Positive Suction Head (NPSH) above a preset minimum. Under the 10% load rejection situation or any other transient situation, this control will automatically maintain adequate feedwater pump suction pressure. The feedwater-flow/heater-drain-flow ratio signal is biased by heater drain tank level, thereby maintaining heater drain tank level within preset limits. Also, the automatic starting of the standby condensate pump will assure adequate flow to the feedwater pumps under all operating conditions. The heater drain system was omitted from modeling and was assumed to be operable during all feedwater system conditions.

Main feedwater isolation valves are affected by a safety injection signal. The isolation valves are hydraulically operated gate valves capable of closure within 5 seconds of receipt of an actuation signal. The valves are also operable from either the main control room or local panels. An additional function of the main feedwater isolation valves is to stop the flow of cold water to the preheater section of the steam generators in the event of a severe loss of load transient, and under startup and light load conditions when the preheater section is bypassed.

An additional 6-inch diameter feedwater nozzle has been installed on each steam generator above maximum water level, as an alternate point of admission for relatively cold feedwater under light load and emergency conditions. When the feedwater temperature is less than 275 °F, water is admitted to the upper nozzle, bypassing the preheater section of the steam generators.

The main feedwater isolation valve, in addition to providing containment isolation under post-accident conditions, performs a non-safety-related function in automatically closing in response to main feedwater temperature and flow conditions utilizing 2 out of 3 logic provided in the water hammer prevention features. This type of logic ensures that a single credible failure will neither prevent the features from operating nor cause a trip. The water hammer prevention features were omitted from the modeling process due to the features only being needed during light load and emergency conditions. In the next section, there is a discussion on how the water hammer prevention features are treated in the modeling process in the case of proceeding back to full power after a reactor trip has occurred.

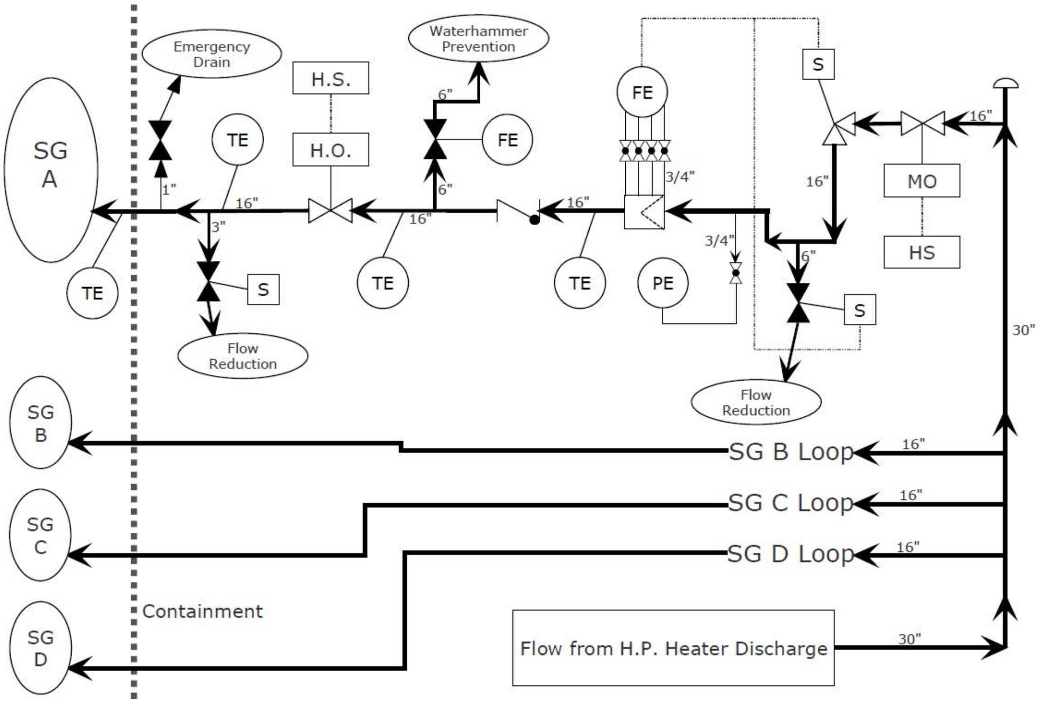


Figure 34. Feedwater system from high-pressure heater discharge to the steam generator inlets.

To maintain the feed lines to the upper steam generator nozzles in a continuously purged and warmed condition, a tempering flow of 95 gpm is maintained under normal operating conditions in each line. There is a cross-connection between each main feedwater line and its respective tempering line, and a feedwater preheater bypass valve in the cross-connecting line allows additional flow to augment tempering flow when the main feedwater isolation valve is closed under light load conditions. The main feedwater line ahead of the isolation valve is purged of cold water by means of flow through the preheater bypass valve.

A small bypass line around the main feedwater isolation valve provides for purging the main feedwater line between the isolation valve and steam generator. A controlled flow through the bypass line ensures that water hammer will not be caused by the purge flow.

When approximately 20% of the Nuclear Steam Supply System (NSSS) rated flow is attained and feedwater temperature is significantly higher than 275 °F and the main feedwater lines have been purged of cold water, the main feedwater isolation valves will open and the preheater bypass valves will close.

Under startup conditions, a feedwater regulator bypass control valve automatically controls the water level in its respective steam generator. At approximately 25% of NSSS rated flow, the main feedwater regulator control valves are placed in service and the bypass control valves are removed from service. Level in the steam generators is therefore automatically controlled at all times. Should the steam generator level decrease to the extent that the preheater section is not completely flooded, the isolation valve for that steam generator will close and flow will be diverted to the upper steam generator nozzle. Except for this provision, the steam generator level is entirely separate and automatically controlled and monitored and is not a part of the water hammer prevention features.

Various timers are included in the automatic controls of the water hammer prevention features to ensure that purge flow is maintained for the required length of time.

If flow to the steam generators remains continuous during a load transient and above a minimum flow rate, feedwater will not be diverted to the upper nozzle even if the temperature of the feedwater has dropped below 275 °F. Interruption or a reduction in flow below the minimum rate concurrent with a feedwater temperature less than 275 °F will cause the feedwater preheater sections of the steam generators to be bypassed.

Since there is always water flowing to the upper nozzle of the steam generator during normal light load operation, it is the required location for introducing cold fluid into the steam generator. Auxiliary feedwater and chemical feed are connected to the tempering feedwater lines rather than to the main feedwater lines. The chemical feed lines are used to add chemicals directly to the steam generators under light-load conditions prior to wet layup.

Continued operation of the system is possible by the use of the multi-stream arrangement and the provisions for removing from service and bypassing equipment and sections of the system if it is necessary to remove a component such as a feedwater heater, pump or control valve from service.

The steam generators are equipped with a three-element feedwater flow controller maintaining a programmed water level which is a function of turbine load.

Instrumentation and controls regulate pump recirculation flow rate for the condensate booster pumps and feedwater pumps. Measurements of the pump discharge pressure are provided for all pumps in the system. Sampling means are provided for monitoring the quality of water in the condensers, condensate pump discharge, and feedwater pump suction.

Steam-pressure measurements are provided at each feedwater heater. Instrumentation and controls are provided for regulating the heater drain flow rate to maintain the proper condensate level in each feedwater heater shell or heater drain tank. High-level alarm and automatic dump-to-condenser action on a high level are provided.

MFW Reliability Modeling

The modeling was based on estimating the lost generation due to failures in the feedwater system. Supporting systems such as instrument air, service water, electric power, etc. were not considered during the modeling process. Therefore, failures of exterior systems or components that fail the feedwater system are not included in the analysis. The reason for omitting supporting systems, is because the failure of these systems causes generation loss unrelated to the feedwater system. The supporting systems are subject to a modeling process outside of the generic model presented in this report.

Each basic event was modeled by component failure rate data and a mission time of 24 hours. Each resultant cut set was multiplied by 365 to convert the probability of failure per mission time (24 hours) to the probability of failure per year. Situations in which components had the possibility of repair before the top event occurred had the MTTR value included in the probability model.

The duration of the derate events in the modeling process was the sum of the MTTR(s) of the failed component(s) and the recovery time to get back up to full power. This duration was multiplied by the probability of failure per year to get Effective Full Power Hours (EFPH) of lost generation per year. The plant's electrical output capacity, 1000 MW, was multiplied by the EFPH values to get the lost generation in terms of MWh per year. The MWh per year value was then multiplied by $33.50 to get the lost generation in terms of dollars per year. The $33.50 is the value of a MWh according to NEI. The equation used to convert the results was based on the EPRI's GRA Plant Implementation Guide, given by the following equation. The equation multiplied by the probability of a derate per year gives the estimated lost generation of the system.

*Total Lost Generation (MWh) = Magnitude of derate * Duration of load reduction*

*= (1 - % of Full Power after load reduction) * Rated Capacity (MW) * (MTTR for the system, combinations of trains, or combinations of components leading to the load reduction + time to restore plant to power, in hours)*

The water hammer prevention features of the system are highly redundant and were deemed negligible in the modeling process for situations in which a reactor trip did not occur. The piping leading to the water hammer prevention path was included in the modeling. To account for proceeding back to 25% power after a plant trip, in which the water hammer prevention features are needed, a 34-hour start-up time was used. After 25% of power was reached it was assumed power would continuously increase by 1.65% power per hour. The 1.65% of reactor power per hour was the power increase rate used during the 50% and 25% derate situations as well.

In the 100% derate scenario it was assumed that no electrical output was being transmitted to the grid until maximum rated power. In the 50% derate scenario it was assumed that only 50% of the electrical output was being transmitted to the grid until maximum rated power. In the 25% derate scenario it was assumed that only 75% of the electrical output was being transmitted to the grid until maximum rated power. Note that in the economic models these assumptions are conservative (in that they would underestimate revenue).

Failure data for the feedwater pump failures were obtained from EPIX and the MTTRs for the pumps were obtained from pc-GAR. Failures of the two turbine-driven pumps were modeled in the 50% derate fault tree. The simultaneous failure of both turbine-driven pumps before the motor-driven pump can start-up and reach capacity was found to be too rare of an event and was omitted from modeling in the 100% derate fault tree. In the 50% derate fault tree, the duration of the derate due to the failure of either pump was taken as the time for the standby pump to start up and restore the plant to full power. The MTTR of the failed pump is the same time it takes for the standby pump to reach capacity; this eliminated the need to model the scenario in which the standby pump fails to start because the event in which the standby pump fails to start and the failed pump is not repaired in a typical amount of time was too rare of an event.

Failure data for the different types of valves were obtained from EPIX and the MTTRs for the valves were obtained from pc-GAR. In the pc-GAR database, there are only two categories of valves in feedwater systems. The MTTR of both valve categories was the same so every valve was assigned the same MTTR. The failures of valves that cause a plant trip were modeled in the 100% derate fault tree. The failures of valves that are isolable in the feedwater pump loops and the high-pressure heater loops were modeled in the 50% derate fault tree. Simultaneous failures of the valves in the pump and heater loops were found to be too rare for inclusion in the 100% derate fault tree. The failures of valves that are isolable in the steam generator feedwater loops were modeled in the 25% derate fault tree. Simultaneous failures of the valves in the steam generator loops were found to be too rare for inclusion in the 100% or 50% derate fault trees.

According to the Summary of SPAR Component Unreliability Data and Results spreadsheet, there were no reports of instrumentation and control failures. Therefore, instrumentation and control failures were omitted from modeling. The same result was found for orifices.

Feedwater piping lengths vary from plant to plant so order of magnitude estimates were made for the generic plant. The longest pipes in the system were given a length of 1000 feet. The shortest pipes in the system were given a length of 10 feet. The pipes that were determined to have lengths in between the longest and shortest lengths were given a length of 100 feet. Feedwater piping was modeled like the feedwater valves. Failures of pipes that resulted in a plant trip were modeled in the 100% derate fault tree. Failures of pipes that are isolable in the feedwater pump loops and high-pressure heater loops were modeled in the 50% derate fault tree. Simultaneous failures of isolable pipes were found to be too rare for inclusion in the 100% derate fault tree. Failures of pipes that are isolable in the steam generator feedwater loops were modeled in the 25% derate fault tree. Simultaneous failures of the pipes in the steam generator loops were found to be too rare for inclusion in the 100% or 50% derate fault tree. The failure data for the piping was given in terms of failure frequency per length in feet.

The operator failure with the override switch control failure rate data was obtained from pc-GAR from the "Operator Error" category. It was modeled with an "AND" gate everywhere that failure of the operation of a valve occurred that an operator would have the ability to correct.

Failure data for the high-pressure heaters were obtained from EPIX in the section on heat exchangers. The MTTRs were obtained from pc-GAR from the categories of "High Pressure Heater Tube Leaks" and "Other High Pressure Heater Problems." The failure of the high-pressure heaters was modeled in both the 100% and 50% derate fault trees. The on-line repair was assumed due to the isolation valves available to each high-pressure heater. The event in which the isolation valves fail to operate or rupture at the same time in either high-pressure heater was found to be too rare of an event for modeling. The MTTR was included in the probability model to account for time to repair one high-pressure heater before the other fails.

Maintenance data were not obtained for modeling of this generic PWR feedwater system. Test and maintenance activities vary from plant to plant. The omission of test and maintenance activities is important to note because the activities can contribute a large amount to lost generation.

Common mode failures were not found while modeling the system. If further modeling were to occur including supporting systems and components, common mode failures would need to be readdressed and included in the fault tree construction. Instrument air is a typical example of a supporting system that would lead to a common mode failure.

Two components were subject to special failure rate and MTTR considerations. The pitot tube and end closure weld cap were not found in either the pc-GAR or EPIX database. Therefore, WASH-1400 was used for failure rates of these SSCs. The end closure weld cap was assigned the failure rate of "closures" from WASH-1400. The pitot tube was assigned the failure rate of "flow meters" from WASH-1400. Since both of these components were connected to piping and were assumed to contribute to a negligible amount of generation loss, the MTTR for piping and supports was used.

The estimation of component failure frequency and MTTR from pc-GAR data follows the same methodology found within the Cooper Nuclear Station GRA report. An Annual Unit Performance and Individual Cause Code report can be generated by pc-GAR allowing for the total number of service hours, the number of failures, and outage time to be obtained. To estimated component failure frequency from the Individual Cause Code report is used to count the number of forced outages (U1, U2, U3) and forced derates (D1, D2, D3). The Annual Unit Performance report yields the mean "Unit Service Hours" and when multiplied by "Unit Years" gives the total service hours. The total number of forced failure events divided by the total service hours yields the component failure frequency. The MTTR values were estimated by obtaining the "Hours Loss/Occ" from the Individual Cause Code Report. Multiplying each "Hours Loss/Occ" value with the respectively forced outage or derate events and summing them together then dividing the sum by the sum of the forced outage events yields the forced derate duration for each category. The average forced derate duration is the MTTR.

The following tables provide the FMEAs conducted for each critical component identified in the study along with the failure data, mission time and MTTRs assigned to each component from pc-GAR, EPIX, and WASH-1400.

Table 20. Steam generator FMEA.

Steam Generator Loops A, B, C, and D						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data / hr**	**Mission Time**	**MTTR**
1FW76A(A,B,C,D) => 1-inch pipe leading to emergency drain (10ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-09	24 Hours	7.6 Hours
1FW029(A,B,C,D) => Manual valve connected to emergency drain.	Valve failure	Steam generator loop failure	Valve leakage or spurious transfer causes inadvertent drainage in steam generator feedwater loop.	2.42E-07	24 Hours	15 Hours
1FW03D(A,B,C,D) => 16-inch pipe on steam generator feedwater line (100ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-08	24 Hours	7.6 Hours
1FW82A(A,B,C,D) => 3-inch pipe for flow reduction to the steam generator (10ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-09	24 Hours	7.6 Hours
1FW042(A,B,C,D) => Solenoid valve connected to flow reduction path.	Valve failure	Steam generator loop failure	Valve failure to control, spurious transfer, or leakage causes inadvertent drainage or inadequate steam generator feedwater supply.	6.45E-07	24 Hours	15 Hours
1FW009(A,B,C,D) => Hydraulically operated valve on steam generator feedwater line.	Valve leaks	Steam generator loop failure	Valve leakage causes inadvertent drainage in steam generator feedwater loop.	1.93E-07	24 Hours	15 Hours
	Valve fails to operate - Hydraulics	Steam generator loop failure	Valve spurious transfer or failure to control causes inadequate steam generator feedwater supply, there is operator override action.	6.45E-07	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW86A(A,B,C,D) => 16-inch pipe on steam generator feedwater line (100ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-08	24 Hours	7.6 Hours
1FW041(A,B,C,D) => Solenoid valve connected to water hammer prevention path.	Valve failure	Steam generator loop failure	Valve failure to control, spurious transfer, or leakage causes inadvertent drainage or inadequate steam generator feedwater supply.	6.45E-07	24 Hours	15 Hours
1FW81A(A,B,C,D) => 6-inch pipe leading to water hammer prevention path (10ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-09	24 Hours	7.6 Hours
1FW008(A,B,C,D) => Check valve on steam generator feedwater line.	Valve failure	Steam generator loop failure	Valve failure to remain open or leakage causes inadequate steam generator feedwater supply.	2.29E-07	24 Hours	15 Hours

Steam Generator Loops A, B, C, and D						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data / hr**	**Mission Time**	**MTTR**
Venturi => Mechanical failure, see description.	Pipe rupture	Steam generator loop failure	Each venturi tube has 4 3/4-inch pipes (10ft) and 4 manual valves. Leakage cause steam generator to be unavailable and failure will cause instrumentation to be unavailable.	2.78E-09	24 Hours	7.6 Hours
	Valve leakage and mechanical			2.42E-07	24 Hours	15 hours
	Venturi tube rupture			1.00E-08	24 Hours	7.6 Hours
1FW11(A,B,C,D)A => 3/4-inch pipe leading to pressure instrument (10ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-09	24 Hours	7.6 Hours
1FW022(A,B,C,D) => Manual valve connected to pressure instrument flow.	Valve failure	Steam generator loop failure	Valve leakage causes inadvertent drainage.	1.91E-07	24 Hours	15 Hours
1FW92(A,B,C,D) => 6-inch pipe for flow reduction (10ft).	Pipe rupture	Steam generator loop failure	Pipe rupture causes leak in steam generator feedwater loop.	2.78E-09	24 Hours	7.6 Hours
1FW5(1,2,3,4)0 => Solenoid operated angle valve on steam generator feedwater line.	Valve failure	Steam generator loop failure	Valve failure to control, spurious transfer, or leakage causes inadvertent drainage or inadequate steam generator feedwater supply.	6.45E-07	24 Hours	15 Hours
1FW03C(A,B,C,D) => 16-inch pipe connected to main feedwater line (100ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW006(A,B,C,D) => Motor operated isolation/regulation valve at the entrance of steam generator loop.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	Steam generator loop failure	Steam generator is unavailable if motor operated valve spuriously transfers or fails to control flow, there is operator override action.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours

Table 21. Main feedwater line FMEA.

Main Feedwater Line						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
End closure weld cap.	Rupture	Feedwater system failure	Rupture of welded cap causes leak in main feedwater line.	3.00E-07	24 Hours	7.6 Hours
1FW03B => 30-inch pipe delivering main feedwater (1000ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-07	24 Hours	7.6 Hours
1FW75A => 1-inch pipe connected to drainage (10ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-09	24 Hours	7.6 Hours
1FW028 => Manual valve connected to drainage path.	Valve failure	Feedwater system failure	Valve leakage or spurious transfer causes leak in main feedwater line.	2.42E-07	24 Hours	15 Hours
Pitot tube	Rupture	Feedwater system failure	Rupture of pitot tube causes leak in main feedwater line.	1.00E-08	24 Hours	7.6 Hours
1FW94 => 3/4-inch pipe from pitot tube to pressure instrument (10ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-09	24 hours	7.6 Hours
1PS023 => Manual valve for path to pressure instrument.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent drainage from main feedwater line.	1.91E-07	24 Hours	15 Hours
1FW10AA => 3/4-inch pipe for flow to pressure instrument (10ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-09	24 Hours	7.6 Hours
1FW021 => Manual valve for path to pressure instrument.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent drainage from main feedwater line.	1.91E-07	24 Hours	15 Hours

Table 22. High-pressure heater and bypass FMEA.

High Pressure Feedwater Heater Paths and Bypass						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW004A => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	H.P. heater loop failure	Heater is unavailable if motor operated valve spuriously transfers or fails to control flow, there is operator override action.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW02AA => 24-inch pipe from H.P. heater A (100ft).	Pipe rupture	H.P. heater loop failure	Rupture causes leak in heater loop but is isolable from main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW01AA => H.P. feedwater heater A.	Tube leaks	H.P. heater loop failure	H.P. heater tubes leak or other problems occur rendering the feedwater heater unavailable.	7.01E-07	24 Hours	7.5 Hours
	Other problems			1.62E-06	24 Hours	13 Hours
1FW01DA => 30-inch pipe delivering flow to H.P. heater A (100ft).	Pipe rupture	H.P. heater loop failure	Rupture causes leak in heater loop but is isolable from main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW003A => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	H.P. heater loop failure	Heater is unavailable if motor operated valve spuriously transfers or fails to control flow, there is operator override action.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW01CA => 24-inch pipe delivering flow to heater loop A (100ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW004B => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	H.P. heater loop failure	Heater is unavailable if motor operated valve spuriously transfers or fails to control flow, there is operator override action.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW02AB => 24-inch pipe from H.P. heater B (100ft).	Pipe rupture	H.P. heater loop failure	Rupture causes leak in heater loop but is isolable from main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW01AB => H.P. feedwater heater B.	Tube leaks	H.P. heater loop failure	H.P. heater tubes leak or other problems occur rendering the feedwater heater unavailable.	7.01E-07	24 Hours	7.5 Hours
	Other problems			1.62E-06	24 Hours	13 Hours

High Pressure Feedwater Heater Paths and Bypass

Component	Failure Mode	Effect	Description	Failure Data	Mission Time	MTTR
1FW01DB => 30-inch pipe delivering flow to H.P. heater B (100ft).	Pipe rupture	H.P. heater loop failure	Rupture causes leak in heater loop but is isolable from main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW003B => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	H.P. heater loop failure	Heater is unavailable if motor operated valve spuriously transfers or fails to control flow, there is operator override action.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW01CB => 24-inch pipe delivering flow to heater loop B (100ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-08	24 Hours	7.6 Hours
1FW03A => 20-inch pipe for bypass flow (1000ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-07	24 Hours	7.6 Hours
1FW005 => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Rupture causes leak in main feedwater line. Failure to regulate flow causes feedwater temperature issues in feedwater system.	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor			9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW16A => 3/4-inch pipe delivering flow to pressure instrument (10ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-09	24 Hours	7.6 Hours
1FW020 => Manual valve delivering flow to pressure transmitter	Valve leakage	Feedwater system failure	Valve leakage causes inadvertent flow from main feedwater line.	1.91E-07	24 Hours	15 Hours
1FW01B => 30-inch pipe delivering flow from pumps to heaters and bypass (1000ft).	Pipe rupture	Feedwater system failure	Pipe rupture causes leak in main feedwater line.	2.78E-07	24 Hours	7.6 Hours

Table 23. Feedwater pump A FMEA.

Feedwater Pump A						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW002A => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Leakage causes inadvertent flow from main feedwater line	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	Fails feedwater pump A loop	Failure to regulate flow inadequately supplies feedwater and the loop must be isolated.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW01AA => 24-inch pipe for flow to regulation valve (100ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW09AA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW09DA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW019A => Open valve for path from venturi tube.	Valve failure	Fails feedwater pump A loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours
1FW019D => Open valve for path from venturi tube.	Valve failure	Fails feedwater pump A loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours
1FW001A => Check valve on feedwater loop line.	Valve failure	Fails feedwater pump A loop	Valve failure to remain open or leakage causes inadequate flow from pump.	2.29E-07	24 Hours	15 Hours
1FW05AA => 18-inch pipe for flow back to condenser (100ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FEFW064 => Flow orifice on path back to condenser.	Rupture	Fails feedwater pump A loop	Orifice allows for monitoring flow back to the condenser.	1.00E-08	24 Hours	7.6 Hours
1FW73AA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW73DA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW541A => Open manual valve on path to flow instrument.	Valve failure	Fails feedwater pump A loop	Valve leakage causes loss of flow from pump loop.	1.91E-07	24 Hours	15 Hours
1FW541D => Open manual valve on path to flow instrument.	Valve failure	Fails feedwater pump A loop	Valve leakage causes loss of flow from pump loop.	1.91E-07	24 Hours	15 Hours
1FW012A => Closed angle valve on path back to condenser.	Valve leakage	Fails feedwater pump A loop	Valve rupture causes leak in pump loop. Failure of associated control instrumentation and operator override restricts flow back to the condenser.	1.72E-07	24 Hours	15 Hours
	Failure of solenoid control			4.73E-07	24 Hours	13 Hours
	Failure of operator override switch			2.80E-05	24 Hours	0 Hours
1FW04AA => 3/4-inch pipe for flow to alternate pressure instrument (10ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours

Feedwater Pump A						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW011A => Closed manual valve to alternate pressure instrument.	Valve leakage	Fails feedwater pump A loop	Valve rupture causes leak in pump loop.	1.91E-07	24 Hours	15 Hours
1FW78AA => 20-inch pipe from feedwater pump A (100ft).	Pipe rupture	Fails feedwater pump A loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW01PA => Motor driven steam generator feedwater pump A.	Feedwater pump failure	Fails feedwater pump A loop	Feedwater pump failure.	3.79E-06	24 Hours	32 Hours

Table 24. Feedwater pump B FMEA.

Feedwater Pump Loop B						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW002B => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Leakage causes inadvertent flow from main feedwater line	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	Fails feedwater pump B loop	Failure to regulate flow inadequately supplies feedwater and the loop must be isolated.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW01AB => 24-inch pipe for flow to regulation valve (100ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW09BA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW09EA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW019B => Manual valve for path from venturi tube.	Valve failure	Fails feedwater pump B loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours
1FW019E => Manual valve for path from venturi tube.	Valve failure	Fails feedwater pump B loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours
1FW001B => Check valve on feedwater loop line.	Valve failure	Fails feedwater pump B loop	Valve failure to remain open or leakage causes inadequate flow from pump.	2.29E-07	24 Hours	15 Hours
1FW05AB => 18-inch pipe for flow back to condenser (100ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FEFW065 => Flow orifice on path back to condenser.	Rupture	Fails feedwater pump B loop	Orifice allows for monitoring flow back to the condenser.	1.00E-08	24 Hours	7.6 Hours
1FW73CA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW73FA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW541F => Open manual valve on path to flow instrument.	Valve failure	Fails feedwater pump B loop	Valve leakage causes loss of flow from pump loop.	1.91E-07	24 Hours	15 Hours
1FW541C => Open manual valve	Valve failure	Fails feedwater	Valve leakage causes	1.91E-07	24	15 Hours

Feedwater Pump Loop B						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
on path to flow instrument.		pump B loop	loss of flow from pump loop.		Hours	
1FW012B => Closed angle valve on path back to condenser.	Valve leakage	Fails feedwater pump B loop	Valve rupture causes leak in pump loop. Failure of associated control instrumentation and operator override restricts flow back to the condenser.	1.72E-07	24 Hours	15 Hours
	Failure of solenoid control			4.73E-07	24 Hours	13 Hours
	Failure of operator override switch			2.80E-05	24 Hours	0 Hours
1FW04BA => 3/4-inch pipe for flow to alternate pressure instrument (10ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW011B => Closed manual valve to alternate pressure instrument.	Valve leakage	Fails feedwater pump B loop	Valve rupture causes leak in pump loop.	1.91E-07	24 Hours	15 Hours
1FW78AB => 20-inch pipe from feedwater pump B (100ft).	Pipe rupture	Fails feedwater pump B loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW01PB => Turbine driven steam generator feedwater pump B.	Feedwater pump failure	Fails feedwater pump B loop	Feedwater pump failure.	1.09E-05	24 Hours	32 Hours
			Other feedwater pump problems.	5.38E-07	24 Hours	19 Hours

Table 25. Feedwater pump C FMEA.

Feedwater Pump C						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW002C => Motor operated regulating valve.	Valve leakage	Feedwater system failure	Leakage causes inadvertent flow from main feedwater line	1.06E-07	24 Hours	15 Hours
	Valve fails to operate - Motor	Fails feedwater pump C loop	Failure to regulate flow inadequately supplies feedwater and the loop must be isolated.	9.14E-08	24 Hours	15 Hours
	Valve fails to operate - Operator			2.80E-05	24 Hours	0 Hours
1FW01AC => 24-inch pipe for flow to regulation valve (100ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW09CA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW09FA => 3/4-inch pipe from venturi tube to instrument (10ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW019C => Manual valve for path from venturi tube.	Valve failure	Fails feedwater pump C loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours
1FW019F => Manual valve for path from venturi tube.	Valve failure	Fails feedwater pump C loop	Valve leakage causes loss of flow from pump loop and spurious transfer inhibits the instrumentation functionality.	2.42E-07	24 Hours	15 Hours

Feedwater Pump C						
Component	**Failure Mode**	**Effect**	**Description**	**Failure Data**	**Mission Time**	**MTTR**
1FW001C => Check valve on feedwater loop line.	Valve failure	Fails feedwater pump C loop	Valve failure to remain open or leakage causes inadequate flow from pump.	2.29E-07	24 Hours	15 Hours
1FW05AC => 18-inch pipe for flow back to condenser (100ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FEFW066 => Flow orifice on path back to condenser.	Rupture	Fails feedwater pump C loop	Orifice allows for monitoring flow back to the condenser.	1.00E-08	24 Hours	7.6 Hours
1FW73BA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW73EA => 3/4-inch pipe to flow instrument (10ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW541B => Open manual valve on path to flow instrument.	Valve failure	Fails feedwater pump C loop	Valve leakage causes loss of flow from pump loop.	1.91E-07	24 Hours	15 Hours
1FW541E => Open manual valve on path to flow instrument.	Valve failure	Fails feedwater pump C loop	Valve leakage causes loss of flow from pump loop.	1.91E-07	24 Hours	15 Hours
1FW012C => Closed angle valve on path back to condenser.	Valve leakage	Fails feedwater pump C loop	Valve rupture causes leak in pump loop. Failure of associated control instrumentation and operator override restricts flow back to the condenser.	1.72E-07	24 Hours	15 Hours
	Failure of solenoid control			4.73E-07	24 Hours	13 Hours
	Failure of operator override switch			2.80E-05	24 Hours	0 Hours
1FW04CA => 3/4-inch pipe for flow to alternate pressure instrument (10ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-09	24 Hours	7.6 Hours
1FW011C => Closed manual valve to alternate pressure instrument.	Valve leakage	Fails feedwater pump C loop	Valve rupture causes leak in pump loop.	1.91E-07	24 Hours	15 Hours
1FW78AC => 20-inch pipe from feedwater pump C (100ft).	Pipe rupture	Fails feedwater pump C loop	Pipe rupture causes leak in pump loop.	2.78E-08	24 Hours	7.6 Hours
1FW01PC => Turbine driven steam generator feedwater pump C.	Feedwater pump failure	Fails feedwater pump C loop	Feedwater pump failure.	1.09E-05	24 Hours	32 Hours
			Other feedwater pump problems.	5.38E-07	24 Hours	19 Hours

Figure 35, Figure 36, and Figure 37 show the FT structure of each derate scenario.

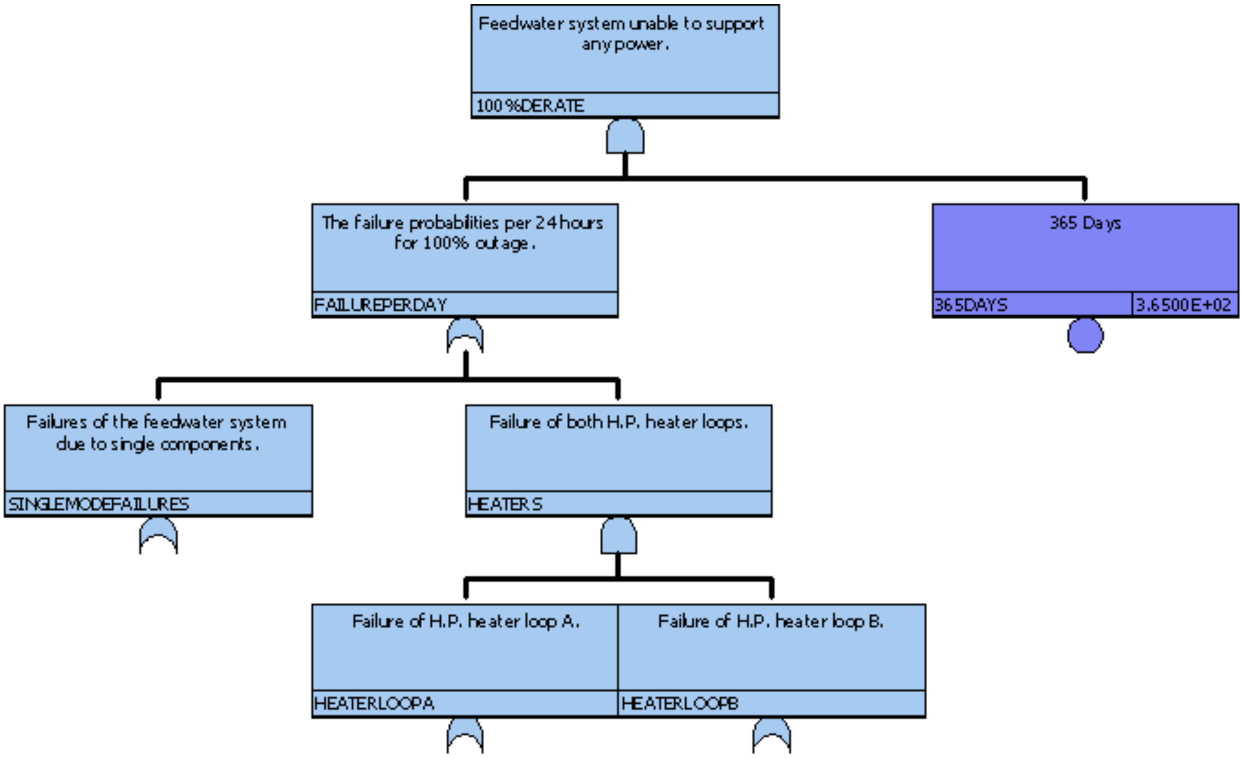

Feedwater system unable to support any power.
100%DERATE
The failure probabilities per 24 hours for 100% outage.
FAILUREPERDAY
365 Days
365DAYS
3.6500E+02
Failures of the feedwater system due to single components.
SINGLEMODEFAILURES
Failure of both H.P. heater loops.
HEATERS
Failure of H.P. heater loop A.
HEATERLOOPA
Failure of H.P. heater loop B.
HEATERLOOPB

Figure 35. Feedwater system 100% derate fault tree.

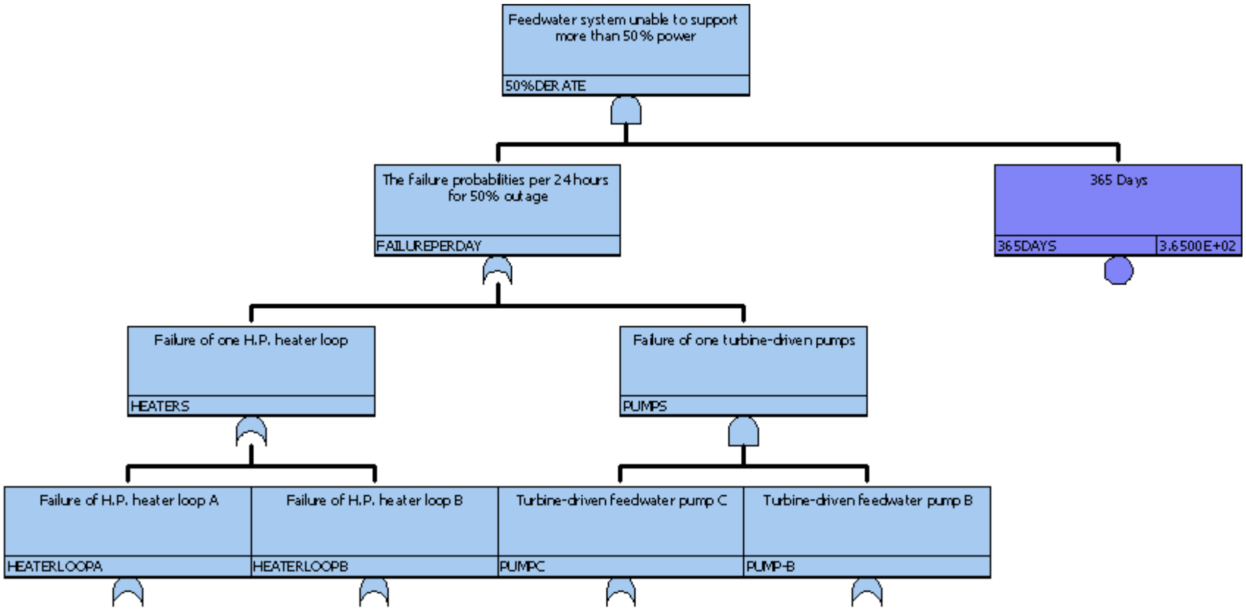

Feedwater system unable to support more than 50% power
50%DERATE
The failure probabilities per 24 hours for 50% outage
FAILUREPERDAY
365 Days
365DAYS
3.6500E+02
Failure of one H.P. heater loop
HEATERS
Failure of one turbine-driven pumps
PUMPS
Failure of H.P. heater loop A
HEATERLOOPA
Failure of H.P. heater loop B
HEATERLOOPB
Turbine-driven feedwater pump C
PUMPC
Turbine-driven feedwater pump B
PUMP-B

Figure 36. Feedwater system 50% derate fault tree.

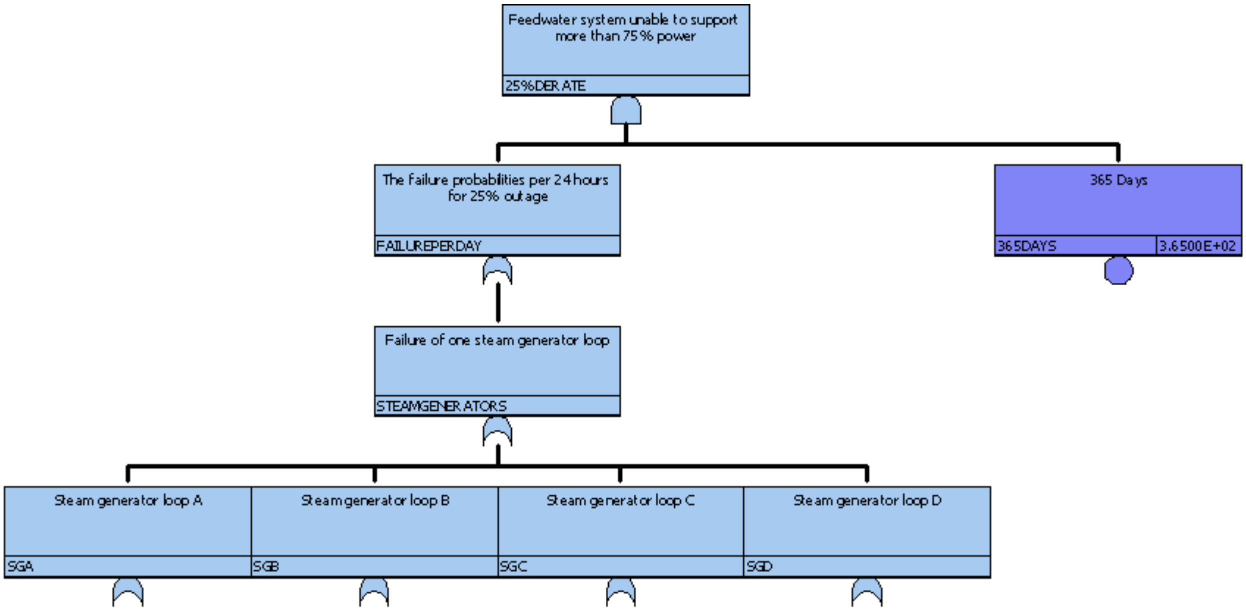


Figure 37. Feedwater system 20% derate fault tree.

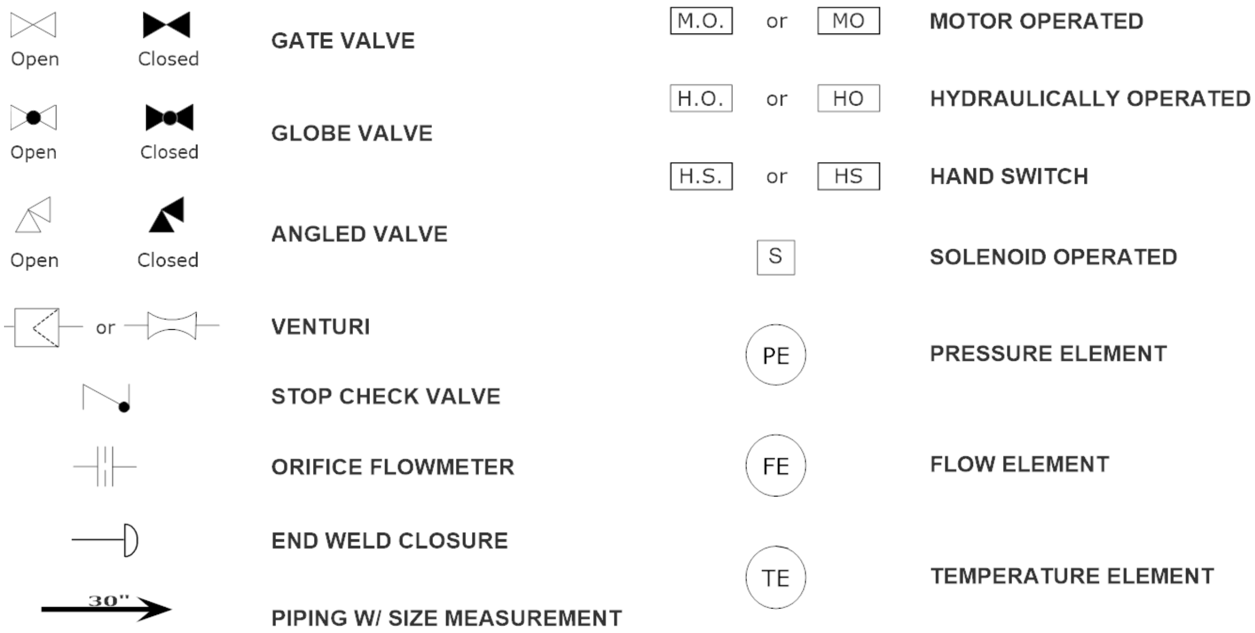


Figure 38. Feedwater system drawing symbol legend.

Appendix I

MFW GRA RESULTS

The results obtained from the SAPHIRE [158] models concluded that there are four main contributors to lost generation in the feedwater system: pipes, valves, pumps, and heaters. Table 8 shows the contributions to lost generation per year. The estimated lost generation from this model for the feedwater system represents approximately 0.1% of total plant generation if a 100% capacity for the year would be achieved.

Figure 39 displays the lost generation due to the categories of components to capture the relative generation loss contributions. As would be expected based on general industry operating experience, the estimated lost generation is dominated by failures of the active components (pumps and valves) as opposed to the passive components (pipes and heaters) in the system.

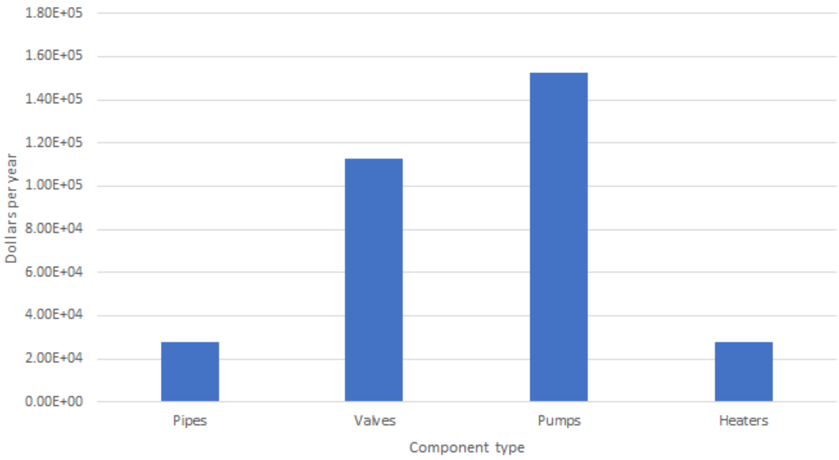


Figure 39. Lost generation contributions from the top categories of components.

The 65 valves evaluated in the study contributed to a large amount of the estimated generation loss. Five different types of valves were considered in the model. The average cost of lost generation per valve is shown in Figure 40.

Figure 40 shows that each motor valve contributes more to lost generation than any other valve type. Each motor-operated valve is estimated to cost around 3,000 dollars per year due to unavailability from failure. The values used to obtain Table 8 and Figure 39 and Figure 40 were composed of the sum of lost generation from all three derate scenarios. The 50% derate scenario contributed more to generation loss than the 25% and 100% scenarios. Figure 41 shows the lost generation contributions from the different derate scenarios.

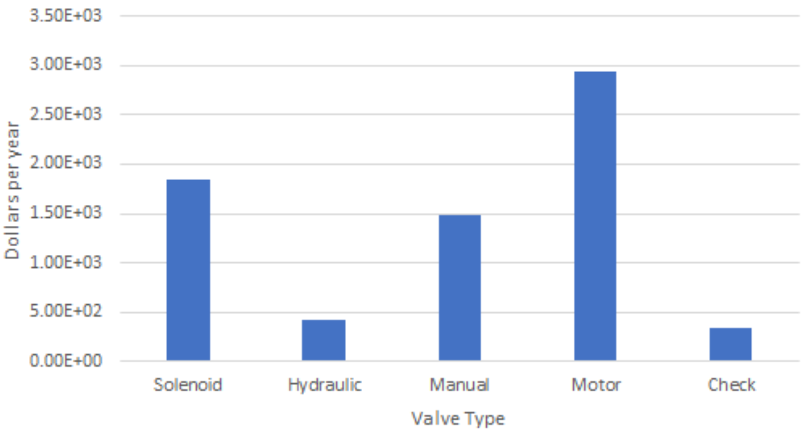


Figure 40. Lost generation per valve.

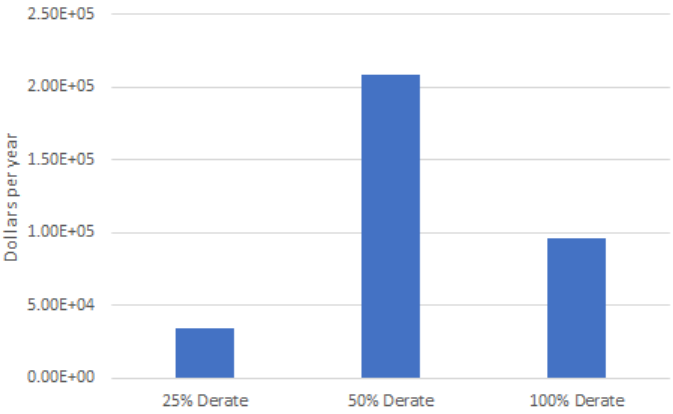


Figure 41. Lost generation contributions from the different derate scenarios.

The top cut sets of the 50% derate scenario are the failure of either running feedwater pump and failure of either high-pressure heater. The high-pressure heaters were assumed to be repairable online which led to a relatively small lost generation contribution when compared to other industry GRA results of feedwater systems. To identify how this assumption affected the results, the 100% derate fault tree was modified on the basis that online repair of either high-pressure heater was not possible. Figure 42 shows the difference in lost generation through changing the repair capability of the high-pressure heaters.

The value of lost generation caused by the high-pressure heater unavailability increases by more than a factor of five. Modification of this repair assumption increases the lost generation due to the feedwater system by more than 100,000 dollars per year. The value increase would be more substantial if test, maintenance, and repair costs were included in the evaluation. Figure 43 displays the contributions from the different derate scenarios when the online repair capability of the high-pressure heaters is removed.

The results above show that the high-pressure heaters do not contribute as much to risk as the industry would suggest when repairable at derated power levels. The ability to repair a high-pressure heater while at derated power level has positive impact on economic risk.

RAW and FV importance measures were obtained for each basic event in the fault trees. The values were plotted on a four-quadrant plot to view the relative positions of each basic event. Figure 44 displays the four-quadrant plot composed of 17 basic event types.

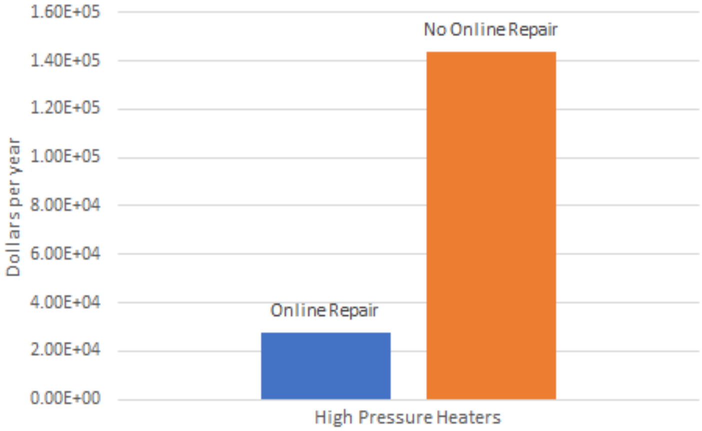


Figure 42. Lost generation comparison related to heater repair capability.

The plot is on a log-log scale. Plotting the two importance measures for each basic event category on a four-quadrant plot provides valuable insights for managing generation risk activities. The thresholds in the plot should be viewed as large bands of grey. Threshold lines in four-quadrant plots are used to weigh out cost-benefit risk-mitigating decisions for proposed component modifications. The relationships of the components with one another is useful for analysis. Consideration of the figure yields conclusions that correspond to other industry GRA models of feedwater systems. Figure 45 and Figure 46 display the feedwater system four-quadrant plots from Cooper Nuclear Station GRA and GRA Plant Implementation Guide, respectively.

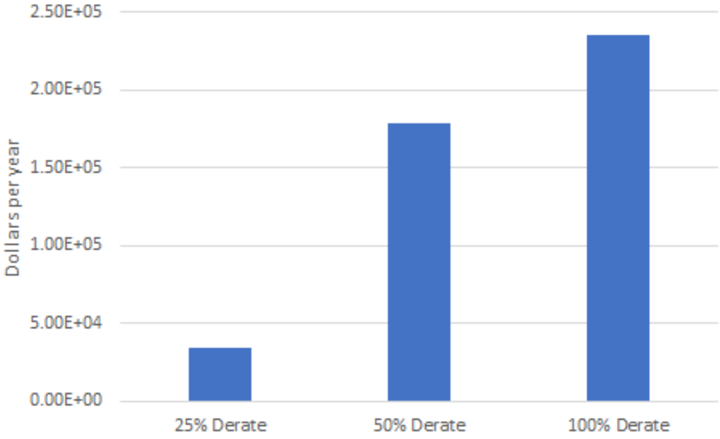


Figure 43. Lost generation contribution when heaters are not repairable online.

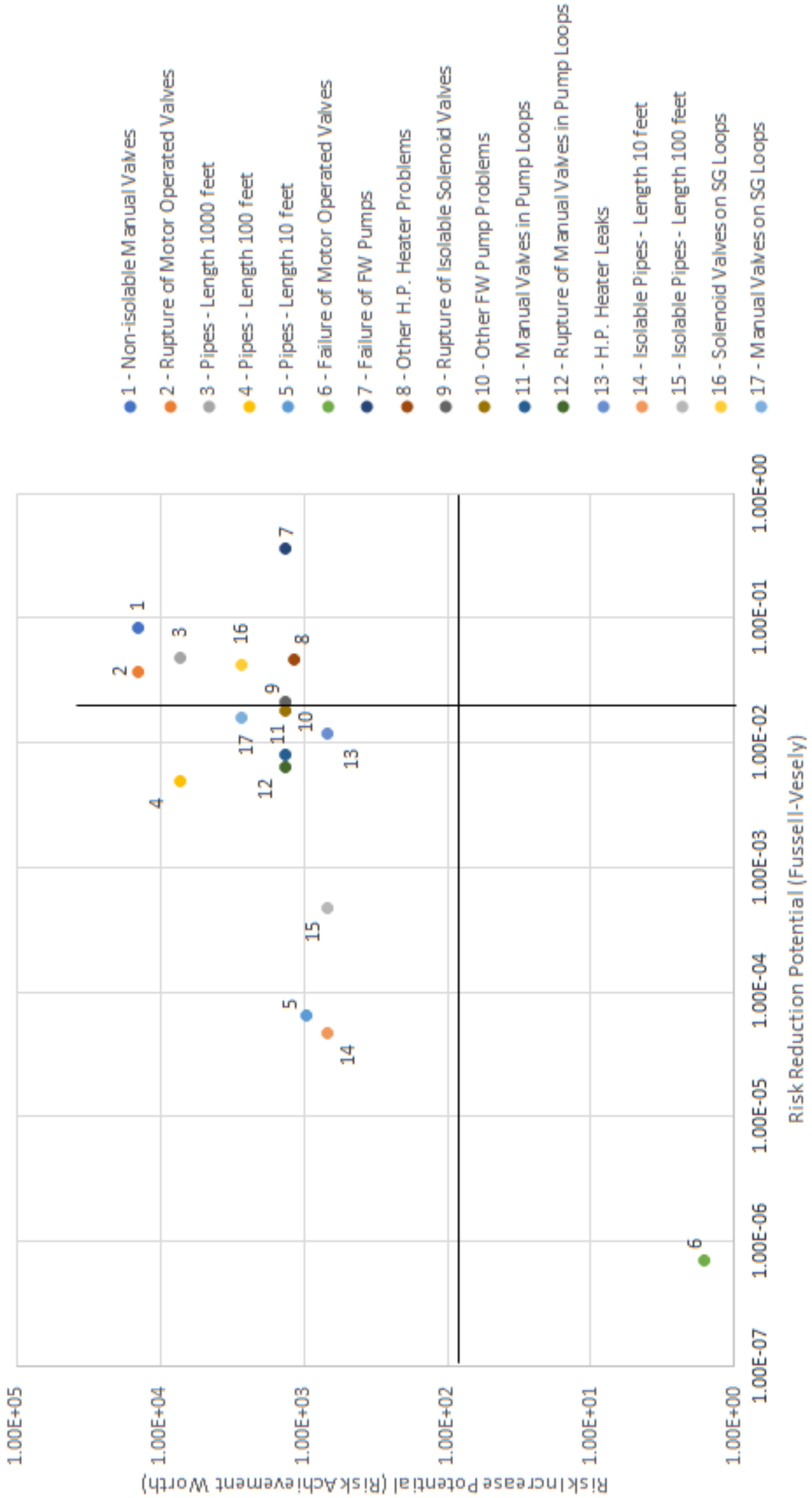


Figure 44. GRA feedwater system four-quadrant plot.

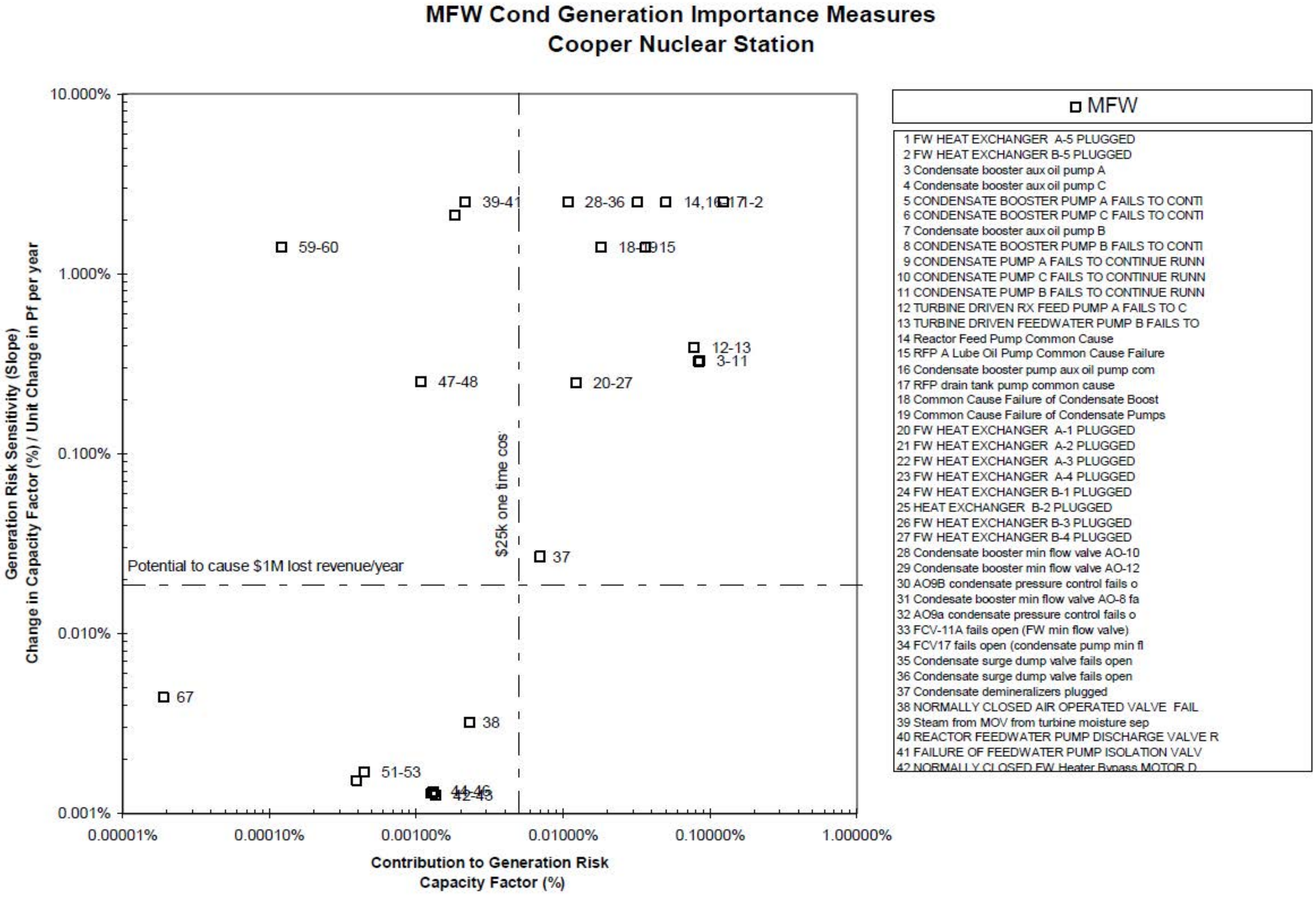


Figure 45. Cooper nuclear station feedwater/condensate four-quadrant plot.

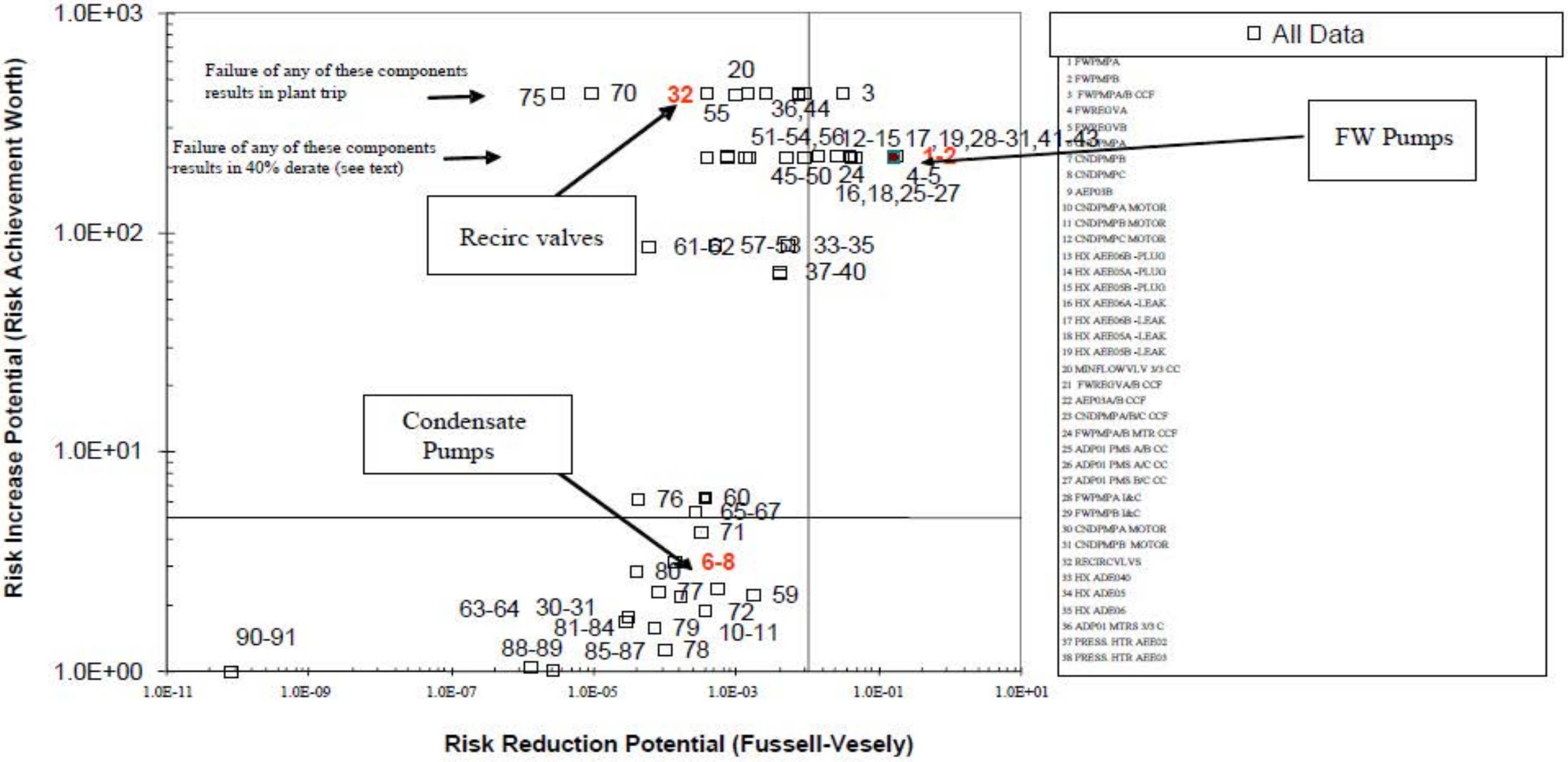


Figure 46. GRA plant implementation guide feedwater/condensate four-quadrant plot.

Ignoring the points obtained from the condensate system in Figure 45 and Figure 46, the relationships between the components in the feedwater systems are related. For example, the feedwater pumps are located far to the right but not as high as some valve types in the system. An additional comparison is the motor-operated valve location on the generic GRA model and the Cooper Nuclear Station GRA model four-quadrant plots. Further comparisons yield the same revelations for many components.

Although the online repair capability has a substantial impact on the high-pressure heaters' contributions to lost generation, the repair capability should have little effect on the four-quadrant plot. This may suggest the failure frequency obtained from EPIX is lower than industry experience suggests. The reason for this could be due to EPIX not differentiating between low-pressure heaters and high-pressure heaters. Different data sources would need to be assessed to reach an adequate conclusion. The model evaluated in this report was conducted to provide a basis for a generic feedwater system GRA model. The generic model provides a solid foundation for the development of a more detailed GRA model for any 4-loop PWR.

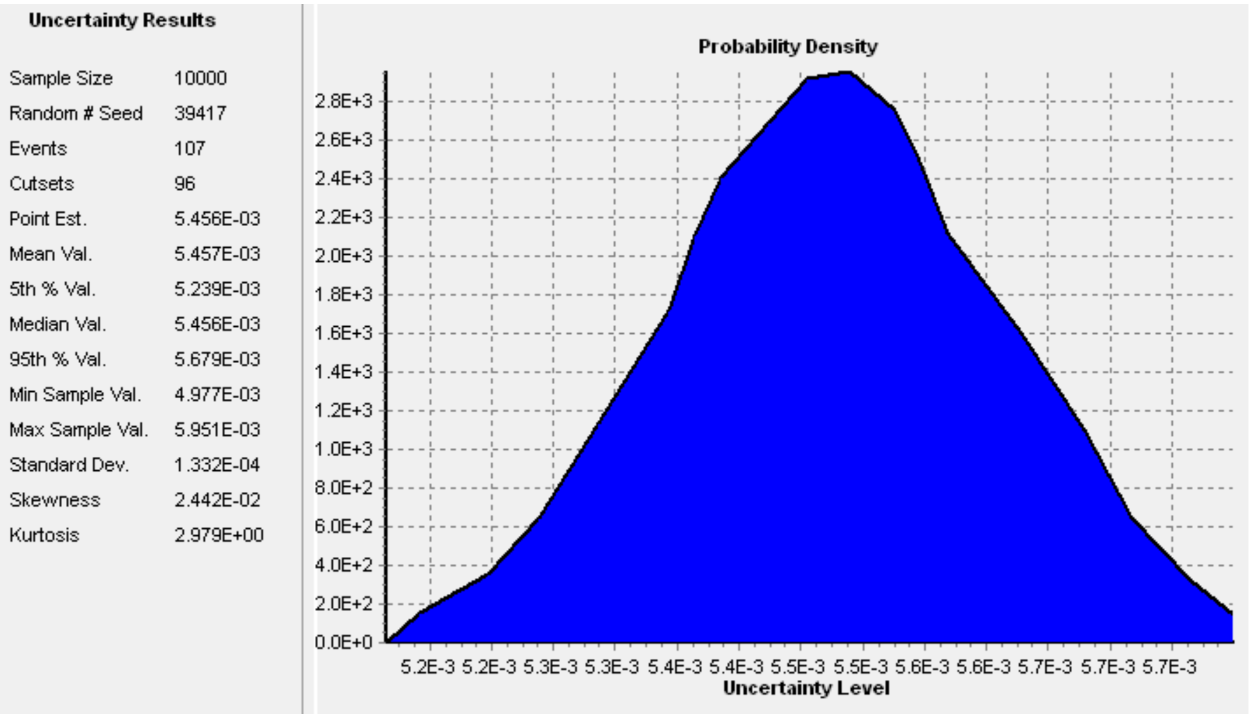
Uncertainty Analysis

The uncertainty distributions for the failure rates were given in the EPIX spreadsheet. The uncertainty values for failure rates were based on a gamma distribution. Table 26 shows how the uncertainty values were given from EPIX.

Table 26. SPAR Component unreliability data and results.

Description	Failure rate [hr^{-1}]	Distribution	α
Turbine-driven pump external leakage (small)	5.38E-07	Gamma	15.5
Motor operated valve fails to remain open	3.24E-08	Gamma	0.593
Hydraulic valve fail to control	4.57E-07	Gamma	42.5

Any basic event failure rate that was not obtained from the EPIX spreadsheet was assigned a gamma distribution with an alpha value of 10. SAPHIRE used the Monte Carlo evaluation method for uncertainty with a sample size of 10,000. The random number seed was a default value obtained from SAPHIRE. The uncertainty evaluation was based on the unavailability of the feedwater system to support full power per 24 hours due to the unavailability of equipment. Therefore, the failure rate and the mean time to repair values of components were taken into consideration. An uncertainty analysis was not able to be conducted on the lost generation values, such as dollars lost per year. In SAPHIRE, the values used to convert the plant derate probability into lost generation were point values and the assumption that there was no associated uncertainty with the values was made. The mean time to repair values were difficult to assign an uncertainty due to the method of obtaining the values. The pc-GAR database does not provide values of uncertainty. Therefore, in the case of the generic plant, the values were assumed to be exact point values. The following figures are the probability density and cumulative distribution plots for the different derate scenarios. Figure 47 and Figure 48 are the distributions for unavailability (in hours) of the feedwater system to support more than 75% power per 24 hours.


Uncertainty Results

Sample Size	10000
Random # Seed	39417
Events	107
Cutsets	96
Point Est.	5.456E-03
Mean Val.	5.457E-03
5th % Val.	5.239E-03
Median Val.	5.456E-03
95th % Val.	5.679E-03
Min Sample Val.	4.977E-03
Max Sample Val.	5.951E-03
Standard Dev.	1.332E-04
Skewness	2.442E-02
Kurtosis	2.979E+00

Figure 47. 25% derate probability density.

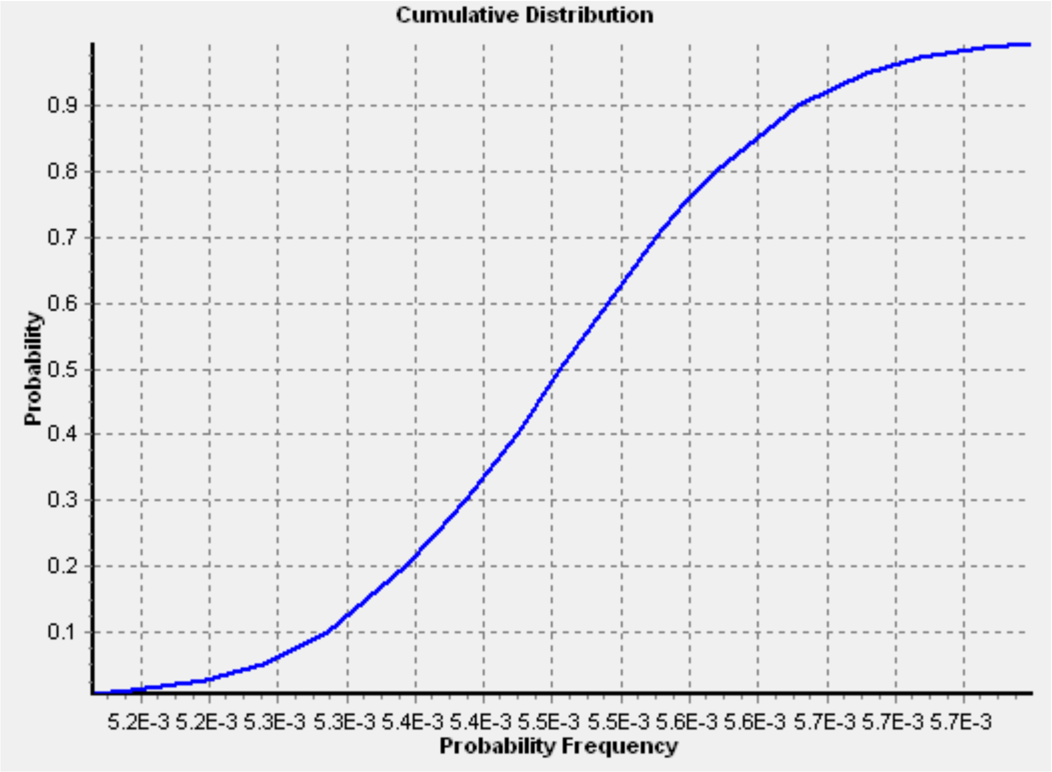
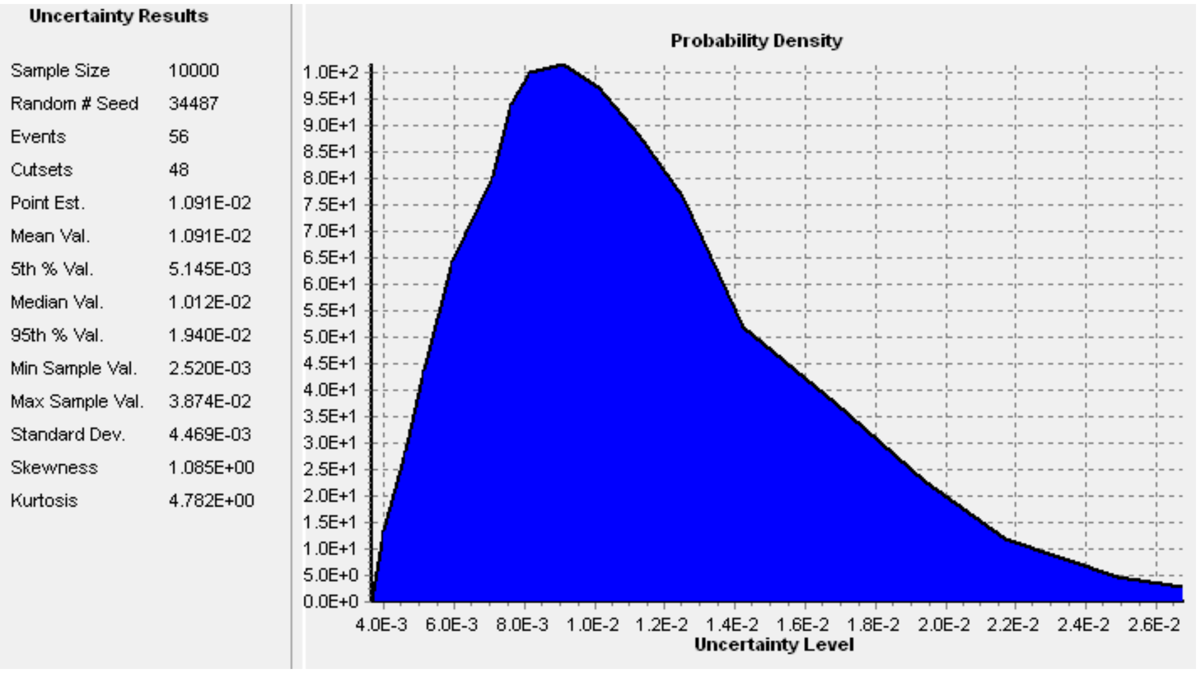


Figure 48. 25% derate cumulative distribution.

Figure 49 and Figure 50 are the distributions for unavailability (in hours) of the feedwater system to support more than 50% power per 24 hours.



Uncertainty Results

Sample Size	10000
Random # Seed	34487
Events	56
Cutsets	48
Point Est.	1.091E-02
Mean Val.	1.091E-02
5th % Val.	5.145E-03
Median Val.	1.012E-02
95th % Val.	1.940E-02
Min Sample Val.	2.520E-03
Max Sample Val.	3.874E-02
Standard Dev.	4.469E-03
Skewness	1.085E+00
Kurtosis	4.782E+00

Figure 49. 50% derate probability density.

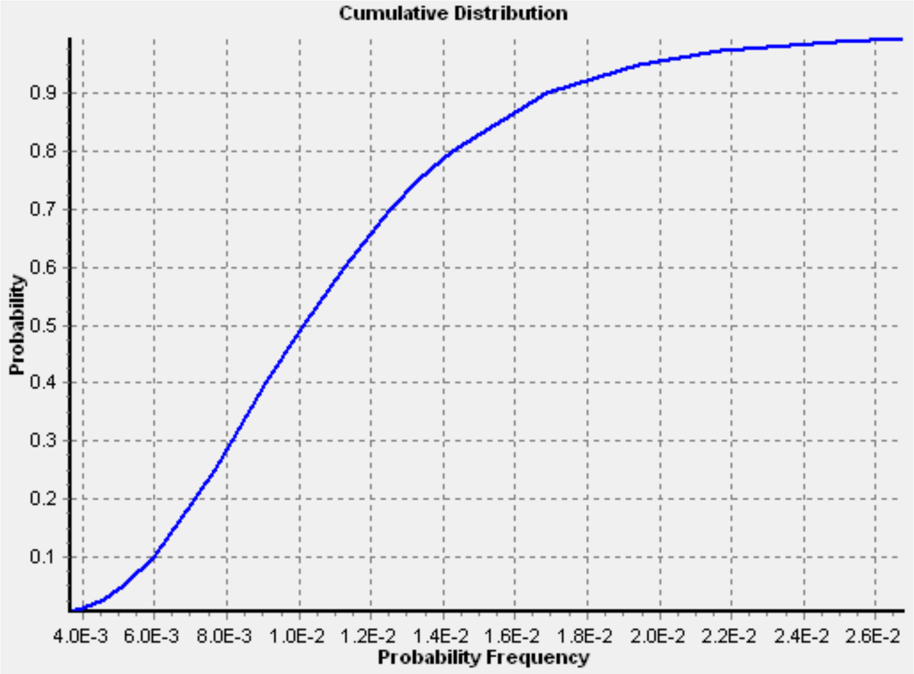
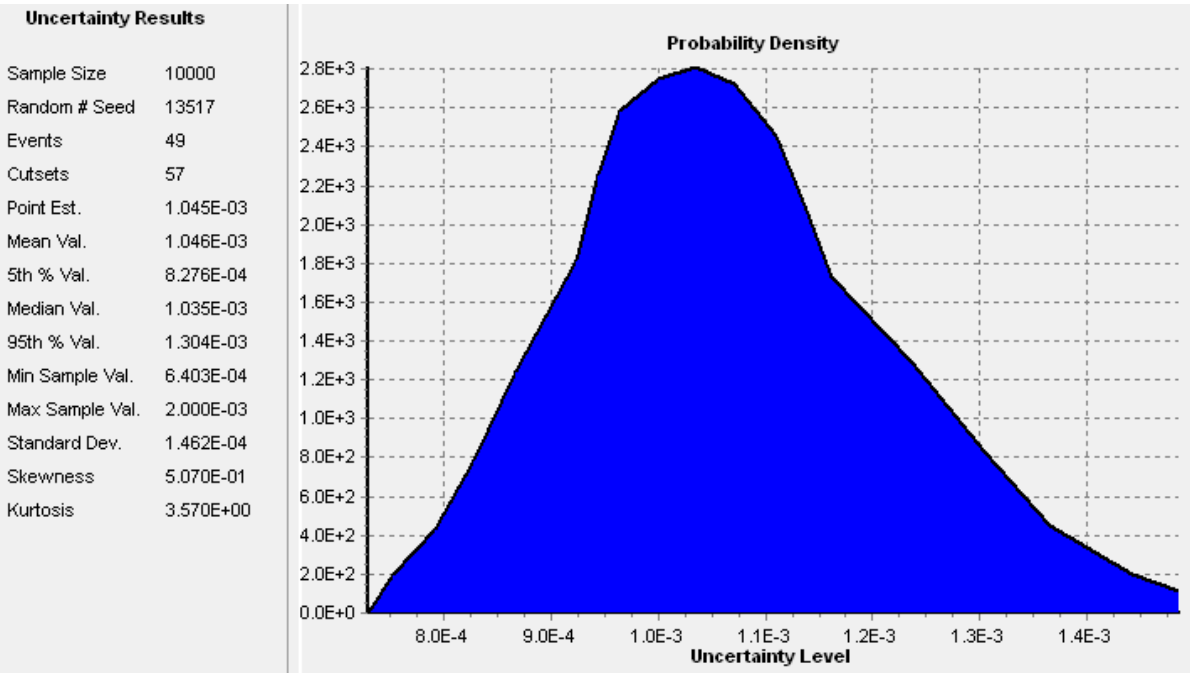


Figure 50. 50 % derate cumulative distribution.

Figure 51 and Figure 52 are the distributions for unavailability (in hours) of the feedwater system to support any power per 24 hours.



Uncertainty Results

Sample Size	10000
Random # Seed	13517
Events	49
Cutsets	57
Point Est.	1.045E-03
Mean Val.	1.046E-03
5th % Val.	8.276E-04
Median Val.	1.035E-03
95th % Val.	1.304E-03
Min Sample Val.	6.403E-04
Max Sample Val.	2.000E-03
Standard Dev.	1.462E-04
Skewness	5.070E-01
Kurtosis	3.570E+00

Figure 51. 100% derate probability density.

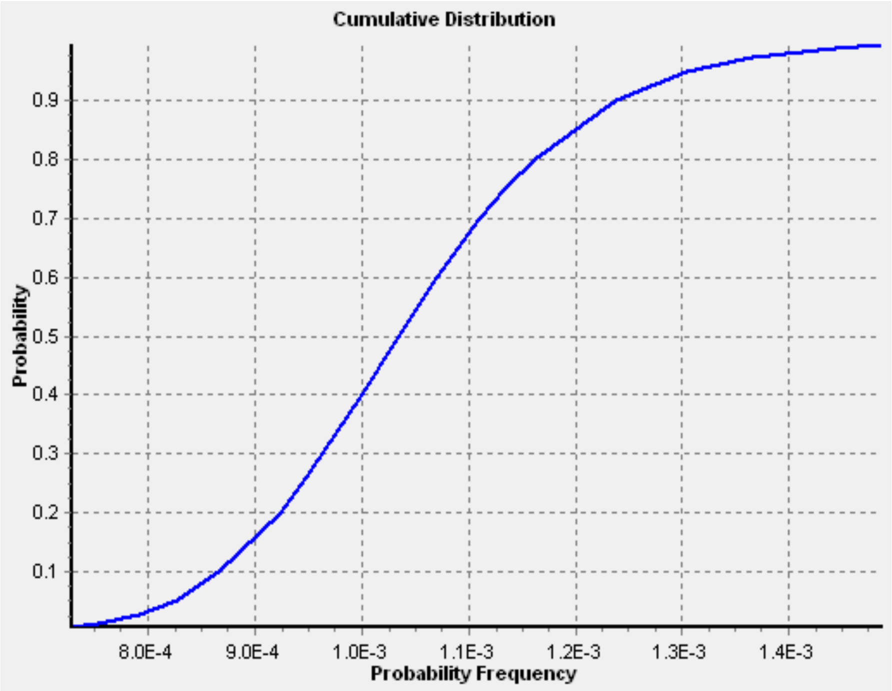


Figure 52. 100% derate cumulative distribution.

Appendix J

RAVEN CODE CAPABILITIES

RAVEN is a flexible and multi-purpose Uncertainty Quantification (UQ), regression analysis, PRA, data analysis and model optimization software. Depending on the tasks to be accomplished and on the probabilistic characterization of the problem, RAVEN perturbs (through Monte-Carlo, Latin Hypercube, reliability surface search [8] sampling methods) the response of the system by altering its parameters. The system is modeled by third party software (e.g., RELAP5-3D, MAAP5) and accessible to RAVEN either directly (software coupling) or indirectly (via input/output files). The data generated by the sampling process is analyzed using classical and more advanced data mining approaches. RAVEN also manages the parallel dispatching (i.e., both on desktop/workstation and large High-Performance Computing machines) of the software representing the physical model. RAVEN heavily relies on artificial intelligence algorithms to construct surrogate models of complex physical systems in order to perform UQ, reliability analysis (limit state surface), and parametric studies. The RAVEN architecture is shown schematically in Figure 53.

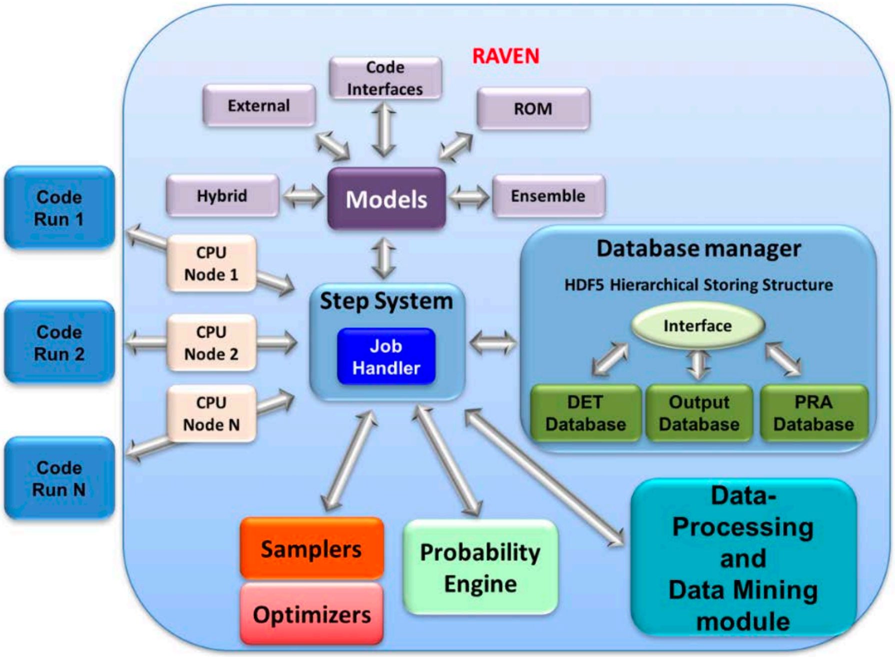


Figure 53. RAVEN abstracted module scheme.

RAVEN's scope is to provide a set of capabilities to build analysis flows based on UQ, reliability analysis, optimization and data analysis techniques to be applied to any physical model(s). The main objective of RAVEN is to assist the engineer/user to:

- Identify the best design (on any physics/model) and its safety impact

- Estimate the likelihood of undesired outcomes (risk analysis)
- Identify main drivers/events to act on for reducing impact/consequences of anomalous dynamic behaviors of the system under analysis
- Construct analysis flows combining multiple physical models and analysis procedures

In other words, the RAVEN software can be employed to perform:

- Uncertainty Quantification
- Sensitivity Analysis / Regression Analysis
- Probabilistic Risk and Reliability Analysis
- Data Mining Analysis
- Model Optimization

The RAVEN software employs several novel and unique techniques, based on extensive use of artificial intelligence algorithms, such as adaptive (smart) sampling, adaptive branching algorithms (Dynamic Event Tree), time-dependent statistical analysis and data mining. The overall set of algorithms implemented in the RAVEN software are designed to handle highly non-linear systems, characterized by system response discontinuities and discrete variables. These capabilities are crucial for handling complex system models, such as those used in the analyses of NPPs. For example, reliability surface analysis, as implemented in RAVEN, is unique and capable to handle non-linear, discontinuous systems, allowing for faster and more accurate assessing of failure risk for complex systems.

Among the different capabilities, RAVEN provides the unique functionality to combine any model (e.g. physical models, surrogate models, data analysis models, etc.) in a single entity (named Ensemble Model) where each model can feedback into others. In the following section, a more detailed description of this capability is reported.

Ensemble Modeling in RAVEN

In several cases multiple models need to be interfaced with each other since the initial conditions of some models are dependent on the outcomes of others. In order to solve this problem, RAVEN provides a model entity named *EnsembleModel* [21]. This class is able to assemble multiple models of other categories (i.e., Code, External Model, Reduced Order Models - ROM), identifying the input/output connections, and, consequentially the order of execution and which sub-models can be executed in parallel.

Figure 54 shows an example of an *EnsembleModel* that is constituted of 3 sub-models (e.g., Reduced Order Models [13], Codes, or External Models) where:

- *Model 2* is connected with *Model 1* through the variable Θ (Model 1 output and Model 2 input);
- *Model 3* is connected with *Model 2* through the variable Π (Model 2 output and Model 3 input);

In this case, the *EnsembleModel* is going to drive the execution of all the sub-models in sequence, since each model (except the *Model 1*) is dependent on the outcomes of previously executed models.

In several cases, the input of a model depends on the output of another model whose input is the output of the initial model. In this situation, the system of equations is non-linear, and an iterative solution procedure needs to be employed. The *EnsembleModel* entity in RAVEN is able to detect the non-linearity of the sub-models' assembling and activate the non-linear solver: an iterative scheme. Figure 55 shows an example of when the *EnsembleModel* entity activates the iteration scheme, which ends when the residue norm (between an iteration and the other) falls below a certain input-defined tolerance.

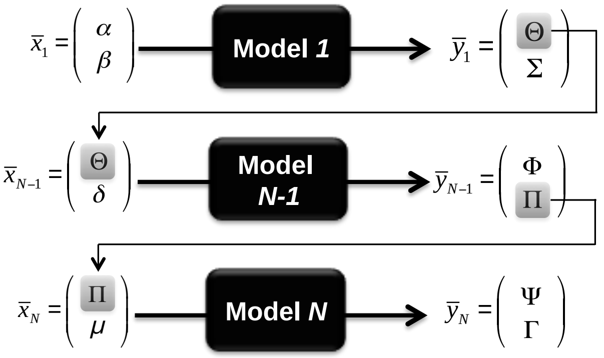

$\bar{x}_1 = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
Model 1
$\bar{y}_1 = \begin{pmatrix} \Theta \\ \Sigma \end{pmatrix}$
$\bar{x}_{N-1} = \begin{pmatrix} \Theta \\ \delta \end{pmatrix}$
Model N-1
$\bar{y}_{N-1} = \begin{pmatrix} \Phi \\ \Pi \end{pmatrix}$
$\bar{x}_N = \begin{pmatrix} \Pi \\ \mu \end{pmatrix}$
Model N
$\bar{y}_N = \begin{pmatrix} \Psi \\ \Gamma \end{pmatrix}$

Figure 54. Example of an *EnsembleModel* constituted of 3 sequential sub-models.

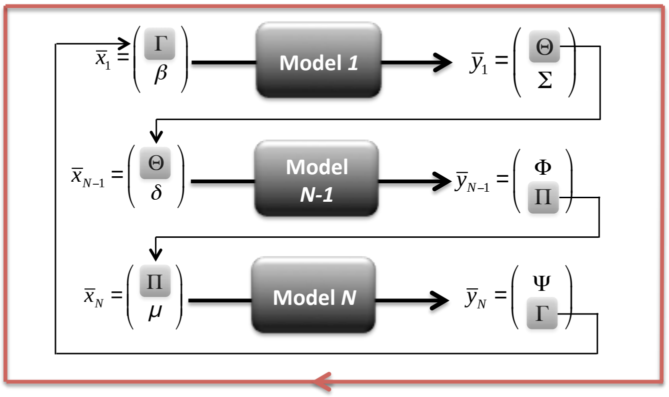

$\bar{x}_1 = \begin{pmatrix} \Gamma \\ \beta \end{pmatrix}$
Model 1
$\bar{y}_1 = \begin{pmatrix} \Theta \\ \Sigma \end{pmatrix}$
$\bar{x}_{N-1} = \begin{pmatrix} \Theta \\ \delta \end{pmatrix}$
Model N-1
$\bar{y}_{N-1} = \begin{pmatrix} \Phi \\ \Pi \end{pmatrix}$
$\bar{x}_N = \begin{pmatrix} \Pi \\ \mu \end{pmatrix}$
Model N
$\bar{y}_N = \begin{pmatrix} \Psi \\ \Gamma \end{pmatrix}$

Figure 55. *EnsembleModel* resolving in a non-linear system of equations – Numerical iterations.

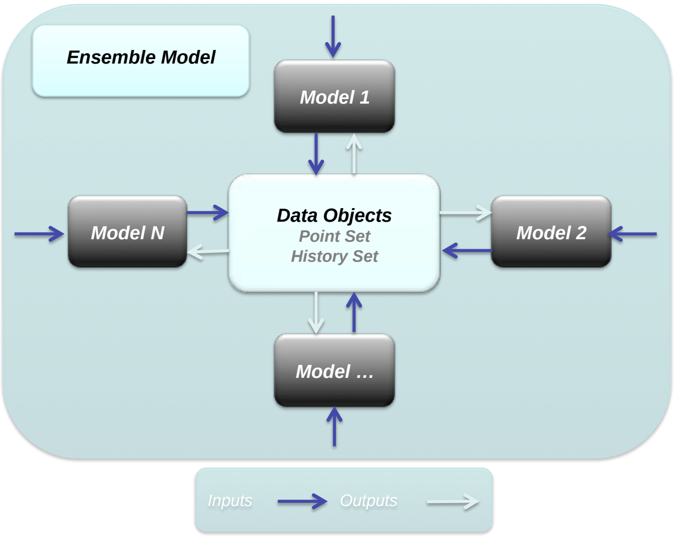


Figure 56. *EnsembleModel* data exchange.

In RAVEN all the models' outputs are collected in internal containers (named *DataObjects*) that store time-series and input/output data relations in a standardized fashion (see Figure 56); in this way, the communication of the output information among different entities (i.e. Models) can be completely independent with respect to the particular type of output generated by a model. The *EnsembleModel* entity fully leverages this peculiarity in order to transfer the data from a Model to the other(s). Based on the Input/Output relations of each of the sub-models, the *EnsembleModel* entity constructs the order of their execution and, consequentially, the links among the different entities.

Appendix K

REVIEW OF METHODS FOR SUPPLY CHAIN SURVEILLANCE AND PRODUCT EVALUATION

According to the Jesse Garant Metrology Center, an aerospace company can save millions of dollars in costs to fix a post-production problem if they spend tens of thousands of dollars (1% of a million) in pre-production inspection. This conclusion corresponds to the fact that if the materials supplied by the supplier are defective, then the products manufactured using those materials are also defective.

Industries today focus on quality starting right from the raw materials to the final manufactured product. The raw materials and products supplied by the suppliers that do not conform to the industry expectations can be avoided by implementing several methods and techniques defined under the term "Supply Chain Surveillance."

Supply Chain Surveillance (SCS) is the process of identifying, analyzing and maintaining the quality standards of the materials and products sent by the supplier with respect to the industry expectations. Additionally, it helps to evaluate the potential supplier, establish a healthy relationship with the suppliers, set expectations for the tolerable defects and quality standards, and verify those expectations.

This appendix provides a literature survey on the methods used in Supply Chain Surveillance. Review was conducted for tools used by various industry sectors and independent of specific NPP supply chain. Some of these tools and their background are summarized in this report.

Using Blockchain in Supply Chain Provenance and Traceability

Industries today are trying to manage hyper-complex, global supply chains, which involve the production, transportation, and fulfillment of products among widespread suppliers. The lack of transparency and the difficulties associated with the investigation of suspicious illegal or unethical practices are the major concerns in today's supply chain management. Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks [65]. Blockchain might find the right place in the supply chain to provide the proof of origin for parts and authentication. Blockchain can be adopted to many applications used for any exchange, agreements, tracking, and payments. It is a decentralized system with everyone in the chain takes ownership for every other asset on the blockchain. These assets are recorded and cannot be erased, which aids in bringing out the transparency of the system. The data in blockchain flows seamlessly in and around, and in real-time, manufacturers can optimize manufacturing planning and store-level forecasting. They can ensure that the right amount of stock is available to satisfy demand with limited excess, thereby eliminating lost sales, minimizing carrying costs and increasing profitability [66]. Figure 57 from the National Institute of Standards and Technology (NIST) shows the layout of blockchain integration with the supply chain.

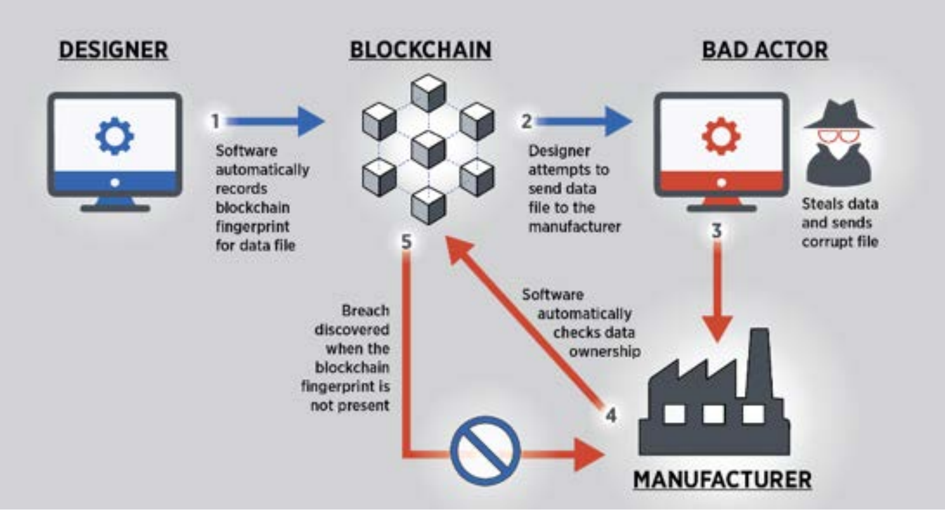

DESIGNER
BLOCKCHAIN
BAD ACTOR
1
Software automatically records blockchain fingerprint for data file
2
Designer attempts to send data file to the manufacturer
Steals data and sends corrupt file
3
5
Breach discovered when the blockchain fingerprint is not present
Software automatically checks data ownership
4
MANUFACTURER

Figure 57. Blockchain layout.

Many large companies like IBM, Walmart, Unilever, Nestle, use this concept in their supply chain management to enhance their provenance, traceability, transparency, immutability, and trust with the suppliers. For example, IBM has come up with a concept of crypto-anchors which when combined with the blockchain technology act as a tamper-proof digital signature helping in authenticating products sent by the supplier. According to IBM, these crypto-anchors are smaller than a grain of salt that has as many as one million transistors and costs less than ten cents to manufacture. According to the 2018 MHI annual industry report, it is expected that the inculcation of blockchain technology in the supply chain in many of the industries will rise to 54% over the next five years. The advancements in microfluidics, packaging platforms, cryptography integrated with blockchain technology will find a new solution to combat the current problems of the supply chain.

Evaluation of Suppliers Using Data Envelopment Analysis (DEA)

Supplier selection is a multi-criterion problem, which includes both qualitative and quantitative factors. The relationship between the industry and the supplier has always been critical. The essential criteria typically utilized for this purpose are pricing structure, delivery product quality and service. A DEA is multifactor, non – parametric productivity analysis tool, which effectively considers multiple inputs and output measures in evaluating relative efficiencies [67]. This data analysis tool evaluates the suppliers based on their inputs and outputs, from which their performance and relative efficiency are calculated. These values are beneficial in benchmarking the right supplier. The data collected here as inputs and outputs are analyzed using the weighted average formula, as shown below in the equation (K-1)[68]:

$$E = \frac{weighted\ sum\ of\ outputs}{weighted\ sum\ of\ inputs} = \frac{\sum_{\mathrm{k=1}}^{\mathrm{s}} \mathrm{u_k} \cdot \mathrm{y_{kp}}}{\sum_{\mathrm{j=1}}^{\mathrm{m}} \mathrm{v_j} \cdot \mathrm{x_{jp}}} \qquad \text{(K-1)}$$

where m is the number of inputs, s is the number of outputs, $\mathrm{y_{kp}}$ is the amount of k-produced by the supplier, $\mathrm{x_{jp}}$ is the amount of input j utilized by the supplier, $\mathrm{v_j}$ is the weight given to the input k, and $\mathrm{u_k}$ is the weight given to output j. The DEA method is not only helpful in evaluating the supplier based on their efficiency but it also helps in focusing on the critical parameter(s) that the supplier should work to meet the expectations of the industry. Many third-party agencies had developed their own DEA software to analyze the complex input and output data and help in finding an efficient supplier for the industry.

Evaluation Of Suppliers Using Factory Audits

The quality of the imported products depends wholly on the suppliers and their factory working conditions that should comply with the international standards. Having an unqualified supplier who does not conform with the international standards can subject the recipient to supply chain risks, from factory disasters and negative publicity to legal repercussions and quality issues. The lack of a standardized audit framework has led to "audit fatigue" in the industry.

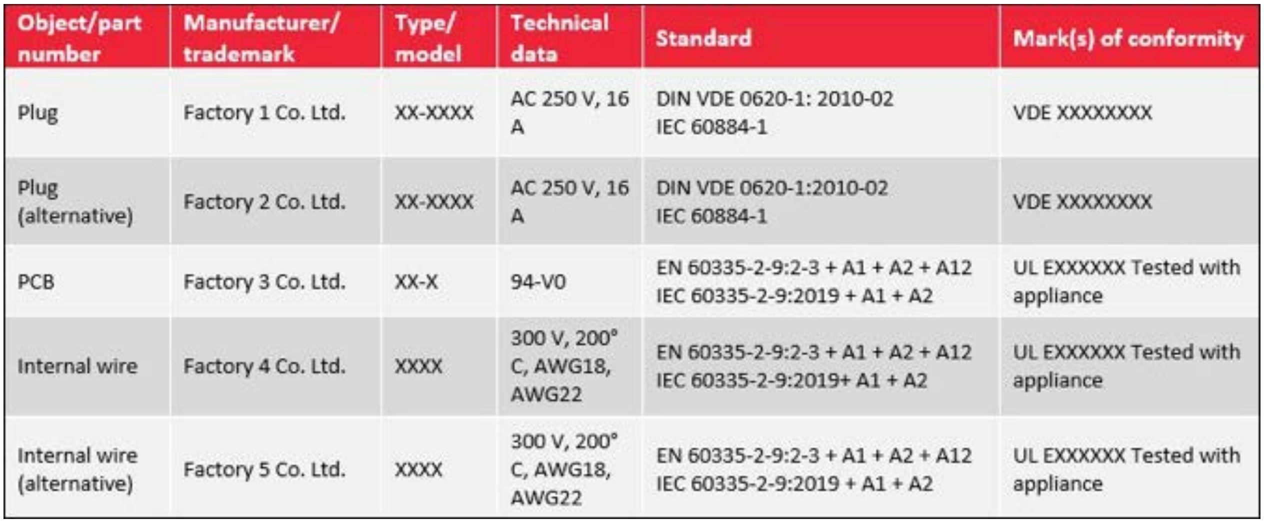
ISO 9001 is a quality management standard developed by the International Organization for Standardization (ISO). It is the only standard that can be attributed to quality management in the ISO 9000 family. A typical ISO 9001 standard quality system includes evaluating the following: Basic facilities; environment and equipment maintenance; quality management system organization; incoming quality controls for materials and components; during production controls to identify quality issues; finished goods controls and inspection; lab testing capabilities; HR recruitment and training practices; engineering, research and design capabilities; business development and management behavior [70]. Companies like Alibaba evaluate, assess and select the suppliers based on the ISO quality standard audit.

Evaluation Of Supplier Using Reliability Capability

Evaluating supplier by factory audits can be helpful in one way, but the international standards and parameters that establish the ability of a manufacturer to produce a quality product do not necessarily establish the manufacturer's ability to produce a reliable product consistently. Consequently, the ISO 9000 series certifications that act as an international reference for quality requirements cannot be used as a metric for assessing the capability of a manufacturer to produce a reliable product [71]. So, industries should undergo reliability capability assessment to have a pre-facto assurance that the goods and services delivered by their supplier are reliable enough to not have any production flow disruption. Reliability capability is the measure of an electronics manufacturer's ability to identify and understand its reliability-related objectives and the effectiveness of the processes and practices used by the organization to meet those objectives [72]. The reliability capability evaluation process is comprised of three phases. In the first phase, initial information about the process is sent to the company being evaluated. A reliability capability evaluation questionnaire is included for the company to answer and collect evidence supporting the answers. In the second phase, evaluators visit the facility, and verify the responses to the questions with the supporting evidence. The third phase involves the compilation of an evaluation report. After this three-phase process, five levels of reliability capability maturity along with their characteristics are measured with respect to evolutionary transition for a company. To assign a maturity level to a key practice, requirements in terms of reliability tasks have been enumerated. An assessment based on key practices can place companies at one of the five maturity levels using radar charts [73]. It also been proved that this method is very efficient in benchmarking the supplier for reliability based on their activities.

Product's Construction Data Form (PCDF)

Critical components are those which, when they fail compromise the safety of the product. They are crucial in maintaining compliance with the standard. The International Electrotechnical Commission (IEC) specified that critical components, sometimes referred to as safety-critical components, are a primary concern in developing a PCDF [74]. A PCDF should list the following information: part number; manufacturer or trademark name; part type or model; technical specifications; relevant testing standard and certification markings or symbols. An example of PCDF table is shown in Figure 58 [75]. Using this PCDF, the supplier industry checks the critical components for its International Safety Standard along with the quality. It also saves time by providing the requirements for production.



Object/part number	Manufacturer/ trademark	Type/ model	Technical data	Standard	Mark(s) of conformity
Plug	Factory 1 Co. Ltd.	XX-XXXX	AC 250 V, 16 A	DIN VDE 0620-1: 2010-02 IEC 60884-1	VDE XXXXXXXX
Plug (alternative)	Factory 2 Co. Ltd.	XX-XXXX	AC 250 V, 16 A	DIN VDE 0620-1:2010-02 IEC 60884-1	VDE XXXXXXXX
PCB	Factory 3 Co. Ltd.	XX-X	94-V0	EN 60335-2-9:2-3 + A1 + A2 + A12 IEC 60335-2-9:2019 + A1 + A2	UL EXXXXXX Tested with appliance
Internal wire	Factory 4 Co. Ltd.	XXXX	300 V, 200° C, AWG18, AWG22	EN 60335-2-9:2-3 + A1 + A2 + A12 IEC 60335-2-9:2019+ A1 + A2	UL EXXXXXX Tested with appliance
Internal wire (alternative)	Factory 5 Co. Ltd.	XXXX	300 V, 200° C, AWG18, AWG22	EN 60335-2-9:2-3 + A1 + A2 + A12 IEC 60335-2-9:2019 + A1 + A2	UL EXXXXXX Tested with appliance

Figure 58. An example of CDF for an electrical appliance exported to Germany.

Risks of Counterfeit Part and Material Injection

A counterfeit electronic part is one whose identity has been deliberately misrepresented. A counterfeit part is considered a category of non-conforming product. Along with the methods discussed earlier, there is always a risk of counterfeited raw-materials and components making their way into the supply chain. These parts can be avoided by using the tools and methods reported in the literature [76-79] and by use of appropriate supply chain management tools and industry standards. Our primary focus in this report is the methods used in the supply chain surveillance. One of the evaluation criteria for the tools will be the ability to avoid counterfeit parts and materials.

Evaluation Criteria to Compare The Surveillance Tools

The following criteria are selected to evaluate and compare the various methods:

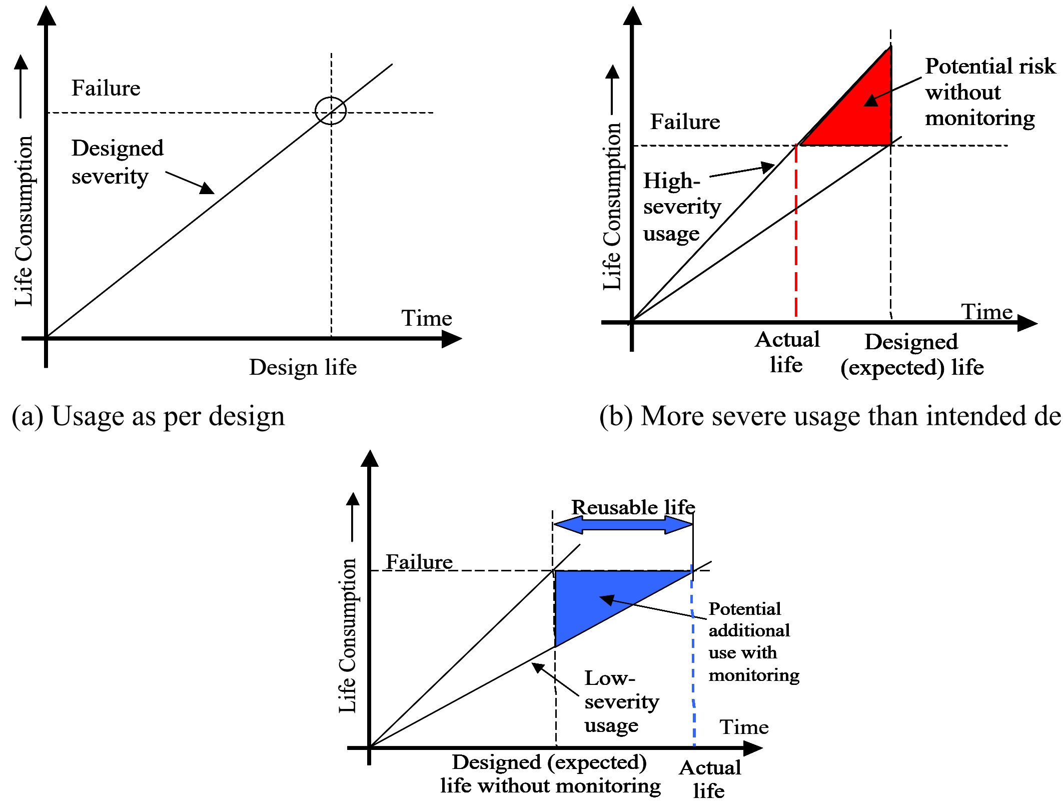
1. **Human resources cost:** The total cost involved in employing the human resource and their services to develop, implement and monitor the pilot process.
2. **Capital cost:** The fixed, one-time setup expenses of the pilot process, per se initial research, administrative and management expenses.
3. **Performance cost:** The cost associated with measuring the performance factors which are represented in the ratio of cost to benefits.
4. **Material cost:** The cost associated with the procuring, storing and buying materials (both direct and indirect) for the implementation of the process.
5. **Workforce skill requirement:** The skill of the manpower for implementing the process based on the methods, in terms of high, medium or low skill requirement.
6. **Process implementation time**: The time taken for implementing the pilot process based on the methodology.
7. **Product evaluation time**: The time taken for evaluating the product.
8. **Number of unscheduled maintenance:** The measure of how frequently the maintenance team will be responding to the product being manufactured from the supplied raw materials that underwent the pilot process developed based on the method.

9. **Ability to detect and avoid counterfeit parts and materials:** Counterfeit parts result in additional risk of not finding a responsible party to make good if a problem arises – the surveillance method should be able to detect and avoid counterfeit parts.

Appendix L

ADVANCED PHM METHODS

Designers often establish the usable life of products and warranties based on extrapolating accelerated test results to assumed usage rates and life-cycle conditions. These assumptions may be based on worst-case scenarios of various parameters composing the end-user environment. In principle, if the assumed conditions and actual use conditions are the same, the product should be reliable for the designed lifetime, as shown in Figure 59 (a). However, this is rarely true, and usage and environmental conditions could vary significantly from those assumed. To address the actual lifecycle conditions, products can be equipped with life consumption monitors for in situ assessment of remaining life. Thus, even if the product is used at a higher usage rate and in harsh conditions, it can still avoid unscheduled maintenance and catastrophic failure, maintain safety, and ultimately save cost. Or if the product is used in a more benign manner, its life can be extended (see Figure 59 (b)).



(a) Usage as per design

(b) More severe usage than intended design

(c) Less severe usage than intended design

Figure 59. Application of health monitoring for product reuse.

One of the vital inputs in making end-of-life decisions is the estimate of degradation and the remaining life of the product. Figure 59 (c) illustrates a scenario in which a working product is returned at the end of its designed life. Using the health monitors installed within the product, the reusable life can be assessed, without having to disassemble the product. Ultimately, depending on other factors including cost of the product, demand for spares, and yield in assembly and disassembly, the manufacturer can choose to reuse or dispose.

Data-driven approaches use data analytics and machine learning to determine anomalies and make predictions about the reliability of electronic devices, systems, and products based on internal and/or external covariates (called endogenous and exogenous covariates). Internal covariates (e.g., temperature, vibration) are measured by sensors on the asset and are only present when the asset is operating. External covariates (e.g., weather data) are present whether the asset is operating or not. The data-driven approach analyzes asset performance data based on a training database of internal and/or external covariates. A failure precursor is a data event or trend that signifies performance degradations that may be indicative of impending failure. A precursor indication is usually a change in a measurable variable that can be associated with subsequent failure. For example, a shift in the output voltage of a power supply might suggest impending failure due to a damaged feedback regulator and opto-isolator circuitry. Failures can then be predicted by using causal relationships between measured variables that can be correlated with subsequent failure and for Phisics of Failure (PoF).

A first step in failure precursor PHM is to select the life-cycle parameters to be monitored. Parameters can be identified based on factors that are crucial for safety, that are likely to cause catastrophic failures, that are essential for mission completeness, or that can result in long downtimes. Selection can also be based on knowledge of the critical parameters established by experience, field failure data on similar products, and qualification testing. More systematic methods, such as Failure Modes, Mechanisms, And Effects Analysis (FMMEA), can also be used to determine parameters that need to be monitored.

In general, to implement a precursor reasoning-based PHM system, it is necessary to identify the precursor variables for monitoring and then develop a reasoning algorithm to correlate the change in the precursor variable with the impending failure. This characterization is typically performed by measuring the precursor variable under an expected or accelerated usage profile. Depending on the characterization, a model is developed—typically a parametric curve-fit, neural network, Bayesian network or a time-series trending of a precursor signal. This approach assumes that there are one or more expected usage profiles that are predictable and can be simulated, often in a laboratory setup. In some products the usage profiles are predictable, but this is not always true.

For a fielded product with highly varying usage profiles, an unexpected change in the usage profile could result in a different (non-characterized) change in the precursor signal. If the precursor-reasoning model is not characterized to factor in the uncertainty in life-cycle usage and environmental profiles, it may provide false alarms. Additionally, it may not always be possible to characterize the precursor signals under all possible usage scenarios (assuming they are known and can be simulated). Thus, the characterization and model development process can often be time consuming and costly and may not always work. There are many examples of the monitoring and trending of failure precursor to assess health and product reliability.

Data-driven approaches for PHM are used for both the diagnosis and prognosis stages, often based on statistical and machine learning techniques, as illustrated in Figure 60.

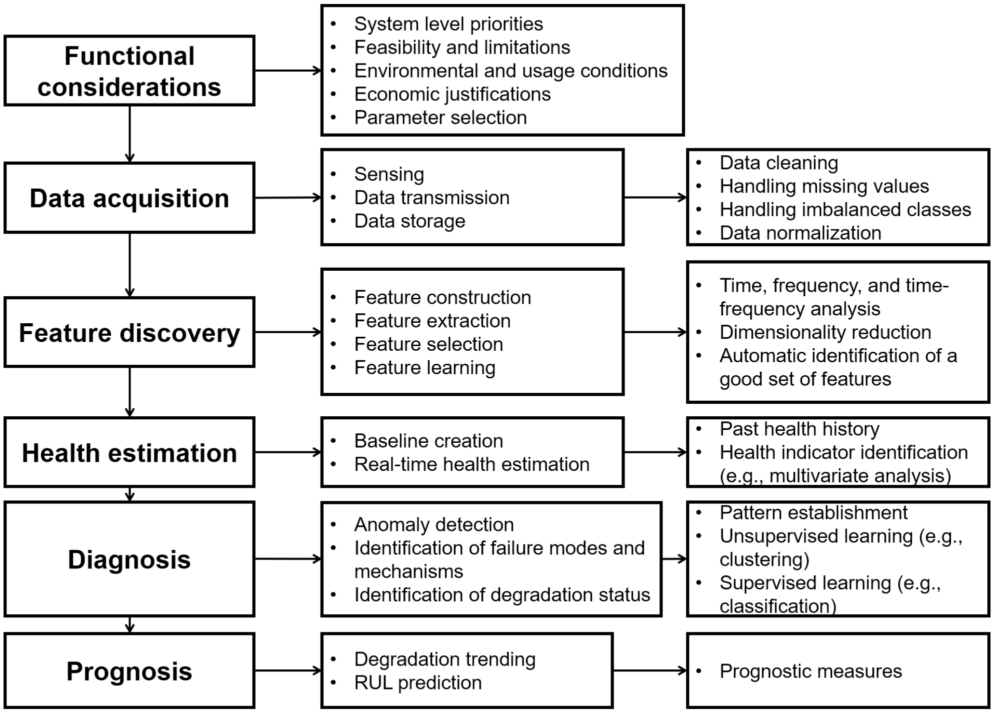

Functional considerations
• System level priorities
• Feasibility and limitations
• Environmental and usage conditions
• Economic justifications
• Parameter selection
Data acquisition
• Sensing
• Data transmission
• Data storage
• Data cleaning
• Handling missing values
• Handling imbalanced classes
• Data normalization
Feature discovery
• Feature construction
• Feature extraction
• Feature selection
• Feature learning
• Time, frequency, and time-frequency analysis
• Dimensionality reduction
• Automatic identification of a good set of features
Health estimation
• Baseline creation
• Real-time health estimation
• Past health history
• Health indicator identification (e.g., multivariate analysis)
Diagnosis
• Anomaly detection
• Identification of failure modes and mechanisms
• Identification of degradation status
• Pattern establishment
• Unsupervised learning (e.g., clustering)
• Supervised learning (e.g., classification)
Prognosis
• Degradation trending
• RUL prediction
• Prognostic measures

Figure 60. A general procedure of a data-driven approach to prognostics.

In Figure 60, data acquisition is to collect data necessary for PHM, including operational and environmental data that can be obtained from sensors by selecting and appropriately locating sensors that provide the capability to collect a history of time-dependent degradation of materials or environmental stresses on a target product. In general, the first step of a data-driven approach to PHM is data pre-processing, including missing value management, data cleansing (e.g., noise removal, outlier removal), normalization or scaling, imbalanced data management, and so forth.

The next step will be feature discovery to find a good set of features that can be used for anomaly detection, diagnosis, and prognosis. More specifically, feature discovery involves feature construction via time, frequency, and time-frequency analyses, dimensionality reduction based on either feature extraction or feature selection, and feature learning using deep neural networks to automatically discover the representations needed for feature detection and classification, typically related to diagnostic tasks in PHM. Note that feature extraction is used to reduce the dimensionality of the given feature vector by using linear or non-linear transformations, whereas feature selection is used to select an optimal subset of the given feature vector for PHM tasks.

Representative feature extraction techniques include Principal Component Analysis (PCA) [80], Kernel PCA [81], Linear Discriminant Analysis (LDA) [82], Kernel LDA [83], generalized discriminant analysis [84], independent component analysis [85], t-distributed stochastic neighbor embedding [86], and so forth. For feature selection, the following methods are representative: filter methods, wrapper methods, and embedded methods. Filter feature selection methods apply a statistical measure to assign a scoring to each feature. The features are ranked by their score and either selected to be kept or removed from a given dataset. The methods are often univariate and consider the feature independently, or with regard to the dependent variable. Some examples of some filter methods include the Chi-square test [87], information gain [88] and correlation coefficient scores [89]. Wrapper methods consider the selection of a set of features as a search problem, where different combinations are prepared, evaluated and compared to other combinations. A predictive model (e.g., k-nearest neighbor, support vector machines, and neural networks) is used to evaluate a combination of features and assign a score based on model accuracy. The search process may be methodical such as a best-first search, it may be stochastic such as a random hill-climbing algorithm, or it may use heuristics, like forward and backward passes to add and remove features. An example of a wrapper method is the recursive feature elimination algorithm [90]. Embedded methods learn which features best contribute to the accuracy of the model while the model is being created. The most common type of embedded feature selection methods are regularization methods. Regularization methods are also called penalization methods that introduce additional constraints into the optimization of a predictive algorithm (such as a regression algorithm) that bias the model toward lower complexity (fewer coefficients). Examples of regularization algorithms are the LASSO [91], elastic net [92] and ridge regression [93] approaches.

The use of handcrafted features for diagnosis has limited improving diagnostic performance [94]. Likewise, handcrafting a good set of features is a manual process that is problem-specific and un-scalable. Accordingly, the need for automatically discovering the features useful for anomaly detection, diagnosis, and prognosis has increased. Zhao et al. [95, 236] verified the efficacy of deep neural networks for feature learning to improve diagnostic performance. Shao et al. [96] used auto-encoders to reduce the dimensionality of the input data and employed a novel convolutional deep belief network to learn the representative features for fault diagnosis. Liu et al. [97] used a Gaussian-Bernoulli deep belief network for fault diagnosis of electronics-rich analog systems by effectively capturing high-order semantic features from analog circuits' voltage signals and verified the effectiveness of the method by comparing with conventional feature extraction methods in terms of diagnostic performance.

Diagnosis extracts fault-related information from the sensor signals caused by anomalies in asset health. Anomalies may result from material degradation, as well as changes in use conditions. Diagnosis relates the signal anomalies to a failure mode(s) and identifies the quantity of damage that has occurred as a health indicator. The results from this anomaly diagnosis can provide advanced warnings of failure. As mentioned above, diagnosis is often referred to as a classification problem due to its nature of identifying failure modes and/or mechanisms, pinpointing the type of faults, and determining the levels of degradation. Accordingly, diverse supervised learning algorithms have been employed for diagnosis, including k-nearest neighbor [98,99], support vector machines [100,101,234], decision trees [102,103], and shallow/deep neural networks [104-106, 238] and petri nets [235].

Despite the fact that the supervised learning algorithms have been studied for fault diagnosis of diverse applications, the problem is that there is no systematic way to identify a specific machine learning model that can work well for fault diagnosis. This is because each of the machine learning models are based on assumptions on one or more properties of data (e.g., non-normality, multimodality, nonlinearity, etc.). For example, a support vector machine assumes the data or its transform using a kernel function to be linearly separable. Likewise, a fundamental assumption of the linear discriminant analysis is that the independent variables (or features) are normally distributed. These assumptions can rarely be met in real-world data, leading to unacceptable errors. With the development of artificial neural network technology, deep learning techniques have become popular. These techniques do not depend on strong assumptions as do many other methods, and their superior accuracy has been reported for a wide range of applications. However, deep learning has yet to overcome the following challenges. First, it is prone to overfitting, leading to large variances. Second, it does not work well for multimodal data. Although some solutions have been proposed for the former challenge, the later challenge will likely remain unresolved into the near future. Thus, ensemble learning methods to overcome the drawbacks of selecting a specific machine learning algorithm for fault diagnosis have been used [107].

Prognosis or remaining useful life estimation methods use statistical and machine learning algorithms to predict the progression of a specific failure mechanism from its incipience to failure within appropriate confidence intervals. Xiong et al. [108] presented a state-of-charge estimation method for lithium-ion batteries using a double-scale particle filtering method. Chang et al. [109] introduced a prognostics-based qualification method for light-emitting diodes by exploiting a relevance vector machine regression model.

This step often requires additional information not traditionally provided by sensors, such as maintenance history, past and future operating profiles, and environmental factors [110], but available within the Internet of Things (IoT) paradigm. The final key aspects of PHM are to effect appropriate decision making; to prevent catastrophic failures; to increase asset availability by reducing downtime and no-fault-founds; to extend maintenance cycles and execute timely repair actions; to lower life-cycle costs from reductions in inspection, repair, and inventory costs; and to improve system qualification, design, and logistical support.

Compared to PoF approaches, data-driven approaches do not necessarily need system-specific information. The behavior of the system based on the data collected can be learnt using the data-driven approaches and can be used to analyze intermittent faults by detecting changes in system features. The approaches can also be used in complex systems with multiple and potentially competing failure modes as long as the system exhibits repeatable behavior. Zhang et al. [237] presented an approach for the prognosis of lithium-ion batteries using Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) to learn the long-term dependencies among the batteries' degraded capacities. In other words, the strength of data-driven approaches is their ability to transform high-dimensional noisy data into lower-dimensional information for diagnostic and prognostic decisions. Reliance on historical data on the failure modes or mechanisms the analyst seeks to detect, are some of the limitations of the data-driven approach. This especially can be an issue when the consequence of failure is high, resulting in reliance on simulated or laboratory rather than field data for the training dataset. Reliance on historical data is also an issue for new products for which an extensive field failure history is not available.

The advantages from the PoF-based and data-driven approaches are combined to allow better RUL prediction capability [111] as shown in Figure 61. This approach reduces the reliance on historical datasets and addresses the issue of previously unseen failure modes.

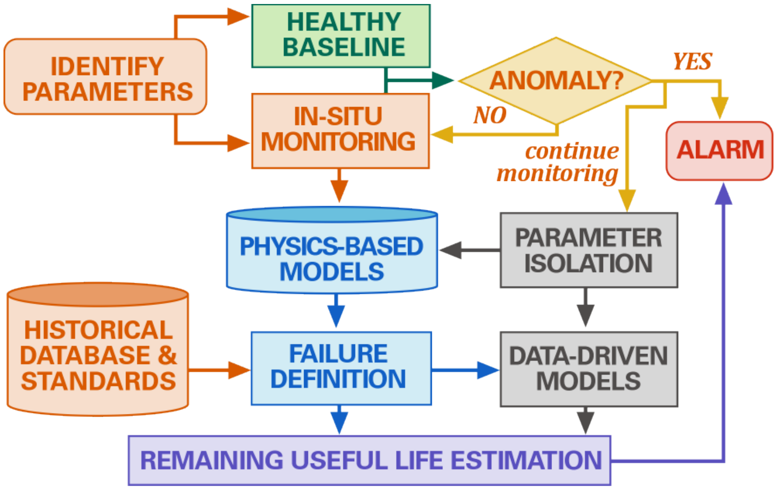


Figure 61. Fusion PHM approach [111].

In fusion PHM, the first step is to determine which variables to monitor. The variables consist of external covariates, including operational and environmental loads, as well as internal covariates based on sensor data. The next step is to identify features of these variables. Then, *in-situ* measurements and deviations from the features associated with healthy states are used to detect anomalous behavior (e.g., Mahalanobis distance [112] (basically a multi-dimensional generalization of the idea of measuring how many standard deviations away a point P is from the mean of a distribution D) , sequential probability ratio test [113], and self-organizing map [114]). Once anomalies are detected, isolation techniques identify features that significantly contribute to the abnormal status. These features are further used as inputs of PoF models for RUL prediction. For the purpose of feature isolation, various data-mining and machine learning-based techniques (e.g., PCA [115], mutual information-based feature selection [116], and support vector machine SVM [117]) can be employed.

PoF models are used to assess *in-situ* degradation of the system under environmental and operating conditions. In fact, a number of potential failure mechanisms may exist in the use of the system. It may not always be the case that, it is theoretically necessary to have PoF model(s) corresponding to each failure mechanism for accurate assessment of in-situ degradation. So, the fusion PHM scheme basically identifies and prioritizes the potential mechanisms for the system under certain environmental and operational conditions. Then, PoF models can be identified from the database involving pre-defined PoF models.

Failure definition is considered as a process of defining the criteria of failure. Additionally, failure definition is based on PoF models, historical usage data, system specifications, or related standards for each potential failure mechanism. In Figure 61, degradation modeling is defined as a process of learning (or predicting) the behavior of the model parameters that are highly correlated with failure. To predict a parameter degradation trend, techniques such as relevance vector machine [118], hidden Markov model [119], and filters (e.g., Kalman filter [120] and particle filter [121]) can be used. If the predictive parameters meet the failure criteria resulting from failure mode definition, then the RUL is predicted using this information. Estimated Time To Failure (TTF) also can be predicted using statistical and machine learning models.

The aim of the fusion approach is to overcome the limitations of both the PoF-based and data-driven approaches for RUL prediction. A fusion prognostic framework was proposed to improve the accuracy of system state forecasting by incorporating the strengths of both the data-driven and PoF approaches. The fusion PHM approach was used to predict the RUL of Multilayer Ceramic Capacitors (MLCCs) [122], avionics systems [123], integrated-gate bipolar transistors (IGBTs) [124], and corrosion fatigue of structures [125]. These fusion-based PHM applications can be appropriate for specific applications. In the future, IoT-based PHM will assist these fusion models in the same way as it will support data-driven models.

Implementation of PHM in a System of Systems

System of systems is the term used to describe a complex system comprising many different subsystems that may be structurally or functionally connected. These different subsystems might themselves be made up of different subsystems. In a system of systems, many independent subsystems are integrated such that the individual functions of the subsystems are combined to achieve a capability/function beyond the capability of the individual subsystems. For example, a military aircraft is made up of subsystems, including: airframe, body, engines, landing gear, wheels, weapons, radar, avionics etc. Avionic sub-systems could include the Communication Navigation and Identification (CNI) system, GPS, inertial navigation system (INS), Identification Friend Or Foe (IFF) system, landing aids, and voice and data communication systems. It is noted that NPPs similarly incorporate numerous subsystems that monitor and control various high-level functions such as core reactivity, core flow and cooling, containment integrity, etc. all with the overall objective of economically and safety generating electricity.

Implementing an effective PHM strategy for a complete system of systems requires integrating different prognostic and health monitoring approaches. Because the systems are so complex, the first step in implementation of prognostics is to determine the weak link(s) in the system. One of the ways to achieve this is by conducting a FMMEA for the product. Once the potential failure modes, mechanisms, and effects have been identified, a combination of canaries, precursor reasoning, and life-cycle damage modeling may be implemented for different subsystems of the product, depending on their failure attributes. Once the monitoring techniques have been decided, the next step is to analyze the data.

Different data analysis approaches like data-driven models, PoF-based models, or hybrid data analysis models can be used to analyze the same recorded data. For example, operational loads of computer system electronics such as temperature, voltage, current, and acceleration can be used with PoF-damage models to calculate the susceptibility to electromigration between metallization and thermal fatigue of interconnects, plated-through holes, and die attach. Also, data about the CPU usage, current, and CPU temperature, for example, can be used to build a statistical model that is based on the correlations between these parameters. This data-driven model can be appropriately trained to detect thermal anomalies and identify signs for certain transistor degradation.

Implementation of prognostics for a system of systems is complicated and in the very initial stages of research and development. But there has been tremendous development in certain areas related to PHM. Advances in sensors, microprocessors, compact nonvolatile memory, battery technologies, and wireless telemetry have already enabled the implementation of sensor modules and autonomous data loggers. Integrated, miniaturized, low-power, reliable sensor systems operated using portable power supplies (such as batteries) are being developed. These sensor systems have a self-contained architecture requiring minimum or no intrusion into the host product, in addition to specialized sensors for monitoring localized parameters. Sensors with embedded algorithms will enable fault detection, diagnostics, and remaining-life prognostics, which will ultimately drive the supply chain. The prognostic information will be linked via wireless communications to relay needs to maintenance staff and decision-makers. Automatic identification techniques such as Radio Frequency Identification (RFID) will be used to locate parts in the supply chain, all integrated through a secure web portal to acquire and deliver replacement parts quickly on an as-needed basis.

Research is being conducted in the field of algorithm development to analyze, trend, and isolate large-scale multivariate data. Methods like projection pursuit using principal component analysis and support vector machines, Mahalanobis distance analysis, symbolic time-series analysis, neural networks analysis, and Bayesian networks analysis can be used to process multivariate data.

Even though there are advances in certain areas related to prognostics, many challenges still remain. The key issues with regard to implementing PHM for a system of systems include decisions of which systems within the system of systems to monitor, which system parameters to monitor, selection of sensors to monitor parameters, power supply for sensors, on-board memory for storage of sensed data, in situ data acquisition, and feature extraction from the collected data. It is also a challenge to understand how failures in one system affect another system within the system of systems and how it affects the functioning of the overall system of systems. Getting information from one system to the other could be hard, especially when the systems are made by different vendors. Other issues to be considered before implementation of PHM for system of systems are the economic impact due to such a program, contribution of PHM implementation to a condition-based maintenance, and logistics.

The elements necessary for a PHM application are available, but the integration of these components to achieve the prognostics for a system of systems is still in the works. In the future, electronic system designs will integrate sensing and processing modules that will enable in situ PHM. A combination of different PHM implementations for different subsystems of a system of system will be the norm for the industry.

Implementation of PHM: Electronics

As an example, in this section we describe implementation of PHM in an industry that is different from commercial NPPs. This section is intended to provide a reference for how such an advanced PHM system could function. In this example we use application of PHM to the commercial electronic devices industry.

Pecht et al. [126] proposed several measurable parameters that can be used as failure precursors for electronic products, including switching power supplies, cables and connectors, CMOS ICs, and voltage-controlled high-frequency oscillators (see Table 27).

Table 27. Potential failure precursors for electronics.

Electronic Subsystem	Failure Precursor
Switching power supply	• Direct-current (DC) output (voltage and current levels) • Ripple • Pulse width duty cycle • Efficiency • Feedback (voltage and current levels) • Leakage current • Radio frequency (RF) noise
Cables and connectors	• Impedance changes • Physical damage • High-energy dielectric breakdown
CMOS IC	• Supply leakage current • Supply current variation • Operating signature • Current noise • Logic-level variations
Voltage-controlled oscillator	• Output frequency • Power loss • Efficiency • Phase distortion • Noise
Field effect transistor	• Gate leakage current/resistance • Drain-source leakage current/resistance
Ceramic chip capacitor	• Leakage current/resistance • Dissipation factor • RF noise
Electrolytic capacitor	• Leakage current/resistance • Dissipation factor • RF noise
RF power amplifier	• Voltage standing wave ratio (VSWR) • Power dissipation • Leakage current

In general, to implement a precursor reasoning-based PHM system, it is necessary to identify the precursor variables for monitoring and then develop a reasoning algorithm to correlate the change in the precursor variable with the impending failure. This characterization is typically performed by measuring the precursor variable under an expected or accelerated usage profile. Depending on the characterization, a model is developed—typically a parametric curve-fit, neural network, Bayesian network or time-series trending of a precursor signal. This approach assumes that there are one or more expected usage profiles that are predictable and can be simulated, often in a laboratory setup. In some products the usage profiles are predictable, but this is not always true.

For a fielded product with highly varying usage profiles, an unexpected change in the usage profile could result in a different (non-characterized) change in the precursor signal. If the precursor reasoning model is not characterized to factor in the uncertainty in life-cycle usage and environmental profiles, it may provide false alarms. Additionally, it may not always be possible to characterize the precursor signals under all possible usage scenarios (assuming they are known and can be simulated). Thus, the characterization and model development process can often be time consuming and costly and may not always work.

There are many examples of the monitoring and trending of failure precursors to assess health and product reliability. Some key studies are presented below.

Early detection of anomalies in any system or component prevents impending failures and enhances performance and availability. The complex architecture of electronics, the interdependency of component functionalities, and the miniaturization of most electronic systems make it difficult to detect and analyze anomalous behaviors. A Hidden Markov Model-based classification technique determines unobservable hidden behaviors of complex and remotely inaccessible electronic systems using observable signals. Dorg et al. [240] presented a data-driven approach for anomaly detection in electronic systems based on a Bayesian Hidden Markov Model classification technique. The posterior parameters of the Hidden Markov Models are estimated using the conjugate prior method. An application of the developed Bayesian Hidden Markov Model-based anomaly detection approach was presented for detecting anomalous behavior in Insulated Gate Bipolar Transistors using experimental data. The detection results illustrated that the developed anomaly detection approach can help detect anomalous behaviors in electronic systems, which can help prevent system downtime and catastrophic failures.

Unexpected circuit failures in analog circuits during field operation can have severe implications. To address this concern, Vasan et al. [247] developed a method for detecting faulty circuit condition, isolating fault locations and predicting the remaining useful performance of analog circuits. Through successive refinement of circuit's response to a sweep signal, features were extracted for fault diagnosis. The fault diagnostics problem was solved as a pattern recognition problem using kernel methods. From the extracted features, a fault indicator was developed for failure prognosis. Further, an empirical model was developed based on the degradation trend exhibited by the fault indicator. A particle filtering approach was used for model adaptation and remaining useful performance estimation.

Khemani et al. [248] developed a simulation based PHM approach for real-world nonlinear analog circuits that could be implemented without any operational data from the circuit. This approach used design of experiments to estimate the criticality of circuit components. The fault diagnosis of the most critical components was carried out using a deep learning model. Individual deep learning models were used for every critical component to predict their degradation and were further used in circuit RUL estimation.

Measurements based on DC resistance have traditionally been used to monitor the reliability of electronic products. Unfortunately, DC resistance is not useful for detecting intermediate stages between a short and an open, such as a partially degraded interconnect. Under cyclic loading conditions, interconnect degradation is caused by fatigue cracking, which often initiates at the surface where the strain range is maximized. At high operating frequencies, signal propagation is concentrated at the circumferential region of an interconnect due to the skin effect. Therefore, RF impedance analysis offers a more sensitive means of detecting interconnect degradation than DC resistance. The skin effect also has implications for the reliability of electronics used in applications such as radar and telecommunications. The use of higher frequencies will make these circuits increasingly susceptible to performance degradation as a result of small cracks or deformation that would go unnoticed in lower frequency applications. The study [149] demonstrated applications of the skin effect to detect interconnect degradation. Mechanical fatigue tests have been conducted with an impedance-controlled circuit board on which a surface mount component was soldered. During solder joint degradation, simultaneous measurements were performed of DC resistance using the Time Domain Reflectometry (TDR) reflection coefficient as a measure of RF impedance. Two TDR reflection coefficients with different frequency ranges were monitored to evaluate the effect of frequency range on the sensitivity of RF impedance to mechanical degradation. The TDR reflection coefficients were consistently observed to increase in response to early stages of solder joint cracking, while the DC resistance remained constant until the solder joint was completely separated. The TDR reflection coefficient measured over a higher frequency range responded earlier than one with a lower frequency range. This demonstrates that as signal frequencies increases, smaller cracks are capable of producing detectable amounts of signal integrity degradation.

Smith and Campbell [136] developed a Quiescent Current Monitor (QCM) that can detect elevated Iddq current in real time during operation. The QCM performed leakage current measurements on every transition of the system clock to get maximum coverage of the IC in real time. Pecht et al. [137] and Xue and Walker [139] proposed a low-power built-in current monitor for CMOS devices. In the Pecht, et al., study, the current monitor was developed and tested on a series of inverters for simulating open and short faults. Both fault types were successfully detected and operational speeds of up to 100 MHz were achieved with negligible effect on the performance of the circuit under test. The current sensor developed by Xue and Walker enabled Iddq monitoring at a resolution level of 10 pA. The system translated the current level into a digital signal with scan chain readout. This concept was verified by fabrication on a test chip.

GMA Industries [140-141] proposed embedding Molecular Test Equipment (MTE) within ICs to enable them to continuously test themselves during normal operation and to provide a visual indication that they have failed. The molecular test equipment could be fabricated and embedded within the individual IC in the chip substrate. The molecular-sized sensor "sea of needles" could be used to measure voltage, current, and other electrical parameters, as well as sense changes in the chemical structure of integrated circuits that are indicative of pending or actual circuit failure. This research focuses on the development of specialized doping techniques for carbon nanotubes to form the basic structure comprising the sensors. The integration of these sensors within conventional IC circuit devices, as well as the use of molecular wires for the interconnection of sensor networks, is a crucial factor in this research. However, no product or prototype has been developed to date.

Electromagnetic coils are widely used components in a variety of industries and systems, including electric motors, solenoids, transformers, and electromechanical contacts. Studies have shown that solenoid valve electromagnetic coils are components within the valve that are susceptible to failure, with over 50% of solenoid valve failures aused by failures in the electrical coil. Moreover, between 26% and 36% of motor failures are due to electromagnetic coil insulation problems. The failure of electromagnetic coil insulation can lead to catastrophic failure of the coil and subsequently, the component and system in which the coil is used. Yet current methods of fault detection in electromagnetic coils cannot be performed in-situ, relegating diagnostic efforts to times when the equipment is shut down. The low tolerance for such failures in defense products motivates the development and exploitation of the ability to detect and forecast electromagnetic coil insulation degradation and failure in-situ. Prior work in the AC motor community on twisted pairs of magnet wire and motor coils has shown that coil impedance measurements can reveal useful diagnostic information. However, there are discrepancies between many studies in the AC motor community regarding the impedance behavior of insulation as it degrades. Furthermore, due to differences in environmental loading conditions, the ability to adaptively locate frequencies where impedance better reflects the health state of the insulation can be enormously useful. For diagnostic and prognostic capabilities to be fully realized, an experimental and theoretical foundation must be established. In [150], the author seeks to experimentally confirm the use of impedance as a health indicator and quantify its use in terms of: a) which frequencies of impedance measurement best reflect the health of the insulation; b) how the environmental loading conditions affect the migration patterns of the impedance measurements; and c) how the impedance measurements reflect the chemical and mechanical changes at work as the insulation degrades. Therefore, ageing experiments will be conducted by testing coils, while measuring impedance spectra, and periodically removing some coils to perform Fourier Transform Infrared (FTIR) spectroscopy and nanoindentation tests on the insulation. This study will deliver a data-driven method for detecting and forecasting failures in electromagnetic coil insulation and will relate the data-driven method with a physics-of-failure understanding of the underlying degradation phenomena.

Cannich and Mamat-Ibrahim [142] developed an algorithm for health monitoring of voltage source inverters with pulse width modulation. The algorithm was designed to detect and identify transistor open-circuit faults and intermittent misfiring faults occurring in electronic drives. The mathematical foundations of the algorithm were based on discrete wavelet transform (DWT) and fuzzy logic (FL). Current waveforms were monitored and continuously analyzed using DWT to identify faults that may occur due to constant stress, voltage swings, rapid speed variations, frequent stop/start-ups, and constant overloads. After fault detection, “if-then” fuzzy rules were used for very large scale integrated (VLSI) fault diagnosis to pinpoint the fault device. The algorithm was demonstrated to detect certain intermittent faults under laboratory experimental conditions.

Self-Monitoring Analysis And Reporting Technology (SMART), currently employed in select computing equipment for Hard Disk Drives (HDD), is another example of precursor monitoring [143]. HDD operating parameters, including the flying height of the head, error counts, variations in spin time, temperature, and data transfer rates, are monitored to provide advance warning of failures (see Table 28). This is achieved through an interface between the computer’s start-up program (basic input/output system, BIOS) and the HDD. Anomaly detection in HDDs is crucial for users to prevent data loss and to backup their data. A fusion approach was proposed to monitor the HDD health status based on Mahalanobis Distance (MD) and Box-Cox transformation [239]. A quality control technique-Shewhart control chart - was introduced using the transformed MD values to detect the anomalies in HDDs.

Table 28. Monitoring parameters based on reliability concerns in hard drives.

Reliability Issues	Parameters Monitored
• Head assembly - Crack on head - Head contamination or resonance - Bad connection to electronics module • Motors/bearings - Motor failure - Worn bearing - Excessive run-out - No spin • Electronic module - Circuit/chip failure - Interconnection/solder joint failure - Bad connection to drive or bus • Media - Scratch/defects - Retries - Bad servo - ECC corrections	• Head flying height: A downward trend in flying height will often precede a head crash. • Error checking and correction (ECC) use and error counts: The number of errors encountered by the drive, even if corrected internally, often signals problems developing with the drive. • Spin-up time: Changes in spin-up time can reflect problems with the spindle motor. • Temperature: Increases in drive temperature often signal spindle motor problems. • Data throughput: Reduction in the transfer rate of data can signal various internal problems.

Systems for early fault detection and failure prediction are being developed using variables such as current, voltage, and temperature continuously monitored at various locations inside the system. Along with sensor information, soft performance parameters such as loads, throughputs, queue lengths, and bit error rates are tracked. Prior to PHM implementation, characterization is conducted by monitoring the signals of different variables to establish a Multivariate State Estimation Technique (MSET) model of the “healthy” systems. Once the healthy model is established using these data, it is used to predict the signal of a particular variable based on learned correlations among all variables [144]. Based on the expected variability in the value of a particular variable during application, a Sequential Probability Ratio Test (SPRT) is constructed. During actual monitoring, SPRT is used to detect deviations of the actual signal from the expected signal based on distributions (and not on a single threshold value) [145-146]. This signal is generated in real time based on learned correlations during characterization (see Figure 62). A new signal of residuals is generated, which is the arithmetic difference of the actual and expected time-series signal values. These differences are used as input to the SPRT model, which continuously analyzes the deviations and provides an alarm if the deviations are of concern [144]. The monitored data are analyzed to provide alarms based on leading indicators of failure and enable use of monitored signals for fault diagnosis, root cause analysis, and analysis of faults due to software ageing [147].

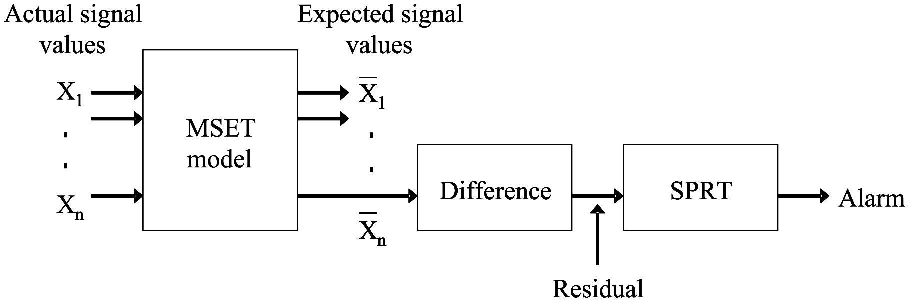


Figure 62. Sun Microsystems' approach to PHM.

Brown et al. [148] demonstrated that the remaining useful life of a commercial Global Positioning System (GPS) can be predicted by using a precursor-to-failure approach. The failure modes for GPS included precision failure due to an increase in position error and solution failure due to increased outage probability. These failure progressions were monitored in situ by recording system-level features reported using the national marine electronics association (NMEA) protocol 0183. The GPS was characterized to collect the principal feature value for a range of operating conditions. Based on experimental results, parametric models were developed to correlate the offset in the principal feature value with solution failure. During the experiment, the BIT provided no indication of an impending solution failure [148].

PHM Applications: Bearings

Bearing faults are the main contributors to the failure of electric motors. Electric motors have been used in various industrial sectors to convert electrical energy to mechanical energy. Different sources have demonstrated that motor bearing failure is the top reason that electric motor fails. The dynamic nature of the development of bearing faults poses a challenge for fault detection. Signals that provide efficient monitoring include vibration signals, motor current signals, acoustic emission signals. Vibration signals have been widely used because of their widespread availability and sensitivity to bearing faults. Usually, raw signals are not adequate to identify the existence of a fault; therefore, fault features are extracted from the time domain, frequency domain, or time-frequency domain analysis. Vibrations signals are nonstationary and hence time-frequency domain methods, such as wavelet analysis and Spectral Kurtosis (SK) analysis, are able to process both stationary and nonstationary signals. SK allows the identification of the frequency band that contains faulty bearing information by detecting impulse series generated by the faulty bearing. However, some other vibration sources, such as gearboxes, also generate impulse series. As a result, the frequency band detected by SK may not be the one that contains the faulty bearing information. Tian et al. [98] presented a method that detected bearing faults and monitors the degradation of bearings in electric motors. Based on SK and cross correlation, the method extracted fault features that represent different faults, and the features were then combined to form a health index using Principal Component Analysis (PCA) and a semi-supervised K-Nearest Neighbor (KNN) distance measure. The method is able to detect incipient faults and diagnose the locations of faults under masking noise. It also provides a health index that tracks the degradation of faults without missing intermittent faults.

Rolling element bearing faults have an amplitude-modulating effect on their characteristic frequencies and hence sub-band analysis was used to determine an optimal sub-band signal that contains intrinsic information about bearing faults. Hence, a bearing abnormality index (BAI) that properly quantifies how much information a sub-band signal contains about bearing faults was also developed.

He at al. [245] proposed a vibration-based health monitoring approach for cooling fans using a wavelet filter for early detection of faults in fan bearings and for the assessment of fault severity. To match the wavelet filter to the fault characteristic signal, a fuzzy rule was introduced to maximize the amplitudes of Bearing Characteristic Frequencies (BCFs), which are an indicator of bearing faults. The sum of the amplitudes of BCFs and their harmonics (SABCF) was used as an index to capture the bearing degradation trend.

Lee et al. [246] conducted a feasibility study to diagnose faults in automotive safety components that are subjected to abnormal vibrations. Four deep learning approaches were developed and evaluated in terms of their suitability for embedding inside a vehicle. As a result, all four architectures were trained and executed on a Raspberry Pi to replicate the expected computational power of the embedded system.

Sometimes situations are encountered where the vibration data available is of insufficient frequency and/or the accelerometer is installed away from where the bearings. CALCE has also explored using fusion prognostics-based methods for RUL estimation of elastomeric bearings in a rotor bearing damper system. Health and Usage Monitoring (HUMS) data consisting of 25 parameters was provided by the manufacturer of the system. The HUMS data available for the project were primarily loading data, <u>not</u> health indicators (i.e., there were no data that indicate the condition of the bearings, only the loads placed on the aircraft). The analysis was further complicated because all the monitoring sensors were physically removed from the bearings and the sampling frequency was 1Hz rendering traditional vibration analysis infeasible. Several data-driven and physics-based approaches were explored to find correlations between the bearing lifetimes and the data from the HUMS parameters; however, none of these approaches led to a significant negative correlation with the life of the bearings as one would expect if lifetime were determined by damage accumulation as a result of the continued application of loads (i.e., if failure were due to a wearout mechanism such as fatigue). To overcome this obstacle, genetic programming was used to construct a feature that had a negative correlation between the bearing life and the cumulative density of excursions of HUMS parameters. A similarity-based model was used to predict the RUL of bearings, where the bearings with the most similar degradation trends formed the basis for the RUL prediction. Similarity-based model makes the use of health indicators constructed using physics of failure approaches and hence is a fusion prognostics approach taking advantage of both physics of failure and data driven approaches.

PHM in the Internet of Things (IoT) Era

The smart, connected elements of IoT require an appropriate technology infrastructure. This infrastructure is represented as a "technology stack" and is shown in Figure 63. A technology stack facilitates data exchange between the system and the user, integrates data from business systems and external sources, serves as the platform for data storage and analytics, runs applications, and safeguards access to systems and the data flowing to and from them [127]. The elements associated with the system are described by the lower half of the technology stack. There are two parts, software and hardware. One of the evolutions currently underway is the addition of embedded sensors, RFID tags, and processors, built into the system. Collectively this enables new data to be collected for PHM. These data need to be transmitted and therefore network connectivity shown in the central block is a key feature of the IoT paradigm. The data collected and transmitted have to be stored and processed in an efficient and interpretable way. This is increasingly being done using cloud computing services represented by the top block in the technology stack. The people who access the results of the analysis as well as those involved in the development and maintenance of the technology stack elements and the models it supports are denoted by the user. On either side to the stack there are blocks that identify the importance of authentication and security at all levels in the technology stack as well as the potential relationships with other systems and sources of information.

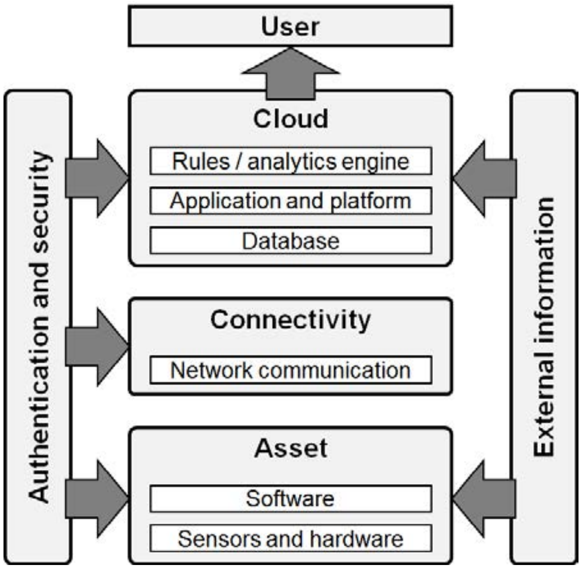


Figure 63. Technology stack for supporting IoT.

The following section considers how IoT has been and will be applied in the near future for PHM applications in different industrial sectors.

IoT-Enabled PHM in Manufacturing

Manufacturing is a major source of economic benefit in many countries. The manufacturing industry has traditionally focused on product quantity for mass production. In order to strengthen competitiveness, the manufacturing paradigm is now shifting towards combining sales with maintenance services enabled by IoT. There is a significant shift underway from a focus on products alone to a focus on platforms. A company's product operates as a facilitator and the product's value is created by the participants instead of the company itself in a platform approach. Examples include platform-based businesses such as Apple, Uber, and AirBnB. A prerequisite for a successful platform is a company's ability to build a value proposition around an ecosystem and not only around its own products.

In the manufacturing industry, Industrie 4.0 and its associated Smart Factory program are initiatives of the German government to assist in the development of cyber-physical platforms that enable IoT developments [128]. Cyber-physical platforms change the traditional manufacturing processes by integrating devices, equipment, and platforms in a factory, connecting factory-to-factory and integrating operational and information technologies. Examples of platforms that support these ideas include the GE Predix platform [129] and SAP Hana [130].

IoT-Enabled PHM Applications: Energy Generation

The energy-generation industry consists of nuclear, thermal power, and renewable energy. Thermal power (oil, coal, and natural gas) generates 81.4% of the world's supply, biofuels 10.2%, nuclear 4.8%, hydro 2.4%, and renewables (geothermal, wind, and heat) 1.2% [131].

Power generation is a significant contributor to CO_2 emissions, responsible for about 50% of total global emissions of this gas. Hence, significant effort is going into improving the efficiency of generation and distribution. Cloud computing is enabling the development of so-called smart grid computing. Smart grids use large numbers of networked sensors, power electronic devices, distributed electricity generators, and communications appliances. Integration of a large quantity of real-time information and data processing is required and as a result, the electric grid is becoming smarter and more complex [132]. IoT-based PHM is an integral part of a smart grid as engineers seek to monitor the health of key components in the network.

Renewable energy includes wind, hydro, solar, and biofuel energy generation. Among these, wind energy generation often encounters reliability issues. In order to deliver desired capacity, wind power plants often require long blades and high towers, which increase the load and stress, and which may eventually cause wind turbine failure. Many wind farms are located in remote locations, such as offshore or on a mountain, where accessibility is limited. A number of organizations, for example, GE (Digital Wind Farm) and Siemens (Wind Service Solutions), now provide IoT service solutions for wind farms. These solutions aim to optimize turbine performance and equipment life by using RUL estimation models to predict maintenance requirements [133].

IoT-based PHM in the energy-generation industry can change the maintenance paradigm by supporting the use of more CBM. It can increase plant reliability and availability, stabilize the power supply with less power interruption, and eventually provide the industry with a good reputation and trust. In addition, IoT-based PHM plays a role in ensuring that ageing power infrastructure is appropriately monitored for unplanned failures and that deteriorated assets are replaced at cost- and risk-effective intervals.

IoT-Enabled PHM Applications: Transportation and Logistics

IoT is playing an increasing role in the transportation and logistics industries as more physical objects are equipped with barcodes, RFID tags, and sensors. Transportation and logistics companies now conduct real-time monitoring as they move physical objects from an origin to a destination across their supply chain. The ability to predict failures has been enhanced using the ability to see how long an item has been in storage and under what conditions (e.g., heat, vibration, humidity, and contaminating environments) from an IoT-based PHM perspective. An asset may undergo several loading conditions or even fail during transportation and storage due to unexpected exposure to mechanical shock and vibration, cosmic radiation, or being in a too dry, wet, or humid environment.

Commercial aviation spends more than 50% of its total expenses on maintenance, repair, and operations [134]. Aircraft component failure results in significant loss of safety, profit, as well as reputation. Integrated Vehicle Health Management (IVHM) is a unified system that assesses the current and future states of vehicles and has evolved over the last 50 years [135]. IVHM with PHM capability has the potential to influence aircraft design by reducing system redundancy, resulting in fewer subsystems and modules on an aircraft. IoT-based PHM application in aviation can reduce unplanned maintenance and no-fault-found events and can improve aircraft availability and safety.

IoT-Enabled PHM Applications: Automobiles

The automobile industry is driving innovation in the application of technology that enables consumers to get advanced notice of problems with their vehicles as well as real-time diagnostics support. For example, cars made by General Motors, Tesla, BMW, and other manufacturers now have their own Application Programming Interfaces (APIs). The APIs allow applications built by third parties to interface with the data collected on the car. This enables the development of applications for IoT-based PHM that add value by increasing connectivity, availability, and safety.

Enabling real-time navigation, remote vehicle control, self-diagnosis, and in-vehicle infotainment service, IoT allows "smart" cars in the field to connect to the network. Smart cars can connect to other cars, as well as infrastructure, to share their route information for efficient route planning. Smart cars are evolving as a connected device, and in the future users may be able to purchase mobility through a driverless car network rather than having to own a car. The reliability of a future smart car network will depend on appropriate use of IoT-based PHM. Just so that unplanned in-service failures, which may affect the car network performance, can be avoided, cars with deteriorating health will need to be scheduled out of the system.

IoT-Enabled PHM Applications: Medical Consumer Products

Medical devices are another area where consumer needs are increasing, and the consequences of the failures can be critical. For example, failures of in-vivo devices, such as pacemakers, can cause patient death. Medical devices can fail due to battery performance degradation. Patients with pacemakers are required to check at a fixed-time interval to ensure the device is functioning correctly. IoT-based PHM allows medical consumer products to be monitored and diagnosed continuously and remotely, and therefore can help these patients by reducing the number of intervals required for regular checking. IoT-based PHM of medical devices can also facilitate remote patient monitoring, homecare service for the elderly, and chronic disease management [136].

IoT-Enabled PHM Applications: Warranty Services

Conventionally, customers seek warranty services when their assets fail. However, seeking a remedy to failure after the failure has occurred is inconvenient and expensive for both the customers and maintainers. The customer loses operational availability, and the maintainers must conduct corrective maintenance, which is generally more expensive than predictive maintenance due to collateral damage, scheduling, diagnosis, and spare parts availability. In addition, waiting until an asset fails can pose safety (and liability) issues.

Figure 64 overviews a predictive warranty service, where the asset is one that the customer has a significant investment in and for which the operational availability of the asset serves a critical function (e.g., cars and aircraft). The inclusion of IoT-based PHM into warranties can augment the customer's ability to make a decision about whether to seek warranty service prior to asset failure by offering useful information, such as the onset of the asset's degradation, type of failure, and RUL. Consequently, the IoT based PHM can facilitate effective logistical support by showing where and how the customer's asset is degrading.

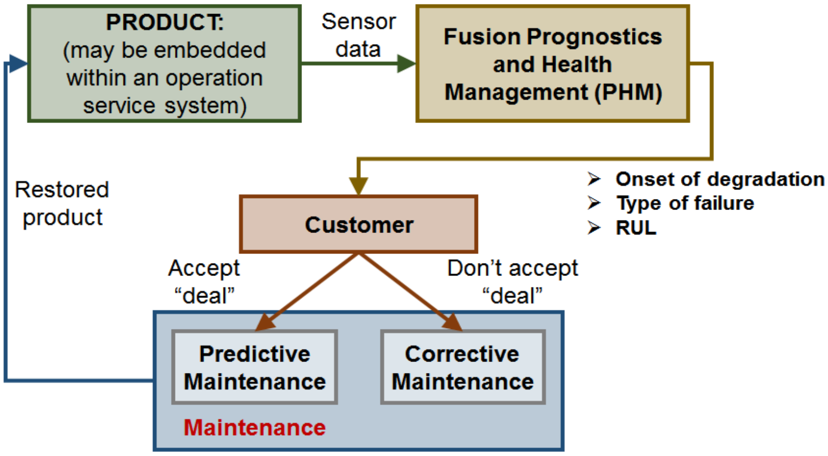


Figure 64. Inclusion of IoT-based PHM in predictive warranty service [110].

IoT-Enabled PHM Applications: Robotics

IoT enables robots to connect to other robots and devices. FANUC's Intelligent Drive Link Drive (FIELD) system is an example of IoT-based PHM. It is a platform that connects not only robots, but also peripheral devices and sensors. FANUC is collaborating with Cisco, Rockwell Automation, and Preferred Networks to establish the platform. IoT expands the definition of robots from simple task performers to autonomous ones with self-learning abilities. This transformation has the potential to make robots play a vital role in interacting with humans. IoT-based PHM can be a key technology for autonomous robots. It enables robots to diagnose themselves based on collecting data and artificial intelligence technologies as a self-cognizant electronic system.

Appendix M

MBSE ARCHITECTURE OF RI-PSH

SysML Language for MBSE

The chosen language for the initial testing/development of this plant MBSE architecture has been SysML[c] [153] since it provides more functionalities when compared to standard UML language. SysML in particular, supports the specification, analysis, design, verification and validation of systems that include hardware, software, data, personnel, procedures and facilities. From a practical perspective, an MBSE model described by SysML is composed by a set of diagrams that operates on different levels and different dimensions. Each diagram represents an element of the considered model. Note that SysML is not a methodology per se but it is, instead, a visual modeling language that provides the following capabilities to the modeler:

- Semantics/syntax: high level abstract representation of a system by employing different classes of diagrams
- Notation: a representation of such system representation

SysML is based on four main "pillars", i.e., four main types of diagrams (see Figure 65):

1. *Structure*: which specifies the internal structure of a model though blocks and how these blocks are being used
2. *Behavior*: which specifies (e.g., by employing a state machine formalism) the interactions and functions of the blocks defined in 1.
3. *Requirements*: which specifies the properties and boundaries required by each block defined in 1. in order to perform the behaviors defined in 2.
4. *Parametrics*: which specifies the mathematical model (e.g., time dependent dynamics) of each block defined in 1. based on the requirements defined in 3.

Figure 66 shows in a graphical form the full list of diagrams available in SysML and their dependencies. The diagrams highlighted in dashed line are the ones that have been added or expanded from UML.

Operational Context for RI-PSH

The starting point for the design of the RI-PSH architecture is the definition of a hypothetical NPP organizational chart as shown in Figure 67. For the scope of this report we are considering not only maintenance and equipment reliability but also other plant divisions such as procurement. These plant divisions are not independent from each other but are coupled to each other with different degrees of coupling.

[c] http://www.omgsysml.org/

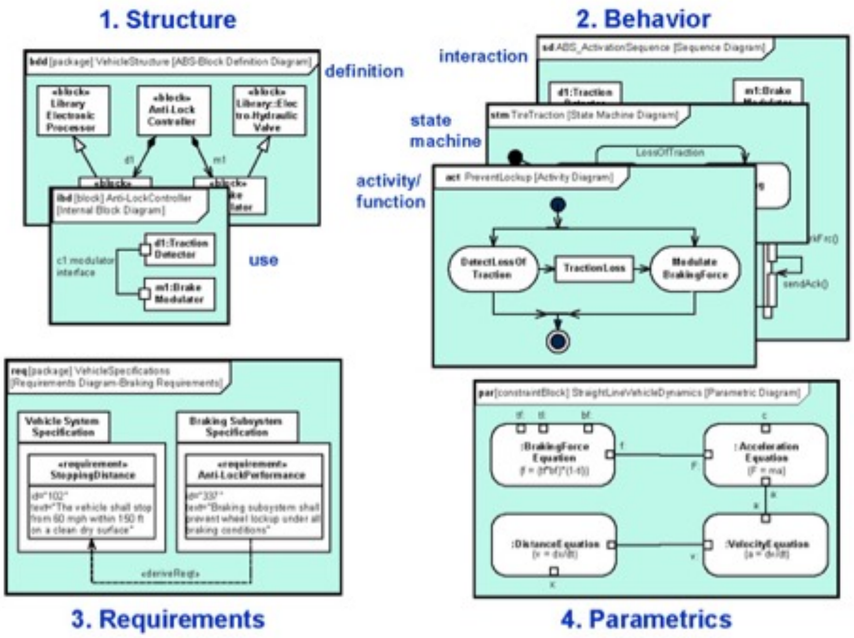

1. Structure
bdd [package] VehicleStructure [ABS-Block Definition Diagram]
«block» Library Electronic Processor
«block» Anti-Lock Controller
«block» Library::Electro-Hydraulic Valve
d1
m1
definition
ibd [block] Anti-LockController [Internal Block Diagram]
c1 modulator interface
d1:Traction Detector
m1:Brake Modulator
use
2. Behavior
interaction
sd ABS_ActivationSequence [Sequence Diagram]
d1:Traction
m1:Brake
state machine
stm TireTraction [State Machine Diagram]
LossOfTraction
activity/ function
act PreventLockup [Activity Diagram]
DetectLossOf Traction
TractionLoss
Modulate BrakingForce
sendAck()
req [package] VehicleSpecifications [Requirements Diagram-Braking Requirements]
Vehicle System Specification
«requirement» StoppingDistance
id="102"
text="The vehicle shall stop from 60 mph within 150 ft on a clean dry surface"
Braking Subsystem Specification
«requirement» Anti-LockPerformance
id="337"
text="Braking subsystem shall prevent wheel lockup under all braking conditions"
«deriveReqt»
3. Requirements
par [constraintBlock] StraightLineVehicleDynamics [Parametric Diagram]
tf: tl: bf:
:BrakingForce Equation
{f = (tf*bf)*(1-tl)}
f
F:
c
:Acceleration Equation
{F = ma}
a
:DistanceEquation
{v = dx/dt}
:VelocityEquation
{a = dv/dt}
v:
x
4. Parametrics

Figure 65. Graphical representation of SysML "pillars" [153].

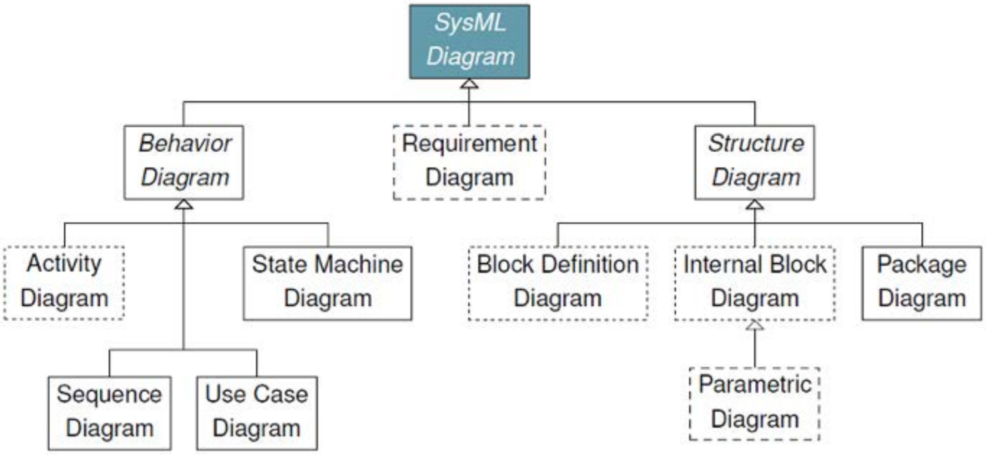


Figure 66. Graphical representation of SysML diagrams [153].

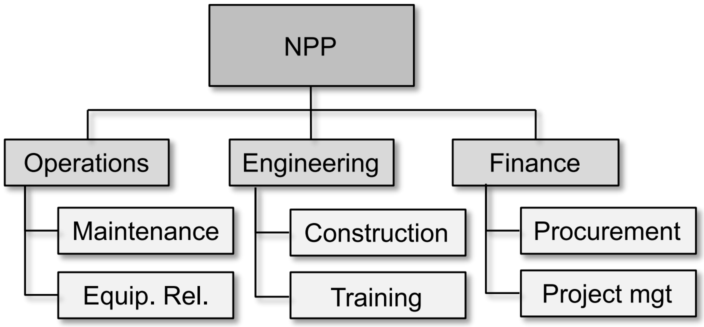


Figure 67. Example of NPP organzuational chart.

Regarding equipment reliability and maintenance divisions we have shown in Figure 68 how equipment reliability and maintenance are coupled to each other. In this figure, incident/event reports and online streaming data are employed to determine plant health and manage maintenance activities, i.e., work orders (see Figure 69 and Figure 70). By employing existing PRA models, plant health data are used to determine the plant risk profile.

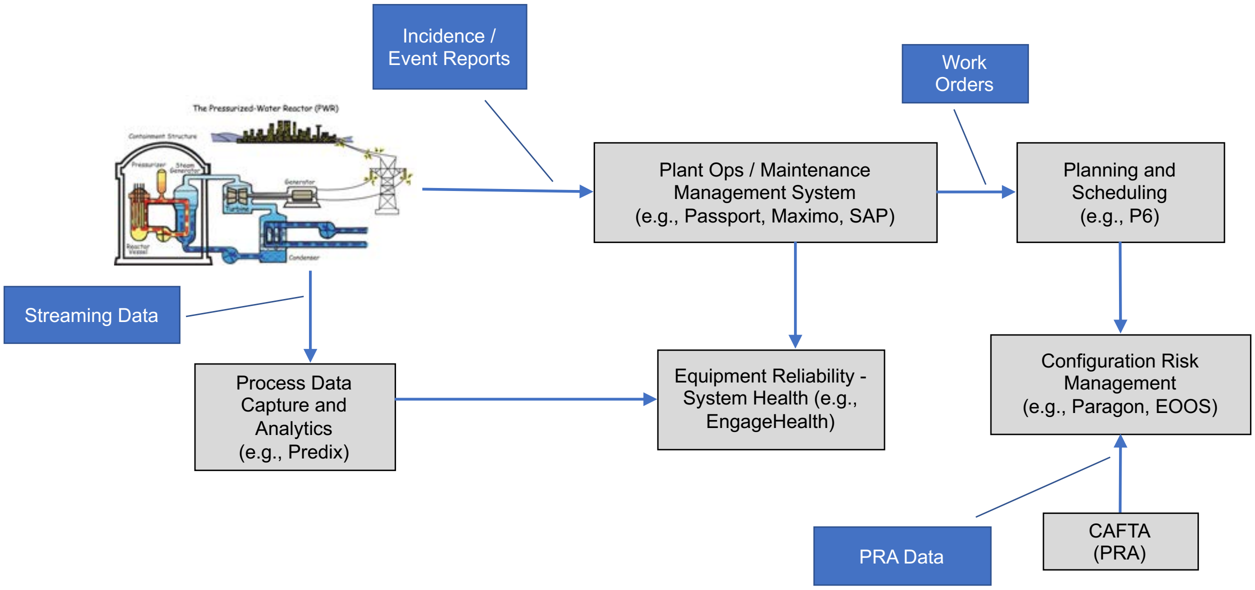

Incidence / Event Reports
Work Orders
The Pressurized-Water Reactor (PWR)
Containment Structure
Pressurizer
Steam Generator
Generator
Turbine
Reactor Vessel
Condenser
Plant Ops / Maintenance Management System (e.g., Passport, Maximo, SAP)
Planning and Scheduling (e.g., P6)
Streaming Data
Process Data Capture and Analytics (e.g., Predix)
Equipment Reliability - System Health (e.g., EngageHealth)
Configuration Risk Management (e.g., Paragon, EOOS)
PRA Data
CAFTA (PRA)

Figure 68. Hypothetical structure of plant equipment maintenance and equipment reliability workflow.

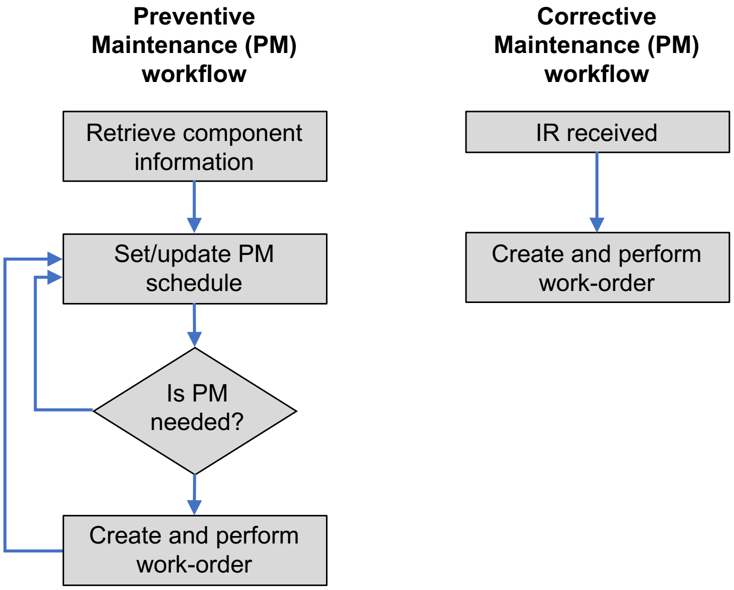

Preventive Maintenance (PM) workflow
Retrieve component information
Set/update PM schedule
Is PM needed?
Create and perform work-order
Corrective Maintenance (PM) workflow
IR received
Create and perform work-order

Figure 69. Examples of workflow for CM and PM.

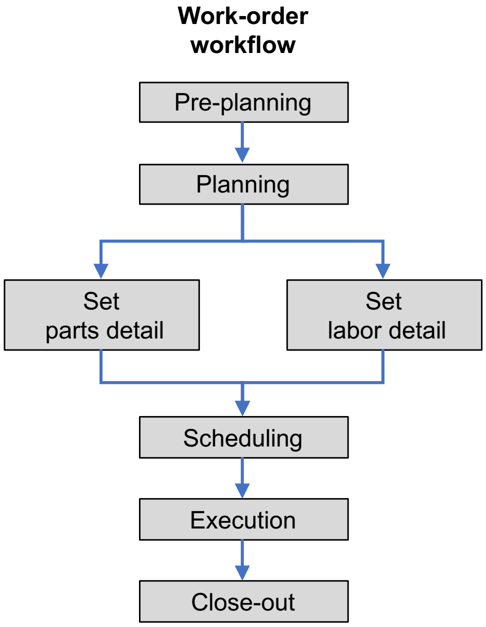


Figure 70. Workflow for plant maintenance work-orders.

The proposed RI-PSH architecture is employing (see Figure 71):

- Data: plant online streaming data but also recovered data at the fleet and industry level
- Models:
    - System model: these models can be either stochastic (e.g., reliability or ageing models for specific components/systems) or deterministic (e.g., system behavior models such as finite state machines, petri nets)
    - System simulators: these models employ simulation-based codes (e.g., RELAP5-3D) to emulate system behavior under different initial/boundary conditions.
    - Engine methods: methods that based on new data:
        - determine plant health parameter and update current pant operations (e.g., component PM intervals) – PHM function
        - forecast plant behavior and update component life-cycle operations (e.g., component replacement strategy) – RIAM function

Initial Design for RI-PSH Architecture

From a MBSE perspective the first modeling step is the definition of the use case for the system under consideration. For the RI-PSH, we have identified 6 main actors:

1. Actual generating station, i.e., plant which provides actual SSC activities
2. Set of databases at the plant/fleet/industry levels which provide extensive operating history knowledge (e.g., failure and maintenance reports)
3. Reactor operators (including sources such as electronic logs and surveillance data)
4. Plant equipment reliability operators/managers
5. Maintenance crews
6. Plant procurement office

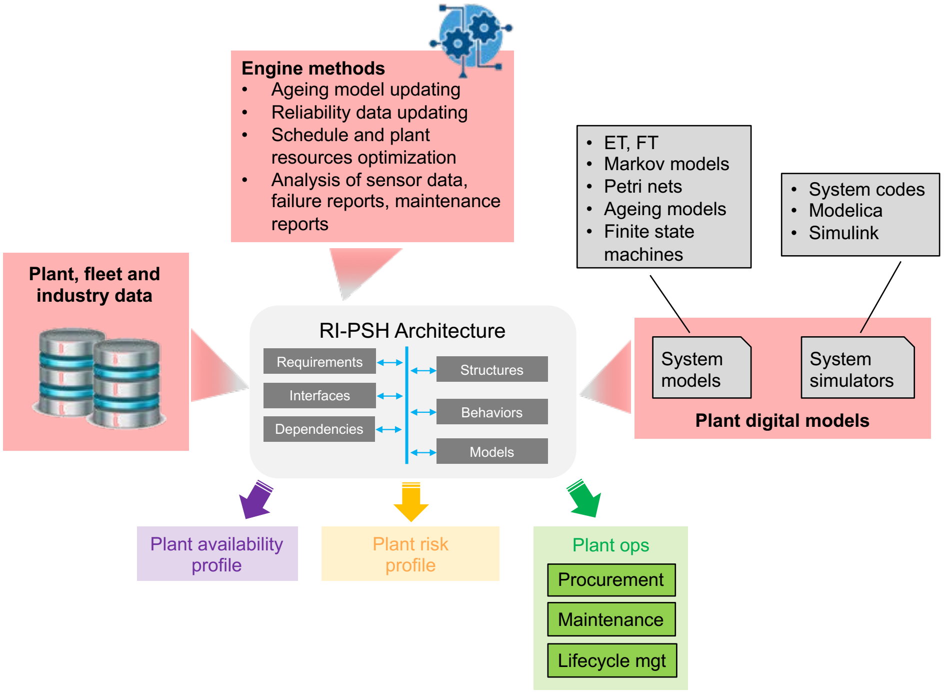


Figure 71. Elements for the proposed RI-PSH architecture.

Figure 72 shows the interactions and the functionalities provided by RI-PSH to the actors listed above. Note that Figure 72 explicitly includes not only PHM (e.g., maintenance related) but also RIAM (e.g., SSC life-cycle related) functionalities.

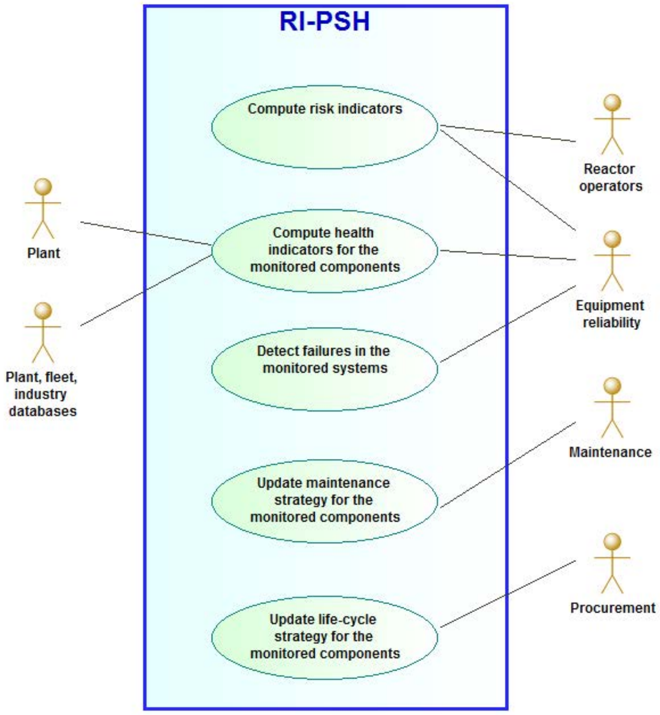

RI-PSH
Compute risk indicators
Compute health indicators for the monitored components
Detect failures in the monitored systems
Update maintenance strategy for the monitored components
Update life-cycle strategy for the monitored components
Plant
Plant, fleet, industry databases
Reactor operators
Equipment reliability
Maintenance
Procurement

Figure 72. Use case diagram for the RI-PSH.

Figure 73, provides more details about the internal structure diagram of the RI-PSH by indicating the main modules designed to provide the functionalities shown in Figure 72. Figure 74 [155] goes more into the details of the PHM module shown in Figure 73.

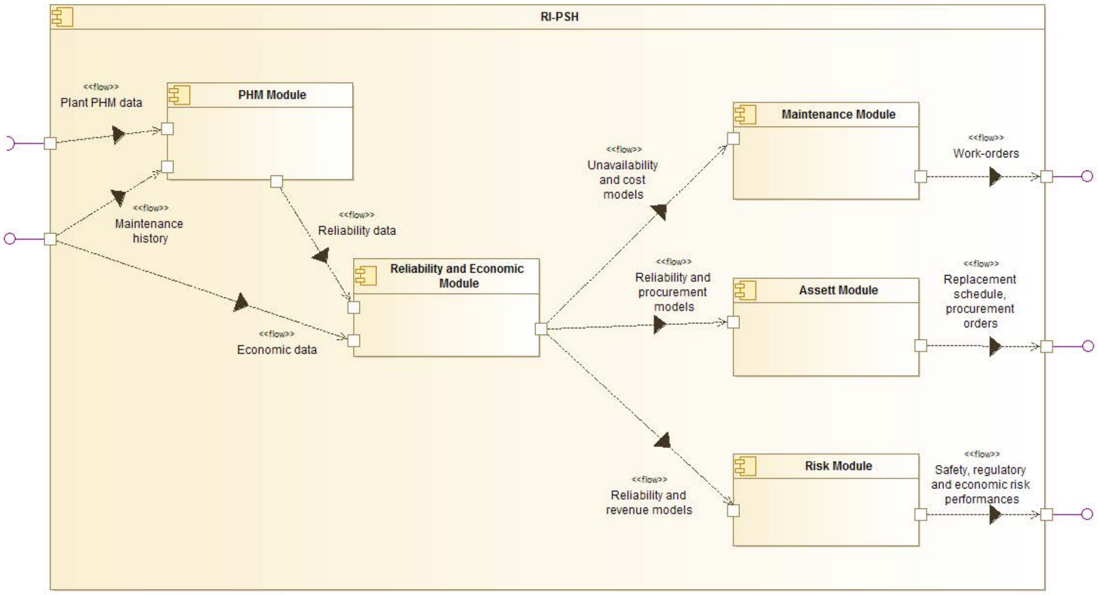

RI-PSH
<<flow>>
Plant PHM data
PHM Module
<<flow>>
Maintenance history
<<flow>>
Reliability data
Reliability and Economic Module
<<flow>>
Economic data
<<flow>>
Unavailability and cost models
Maintenance Module
<<flow>>
Work-orders
<<flow>>
Reliability and procurement models
Assett Module
<<flow>>
Replacement schedule, procurement orders
<<flow>>
Reliability and revenue models
Risk Module
<<flow>>
Safety, regulatory and economic risk performances

Figure 73. Internal diagram in SysML for the RI-PSH.

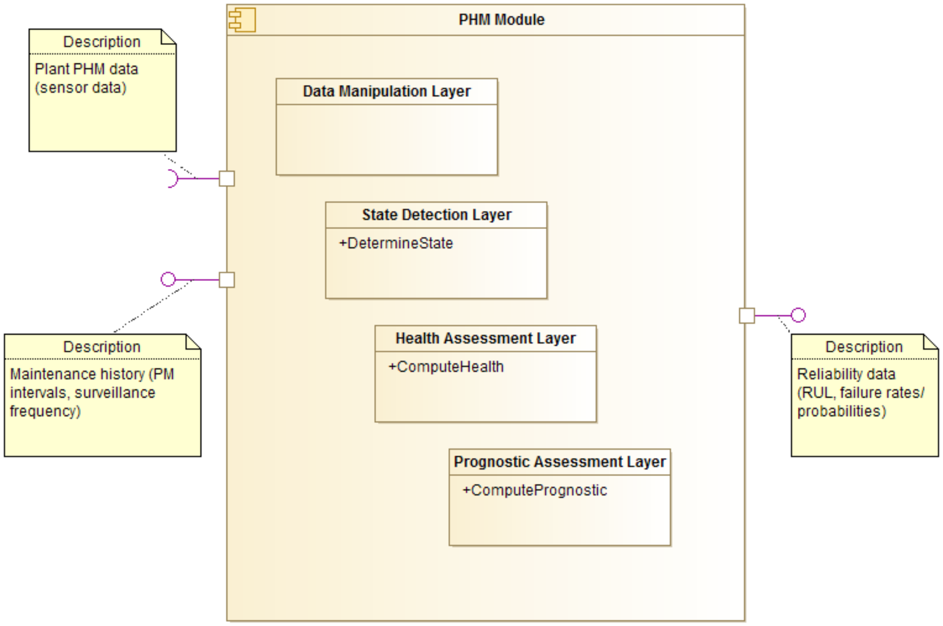

Description
Plant PHM data (sensor data)
PHM Module
Data Manipulation Layer
State Detection Layer
+DetermineState
Health Assessment Layer
+ComputeHealth
Prognostic Assessment Layer
+ComputePrognostic
Description
Maintenance history (PM intervals, surveillance frequency)
Description
Reliability data (RUL, failure rates/ probabilities)

Figure 74. SysML internal diagram for the PHM module [155].

Appendix N

VIEWING GENERATION RISK ASSESSMENT MODELS IN SUCCESS SPACE

When applying logic modeling software, it is common to work in failure space to generate and quantify scenarios that yield adverse consequences (such as minimal cut sets). There are good reasons for doing this. But once this is done, in many applications, there are also good reasons to turn the result around, and view it in success space. In many applications, much is to be learned from a success-space perspective. For example:

- In formulating a safety case for a hazardous facility, it is beneficial to do "prevention analysis" in order to identify combinations of success paths that (together) provide needed levels of functional reliability, required redundancy, required diversity, … . See, for example, reference [17].
- If something goes wrong, and we need to compensate for it lest we lose the function, it is useful to understand what success paths remain available, and which of them are more reliable than the others.

This section looks at GRA Modeling (as exemplified by [157]) with a view to applying success-space thinking in that context.

We begin with some comments about modeling simple series / parallel systems. Next, we review some key aspects of generation risk assessment, beginning with quantification, and then moving on to the way one popular implementation of "unavailability" metrics is carried out in logic model software. Finally, we point out what has to be done to the results from a model of that kind, before it can be interpreted in success space.

Series / Parallel Systems

The following considerations drive much of what goes on in GRA:

- While safety systems are redundant, and sometimes have complicated interdependencies on support systems, much of "generation" has much less redundancy; as a result, the logic models are much simpler. However, capitalizing on whatever redundancy exists is a key part of risk management.
- Quantification is a much different matter in GRA. We are not comparing E-5 CDF contributors to E-7 CDF contributors; we are comparing E-1 unavailability contributors to E-15 unavailability contributors.

Figure 75 shows a notional reliability block diagram for a topologically simple system that is not unlike some of the systems involved in generation risk: for some purposes, we can think of it as mostly being a series system. This diagram is not meant to be a good physical description of the system; it is simply meant to illustrate what is required for functional success. According to this diagram, we need for all of blocks A-E to succeed, and we need for F and G to succeed. F succeeds if either F1 succeeds or F2 succeeds, and similarly for G.

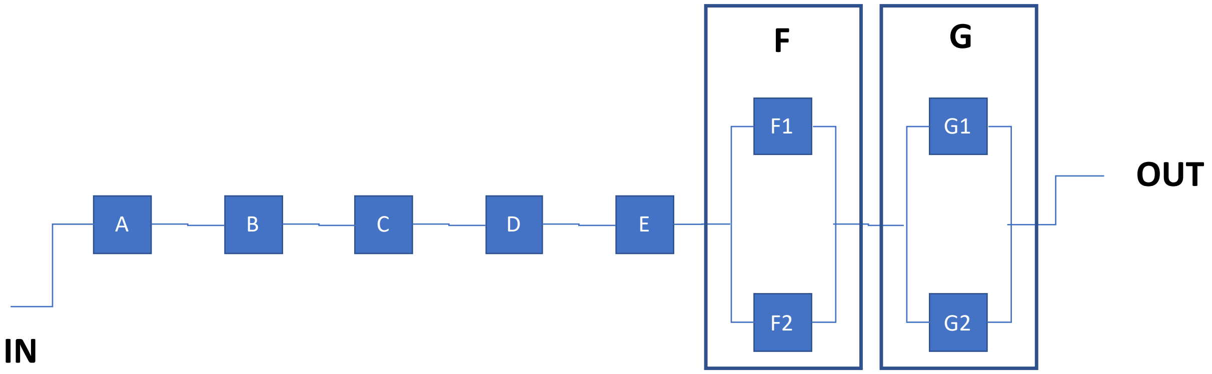


Figure 75. Reliability block diagram for a simple system.

At the level of abstraction shown in the figure, and assuming that there is no functional commonality between any of the blocks, we can write down the minimal cut sets and the minimal path sets by inspection:

Cut Sets: A+B+C+D+E+F1*F2+G1*G2,

Path Sets: /A*/B*/C*/D*/E*(/F1 + /F2)*(/G1+/G2),

where:

- * means the logical "AND,"
- + means the logical "OR,"
- An unmodified letter (A, C, …) means "failure of the indicated block,"
- "/" means "NOT."

Thus, "A" means "Failure of A," "/A" means "NOT Failure of A" (i.e., "Success of A").

From Figure 75, blocks A-E are always needed; failure of any of these blocks represents failure of the function (e.g. plant trip is this represents systems needed for plant generation). Block F causes a trip if and only if both of its elements fail, and similarly for Block G.

In an essentially series system, the most unavailable block in the system limits the availability that is achievable. For example, if the unavailability of C is 0.9, then the system unavailability cannot be less than 0.9, no matter what we do to the other blocks.

Quantification of Unavailability

If the system were simply either "up" or "down," we could use an expression like the above cut set expression to quantify unavailability, which (by definition) would refer to the amount of time spent in the "down" state.

If individual block contributions to unavailability are small enough that they will not occur simultaneously, we can sum the contributions to estimate the total unavailability, and we can model each one within the following approximation.

Consider the state diagram shown in Figure 76, showing "UP" and "DOWN" states for a single component, and arcs representing that component going into the "DOWN" state (i.e., "failed"), and being repaired and restored to the "UP" state.

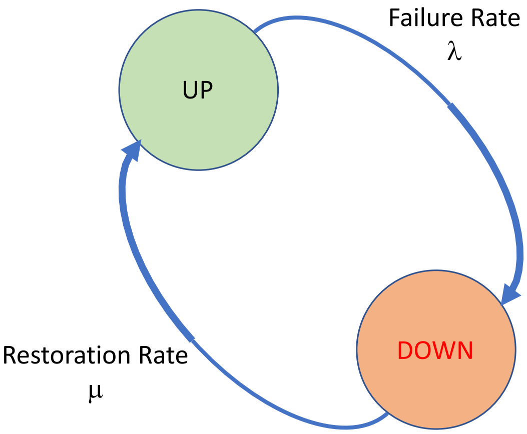


Figure 76. Two state Markov models for a single component.

The arc from "UP" to "DOWN" represents the component going bad ("DOWN"); the rate of this transition is the failure rate λ. The arc from "DOWN" to "UP" represents restoration of the component to being good again ("UP"). We can attribute probabilities to these states; the probability of being in the UP state, P(UP) is the availability, and P(DOWN) is the unavailability. Moreover, within classical reliability theory, we can model the time dependence of these states using the following equations:

$$\frac{dP(DOWN)}{dt} = \lambda(t)P(UP) - \mu(t)P(DOWN) \tag{N.1}$$

$$\frac{dP(UP)}{dt} = -\lambda(t)P(UP) + \mu(t)P(DOWN) \tag{N.2}$$

$$P(UP) + P(DOWN) = 1 \tag{N.3}$$

If λ and μ are constant, a system like this will evolve to a steady state, in which the average rate of actual failures ($\lambda * P(UP)$) is balanced by the average rate of actual restorations ($\mu * P(DOWN)$). In this condition:

$$P(DOWN) = \frac{\lambda}{\lambda + \mu}, \qquad P(UP) = \frac{\mu}{\lambda + \mu} \tag{N.4}$$

The constant repair rate μ implies an average repair time τ, with $\mu=1/\tau$. Recognizing that typically $\mu>>\lambda$, we can write:

$$P(DOWN) \cong \lambda\tau\,. \tag{N.5}$$

In words: within the so-called "lambda-tau approximation," the average unavailability of a particular component is given by the product of its failure rate and the average time needed to restore it.

The above discussion is illustrated in Figure 77. Note that the values of λ and μ have been chosen to make their relationship visible in this plot; they are not meant to be typical. For these values, the steady-state unavailability is in fact given by $P(DOWN) = \frac{\lambda}{\lambda+\mu}$, but the lambda-tau approximation is not particularly good.

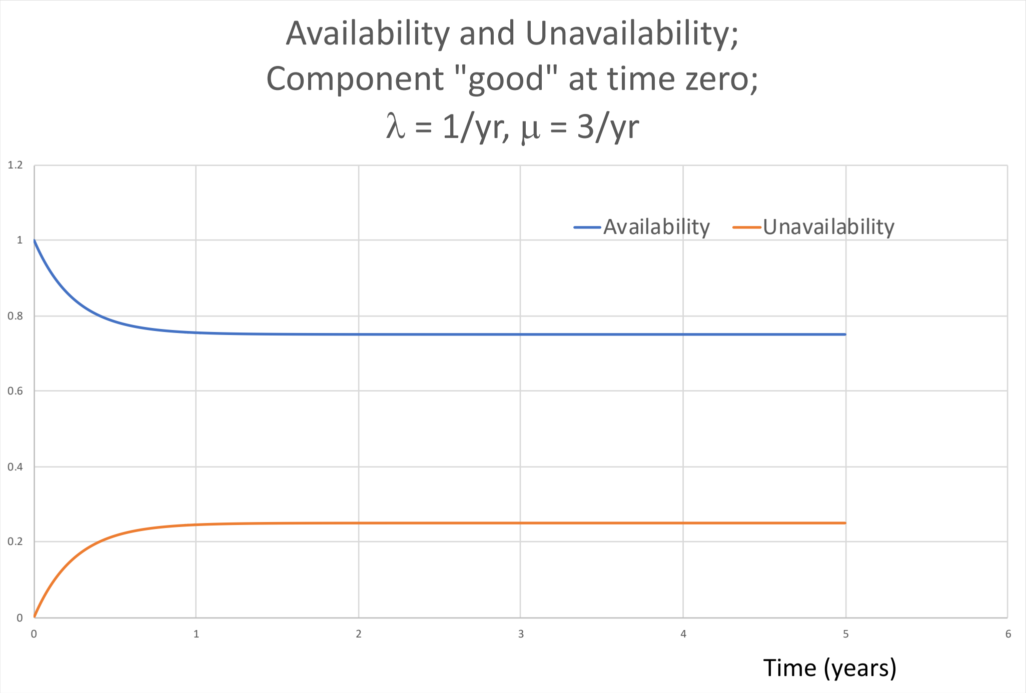


Figure 77. Example plot of availability and unavailability over time.

Let us recapitulate the specializations and approximations in this calculation:

- As illustrated in the above plot, the steady state calculation is valid only after the initial conditions are "forgotten." If we start out an operating cycle with all components as good as new, then the unavailability early in the cycle may be less, perhaps significantly less, than the steady-state calculation would suggest.
- First, we assumed that the failure rate and repair rate were constant. For some components in some environments, the failure rate may be approximately constant; but ageing and wearout, especially if accelerated as a result of some environmental or loading factor, could change this appreciably. The repair process is unlikely to be a stochastic Poisson process; it is more likely that particular failure modes will take particular amounts of time to repair. On the other hand, for a given failure mode, there may well be a typical characteristic restoration time rather than an average over exponentially distributed repair times, and in that case, using that characteristic restoration time in the $\lambda\tau$ approximation is more than reasonable, assuming we are out in the regime where initial conditions are "forgotten."

Generation Risk Assessment

The following formula appears in an EPRI report on generation risk assessment [157]:

$$LMwh = \sum_{i=1}^{m} \lambda_{1,i} P_{1,i} R_{1,i} + \sum_{j=1}^{n} \lambda_{2,j} P_{2,j} R_{2,j} \qquad \text{(N.6)}$$

accompanied by the following explanatory text:

> "In this formula, λ_1 is the average frequency of trip events per year, λ_2 is the average frequency of derate events per year, *P* is the reduced power level [power reduction factor for the event (e.g., 100% for trip and a value between 1% to 99% for derate)], *R* is the restoration time in hours for the event (repair time including the time required for reduction and restoration of power), the index "*i*" covers the combinations of SSC failures that can lead to a trip, the index "*j*" covers the combinations of SSC failures that can lead to a derate. The resulting units are "megawatt hours per year".

The formula seems unexceptionable: it computes average lost megawatt-hours per year by (1) computing block unavailabilities (probabilities of being unavailable) within the lambda-tau approximation discussed above, (2) using these probabilities to weight the associated lost production, and (3) summing over the failure modes that give rise to lost production.

Such a formula can be implemented in different software in different ways. If we were just computing functional unavailability in SAPHIRE [158], the normal thing would be to quantify a basic event for component unavailability by putting λ and τ right into the basic event parameters, and letting the program explicitly compute unavailability of the subject a basic event. But that's not what some of the Generation Risk people do. Knowing that SAPHIRE quantifies cut sets by multiplying basic event probabilities, and that SAPHIRE then quantifies top events by putting together all of these contributions (often using the "min cut upper bound" approximation, which may be better than just summing up cut set probabilities), we can implement the above formula by treating each *factor* in each term as if it were a basic event, with "probability" equal to frequency λ, or fraction of lost power *P*, or restoration time *R*; and then contriving input to the logic software to yield the above expression, knowing that its calculation will perform the indicated products and summations.

Trying to View the Above Expression in Success Space

What happens when we take a model like that and try to view it in success space? Consider the following "cut set" expression resulting from applying the above approach to a two-component system:

LMWH=L1*TAU1*P1+L2*TAU2*P2.

If this were really just a Boolean expression, then complementing it would have a simple meaning. For example, if the left-hand variable meant "Failure of System X," then "NOT Failure of System X" would mean "Success of System X." Instead, complementing LMWH, we have

/LMWH=(/L1+/TAU1+/P1)*(/L2+/TAU2+/P2)

=/L1*/L2+/L1*/TAU2+/L1*/P2+/TAU1*/L2+/TAU1*/TAU2+/TAU1*/P2+

/P1*/L2+/P1*/TAU2+/P1*/P2.

This does not have any particular meaning. Consider the success term /P1*/P2. What might it mean to say that success is achieved if "the power lost due to L1 is 'NOT P1' AND the power lost due to L2 is 'NOT P2?'"? The point is that although we used a Boolean code to quantify the LMWH formula, the "basic events" are not True / False conditions, such as "pump so-and-so is in a failed state." Rather, their values are arithmetic.

Path forward

With some effort, we might be able to contrive a way of interpreting the above form for /LMWH. For example, we could argue that "success" is achieved if the amount of derate resulting from either component is zero. Success is also achieved if the restoration time becomes zero, or if the outage rate becomes zero.

For now, we would rather find a way to map the GRA expression into Boolean form. In order to begin to work with a Boolean expression for unavailability, we have to transform this expression in a couple of ways. Mainly, we need to work with basic events that are either "true" or "false," and whose probabilities we can quantify. Additionally, if we need to distinguish derate from trip, and especially if we need to distinguish degrees of derate, we need to flag subsets of the overall expression, rather as if degree of derate were analogous to "plant damage state." In effect, for some purposes, we would want unavailability expressions for each discrete degree of derate that we wish to consider. Given such a group of expressions, we might impose varying stringencies of prevention measures; maybe we would require high assurance of not having a trip, but only moderate assurance of not derating by 2%.

Returning to the two-cut-set problem discussed above, suppose we rewrite the contributors as basic events corresponding to unavailability, and partition the expression into one expression for each degree of derate. We would then look for ways to sharply reduce high derates, and in parallel, look for ways to somewhat reduce nearly-negligible derates; and then we would "AND" these expressions together, hoping to find an efficient solution where (for example) reduction of some failure rate (or increase of some restoration rate) has the desired effect on both categories of derate at once. In fact, a failure-space importance measure exists for just such an application [156]. It relies on manipulating the values of parameters inside basic event models, implicitly varying (say) a parameter that influences the failure rates of multiple basic events.

For a model in which redundancy and topology are more complex than the pedagogical examples considered here, it would be preferable to start with success-space analysis, especially Prevention Analysis, which requires a model expressed in terms of logic variables. Such an effort may be mounted in the coming year.

Appendix O

SUMMARY OF CONDITION ASSESSMENT APPROACHES

Prognostics and health management technologies rely on accurate, reliable indicators of equipment condition. Significant research and development has investigated appropriate measurements and analyses of those measurements to extract relevant component health indicators. Many of these tools, such as periodic vibration monitoring of rotating equipment and ultrasonic inspection of pressure vessel welds, are commonly employed in current NPPs. Additional equipment condition assessment methods have been proposed in the literature, and in some cases are commonly in use outside the nuclear industry. The following subsections summarize available equipment condition assessment methods for both active and passive systems, structures, and components common to NPPs.

Active Components

Active components include components and systems that physically actuate to perform their functions, e.g., motors, valves, and pumps. Because these systems are performing an action, monitoring and estimation of their health state may be more straightforward. In many cases, the system process performance contains information about the current state of health of the key components that together perform the process. However, relying only on process data may not be sufficient for complex systems with many active components. Techniques have been developed for each of the major classes of components in NPPs; commonly investigated methods are summarized in Table 29 and the associated references. Measurement technologies and feature extraction methods are largely mature for active components, although many of these methods are not commonly used in practice in the nuclear industry.

Many active components share common approaches to condition monitoring and assessment. With few exceptions, active component health is monitored through passive measurements; that is, the components are not interrogated outside of their normal operation in order to measure indicators of component health. Current and voltage monitoring for electrically-powered systems supports common Motor Current Signature Analysis (MCSA) and Motor Power Signature Analysis (MPSA), as well as a variety of other analysis methods that have been developed for bespoke application. All rotating equipment are commonly monitored through vibration analysis and associated joint time-frequency analysis. NPPs employ many of these techniques through periodic ISI, but they are largely amenable to permanently mounted sensors to support continuous or near-continuous in situ monitoring.

Passive Components

Passive components include structures and components that typically provide barriers or conduits and do not move or actuate in the performance of their function, e.g., vessels, pipes, and cables. Passive component health is current monitored through periodic In-Service Inspection (ISI) according to practices outlined in the American Society for Mechanical Engineers (ASME) Boiler & Pressure Vessel (BPV) Code. Current and proposed Nondestructive Test And Evaluation (NDTE) methods for several key passive component classes are summarized in Table 30. Unlike active components, passive components typically must be interrogated with an active signal to obtain health indicators. The results of these active interrogations are then analyzed and correlated back to structure health parameters, such as the existence and propagation of internal cracks.

Significant work remains to identify the most appropriate NDTE signatures and feature extraction methods for monitoring most passive components of interest in NPPs. Many of these techniques have been demonstrated in laboratory settings, but there do not currently exist long-lived, permanently mounted sensors to support in situ health monitoring for passive components. As these measurement technologies mature, many passive component monitoring methods may be well-suited to deep learning and big data analytics approaches for identifying and extracting the key features of measured signals that indicate the current health state of a large, passive structure.

Table 29. Equipment condition assessment methods for common active components.

Active Components			
Component Type	**Measurements**	**Method of Analysis**	**Selected References**
Motors	Current, Voltage	Motor current signature analysis	[159][160][161][162]
		Spectrum synch	[163]
		Bispectrum analysis and active interrogation	[164]
		Time series statistics (e.g., mean, variance)	[165]
	Vibration	Frequency analysis	[166][167]
		Time series statistics (e.g., RMS, variance, kurtosis)	[168]
		Approximate entropy	[169][170]
Motor-driven Pumps	Current, Voltage	Motor current signature analysis	[159][171]
	Acoustic Emission	Amplitude and frequency	[172][173][174]
	State Parameter Estimation	Process monitoring of state variables	[175]
	Vibration	Joint time-frequency analysis	[176][177]
Motor Operated Valves	Current, Voltage	Motor current signature analysis	[159][178][179][180]
		Thrust and torque estimation	[181][182]
Bearings	Acoustic Emission	Envelope analysis	[183][184][185][186]
	Vibration	Joint time-frequency analysis	[176][177][187][188][189]
		Approximate entropy	[169][189][190]

Table 30. Nondestructive evaluation and condition assessment methods for passive components.

Passive Components		
Component Type	**Measurements**	**Selected References**
Heat exchangers	Process variables	[191][192]
Pressure vessel	Thermoelectric properties	[193][194]
	Mechanical strain	[193][195][196][197][198]
	Acoustic emission	[193][199][200][201]
	Magnetic Barkhausen noise	[202][203][204][205]
	Ultrasonic guided waves	[205][206][207][208]
Pipes	Ultrasonic guided waves	[208][209][210]
	Acoustic emission	[210][211][212][213][214]
Cables	Time domain reflectometry	[215][216][217][218]
	Frequency domain reflectometry	[219][220]
	Joint time-frequency domain reflectometry	[221][222][223][224]
	Line Resonance Analysis (LIRA)	[225][226][227][228]
	Indenter modulus	[229][230][231][232][233]