Toward a Functional Failure Modeling Method of Representing Prognostic Systems During the Early Phases of Design

Conference Paper · August 2015

DOI: 10.1115/DETC2015-46400

2 authors:

Caitlin Stack
Colorado School of Mines
1 PUBLICATION **5** CITATIONS
SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS
SEE PROFILE

Proceedings of the ASME 2015 International Design Engineering Technical Conferences &
Computers and Information in Engineering Conference
IDETC/CIE 2015
August 3-5, 2015, Boston, USA

DETC2015-46400

TOWARD A FUNCTIONAL FAILURE MODELING METHOD OF REPRESENTING PROGNOSTIC SYSTEMS DURING THE EARLY PHASES OF DESIGN

Caitlin Stack
Graduate Research Assistant
Nuclear Science and Engineering Program
Colorado School of Mines
Golden, CO, USA
cstack@mines.edu

Douglas L. Van Bossuyt[*]
Assistant Professor
Nuclear Science and Engineering Program
Colorado School of Mines
Golden, CO, USA
dvanboss@mines.edu

ABSTRACT

Current methods of functional failure risk analysis do not facilitate explicit modeling of systems equipped with Prognostics and Health Management (PHM) hardware. As PHM systems continue to grow in application and popularity within major complex systems industries (e.g. aerospace, automotive, civilian nuclear power plants), implementation of PHM modeling within the functional failure modeling methodologies will become useful for the early phases of complex system design and for analysis of existing complex systems. Functional failure modeling methods have been developed in recent years to assess risk in the early phases of complex system design. However, the methods of functional modeling have yet to include an explicit method for analyzing the effects of PHM systems on system failure probabilities. It is common practice within the systems health monitoring industry to design the PHM subsystems during the later stages of system design – typically after most major system architecture decisions have been made. This practice lends itself to the omission of considering PHM effects on the system during the early stages of design. This paper proposes a new method for analyzing PHM subsystems' contribution to risk reduction in the early stages of complex system design. The Prognostic Systems Variable Configuration Comparison (PSVCC) eight-step method developed here expands upon existing methods of functional failure modeling by explicitly representing PHM subsystems. A generic pressurized water nuclear reactor primary coolant loop system is presented as a case study to illustrate the proposed method. The success of the proposed method promises more accurate modeling of complex systems equipped with PHM subsystems in the early phases of design.

1 INTRODUCTION

Many complex systems use Prognostics and Health Management (PHM) systems to detect incipient failures and direct recovery actions performed either by automated recovery systems or by human operators. However, little attention has been paid to PHM systems in the earliest phases of complex system design. Risk analysis methods such as Probabilistic Risk Assessment (PRA) and Function Failure Identification and Propagation (FFIP) do not explicitly consider PHM systems. While PRA can model recovery actions, FFIP does not have the ability to model recovery actions during a failure scenario.

It is important for system designers to have a clear picture of system failure probabilities during the early phases of complex system design. The knowledge of system failure probabilities allows system designers to iterate on potential configurations to achieve a target system risk level within budgetary constraints. The later in the design process that a clear picture of system risk is generated, the more expensive and time-consuming it becomes to fix system design problems that prevent the desired level of

[*] Address all correspondence to this author.

system risk from being achieved.

The Prognostic Systems Variable Configuration Comparison (PSVCC) method presented in this paper provides system designers with an early phase complex system design tool that provides information on PHM systems and recovery actions for failure analysis. System designers can rapidly analyze multiple PHM system configurations and identify the most appropriate configuration for the system based upon desired risk level and budgetary constraints. The PSVCC method is automatable and can be performed with other function failure design methods such as FFIP and Uncoupled Failure Flow State Reasoning (UFFSR).

1.1 Specific Contributions

This paper presents a novel functional failure modeling-based method, the PSVCC, of analyzing PHM system configurations for system failure risk reduction in the early phases of complex system design. System designers can use this method to optimize PHM system configurations that take into account complex system human operator or automated system recovery actions during the progression of a failure event before the failure event has progressed to a system-level failure.

2 BACKGROUND

Many complex systems, such as civilian nuclear power plants, contain PHM equipment to monitor plant systems, detect incipient failures, and take corrective actions before a failure propagates throughout the entire system and causes system-level failure. Risk and reliability analysis methods such as PRA, Failure Modes and Effects Analysis (FMEA), and other industry-standard tools offer limited insight to account for PHM equipment during the design phase of a complex system. Early risk-informed conceptual design phase tools based on functional modeling such as FFIP, Flow State Logic (FSL), UFFSR, and others do not yet have the ability to explicitly model PHM systems and their functions within complex systems. The work presented in this paper bridges the gap between the early phases of conceptual system design and the installation of PHM systems to give system designers the ability to model PHM equipment as early as possible in the design process. A review of relevant literature to this paper is presented below specifically focusing on industry-standard tools (PRA, FMEA, RBD) that are deficient in PHM considerations and early conceptual design tools (FFIP, FSL, UFFSR) that the method developed in this paper is based upon.

2.1 Prognostics and Health Management

PHM provides information on system health status and predictions about when a system or component will fail by using realtime system data from sensors and other signal sources. Remaining useful life predictions can be used to inform maintenance staff and system operators of how much longer a system can be run before it needs to be maintained or repaired. PHM information can also be used to notify operators of impending failure events so that recovery actions can be taken to prevent system-level failure. Many complex systems, such as nuclear power plants, make extensive use of PHM systems to improve safety and reliability [1–7].

2.2 Failure Modes and Effects Analysis

FMEA is a tool used in the early phases of design to assess system and component failures. A Risk Priority Number (RPN) is generated from determining the probability of occurrence, the detectability of the problem before it becomes a realized system fault, and the severity of the resulting chain of events. This method relies upon expert judgement and prior system knowledge to generate potential failure modes of the system under development. While FMEA is a useful tool and can be used to analyze limited data from other PHM systems, it is not well suited to comprehensively analyze potential design configurations for PHM systems in large complex system designs [8, 9].

2.3 Reliability Block Diagrams

Reliability Block Diagrams (RBDs) have been used for many decades for early phase system development. The RBD method graphically illustrates the flow of energy or material through a system by presenting blocks representing components or subsystems and connecting them with lines representing how subsystems or components interact with one another. Reliability statistics can be attached to the individual component or subsystem blocks. The reliability information can be compiled into a system reliability probability that allows designers to search for single point sources of failure in a system design. RBD methods can be used to model parts or sections of a PHM subsystem (those which are directly in line with the failure flow being analyzed within the RBD). However, the inability of the RBD method to explicitly consider and compare potential PHM equipment configurations and recovery actions for the purposes of design and optimization creates the demand for a novel method to approach this early stage design problem [10–12].

2.4 Probabilistic Risk Assessment

In the civilian nuclear power industry, PRA has been developed to analyze highly complex nuclear power generation stations. The nuclear industry follows a strict defense in depth philosophy which requires multiple redundant and diverse systems to prevent single point failures causing significant accidents [13–15]. A critical system-level failure in a nuclear power plant could lead to the release of radiation beyond the site boundary and a significant loss of revenue for a utility operator. PRA was developed in part to verify defense in depth design strategies as being effective and in part to seek out ways to further reduce system failure risk. Highly complex, multi component and multi subsystem failure events can be modeled using PRA to determine failure propagation pathways that otherwise would not have been discovered during the design of a power plant [16,17]. PRA uses Fault Trees (FTs) and Event Trees (ETs) with statistical models developed from idealized component models and updated using Bayesian statistics with plant operation data. Cut sets are generated that provide information on the minimum number of components or subsystems that need to fail in order to cause a system-level failure (often defined as partial melting of the Zircaloy fuel cladding). The statistical failure information from each failed component is brought together using boolean algebra to determine the probability of a specific failure sequence occurring. All of the cut sets generated from a PRA model are summed together to determine total system-level failure risk. Beyond the nuclear power industry, several other industries have adopted PRA including the aerospace industry, the automotive industry (in certain sectors), and most recently, the petroleum industry.

PRA contains limited abilities to model PHM equipment and recovery actions in the form of recovery events and Human Reliability Analysis (HRA). HRA is a suite of methods that allow the calculation of likelihood that a human plant operator will be able to perform an action or sequence of actions to recover a system from a failure progression back to a safe system state (often a cold shutdown state in a nuclear power plant) [18–20]. Most HRA methods require operators to be presented with plant state information so that operators can detect an incipient failure event and react before the failure has propagated to a system-level failure. The hardware involved in detecting plant state and reporting it to the operator is generally not analyzed and is assumed to function without failure. The success or failure of operators to conduct a recovery action is determined through various analysis techniques in the various HRA methods but all result in a probability of a successful recovery action. The probability can be put into PRA models to provide a more realistic probabilisitic failure model that includes humans.

2.5 Functional Modeling Tools

As it became clear over the last two decades that a more rigorous method of modeling complex systems at the earliest phases of design was needed, Stone and Wood developed the Functional Basis for Engineering Design (FBED) [21–24]. FBED provides a standardized method of representing system functionality in complex systems through mapping functions and the flows of energy, material, and data between the functions. Many methods extending FBED have been developed since its introduction. The Function Failure Design Method (FFDM) was developed to link failure data with individual functions to provide system designers with information on likely sources of failure in the component embodiment of a specific function so that design decisions can be made to reduce failure probability in the physical system [25]. Function-based Analysis of Critical Events (FACE) provides a means of analyzing different phases of a complex systems mission, such as various operation and shutdown phases of a nuclear power plant [26]. FFIP was introduced to analyze failure flows through a complex system after a single point failure has occurred [27]. FSL followed FFIP to provide a rigorous quantitative probabilisitic analysis tool for calculating system failure probabilities based on FFIP failure flow information [28,29].

Shortcomings were found in the original FFIP methodology such as the inability to model uncoupled failure flows across functional boundaries. PRA has some tools available to do this such as fire and flood analysis that provide information on the likelihood of a failure propagation path across uncoupled systems from a fire or flood event. However, the PRA fire and flood analysis implementations are imprecise in their analysis and are impractical to use in the early phases of complex system design [30–34]. The UFFSR method was developed to expand upon FFIP and provide the ability to model failure flows that cross functional and system boundaries [35,36]. To date, PHM modeling using function failure modeling has not yet been developed. This paper introduces the PSVCC method of modeling PHM systems in the early phases of complex system design.

3 METHODOLOGY

In this section, the PSVCC method for analyzing the effects that PHM equipment has on system failure probability in the early stages of design is presented. The PSVCC method builds upon the function failure modeling methods of FFIP and FSL that in turn build upon FBED. By inserting PHM equipment into a functional failure model and crediting recovery actions taken by either system operators or by automated recovery systems, a more complete understanding of system failure risks can be attained earlier in the design process.

The values used within the paper to demonstrate the PSVCC methodology– such as epsilon values, DFP values, sigma values, and RFF values– are intentionally fictional but representative of nominal values within a variety of nuclear power industry sources, such as handbooks, manuals, and technical papers published by the Nuclear Regulatory Commission and the International Atomic Energy Agency [37]. It should be noted that the values used here to demonstrate the presented methodology, while intentionally fictional, have been chosen as a reasonable representation of expected values with the discretion of the author's expert opinion as a former nuclear submarine plant operator. The authors believe these values to be of merit, based upon the Nuclear Regulatory Commission's Probabilistic Risk Assessment Tutorial which states that operating experience is the primary source for risk assessment data, such as ”frequency of many initiating events, failure rates of plant equipment, average availability of plant equipment, [and] probabilities of repair and recovery" [37]. "Expert elicitation" is declared by the NRC as a special method for vital risk assessment value determination in severe casualty situations. Significant work beyond the scope of this paper is necessary to collect sufficient data from real systems and operators to develop accurate sigma, epsilon, DFP, and RFF values. The values created for use in this methodology do not represent a specific, real physical system, but are representative of a class of systems. Note again, this paper uses values derived from expert opinion and industry resources for the purpose of illustrating the method; these specific values should not be used for safety-critical analysis.

The steps to perform PSVCC are presented below:

Step 1: Create a FBED model of the system of interest and generate a FFIP model of potential failures and failure paths. The FBED model can be generated in a variety of ways including from an existing system's Piping and Instrumentation Diagram (P&ID) as in the case of an existing system redesign or reanalysis. For new systems in the early stages of design, a FBED model can typically be generated from the conceptual design to create a preliminary model of the system. As the FBED is a simplistic, functional-level model, generating a FBED during the early stages of design is practical and effective.

Step 2: Generate a list of prospective PHM parameters to be monitored and potential locations for PHM devices to be installed in the system. The authors suggest that these devices be represented on the system's FFIP model, using a generic conventional P&ID symbol for an instrumentation tap. Visually indicate PHM parameter signal feeds on the functional model from each PHM device to any/all components or functions that are considered to be significantly influenced by the state of the monitored parameters.

Step 3: Determine the states of impending system failure, identifying values for Categories of Concern (Low, High, Fail), as well as the probabilities that the impending system failure being analyzed results in each of the Categories of Concern (represented as σ-values). These categories are a direct analogue to the parameter value bands of concern marked on an instrumentation gauge commonly found in complex systems such as civilian nuclear power plants. Figure 1 illustrates an example of these Categories of Concern as represented on a gauge readout. Note that the authors advocate that in most cases category ranges should be defined for values both above and below normal operating range, as illustrated in the figure.

Step 4: Determine for each PHM sensor, and in each of the Categories of Concern, the failure probability of the PHM device to detect the condition, the Detection Failure Probability (DFP). Tabulate this information into a database for automated generation of cut sets later on in PSVCC.

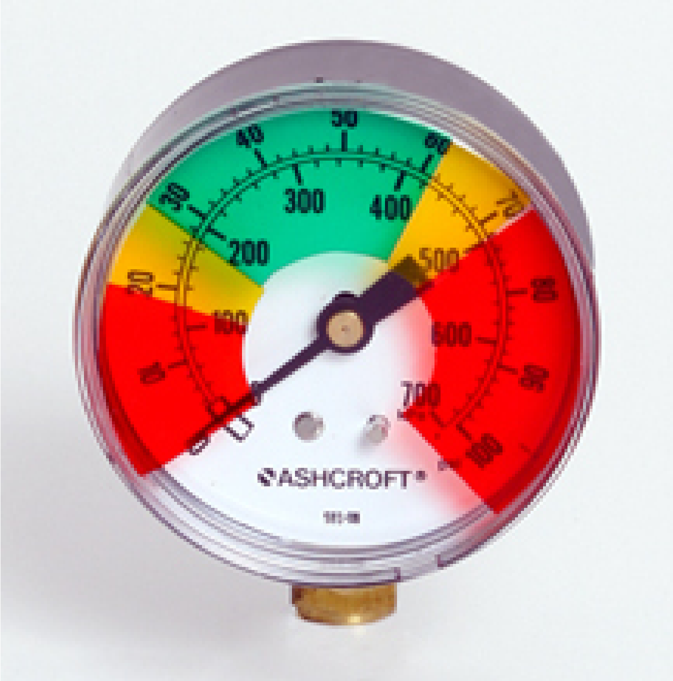


FIGURE 1. GAUGE INDICATIONS OF CATEGORIES OF CONCERN. THE GREEN AREA OF THE GAUGE (200-400 KPA) REPRESENTS NORMAL OPERATING CONDITIONS. THE YELLOW AREAS OF THE GAUGE (100-200KPA, 400-500 KPA) REPRESENT AN AREA OF LOW CONCERN. THE AREAS OF RED ON THE GAUGE (0-100 KPA, 500-700KPA) REPRESENT AREAS OF HIGH CONCERN. AREAS BEYOND THE HIGH AREAS OF CONCERN REPRESENT AREAS OF FAILURE CONCERN.

Step 5: For each Category of Concern, determine the probabilities of various system functions failing before plant operators have time to correct the fault (ε-values). This is equivalent to an on-demand failure probability for components modeled in a PRA analysis.

Step 6: Determine the probabilities of operator action/inaction failing to restore system functionality, Restore Functionality Failure (RFF), for each Category of Concern. This information can be generated from existing HRA methods.

Step 7: Perform cut set analysis on the system. "Cut set" analysis is a term used within the risk assessment field which refers to the act of "cutting" the logic branches of a fault tree. Each cut set evaluates a combination of events which will result in system-wide failure. The cut sets performed for this methodology provide values for system-wide failure probabilities on a yearly basis. Further information on cut set analysis methods can be found in the reference material. Cut set analysis can be accomplished through an automated software-driven process or on small enough systems can be performed by hand. An important point here is that each potential PHM sensor configuration should have a full set of cut sets developed separately. The next step will use the cut sets developed for each potential PHM sensor configuration to search for the optimized PHM system configuration.

Step 8: Compare the cut sets for the different sensor configurations. The cut set results may be used to determine how many sensors are useful for the system. Most likely, one or more proposed PHM sensors will be found to not be useful to overall system reliability and can be removed. It is also important to compare the various cut sets with the FFIP-generated failure probability of the system. The cut set failure probabilities are expected to be lower with the use of PHM equipment unless the PHM equipment has no effect in the failure scenario. If the PHM configuration cut sets have little or no effect on system reliability when compared with FFIP results, a reanalysis of potential PHM configurations and recovery actions must be performed. This also may be an indicator that redundant systems need to be developed if recovery actions cannot be performed on the system of interest before a Category of Concern failure progresses to a system failure.

The PSVCC method presented in this section provides system designers with a functional failure modeling tool that can be used in the early stages of complex system design for analysis of PHM equipment effects on system reliability. In the event that a Category of Concern failure initiates but before a failure has progressed to a system failure, recovery actions by either plant operators or by automated systems may recover from the fault state and preserve nominal system operation. The PSVCC method can be performed by hand on small systems but is best suited for automated software analysis.

4 CASE STUDY

To illustrate the PSVCC method, a case study is presented in this section based upon a single, simplified primary Reactor Core Coolant Loop (RCCL) in a large generic commercial Pressurized Water Reactor (PWR) nuclear power plant. It should be noted that the RCCL modeled here for the purpose of the case study is a single loop; multiple-loop redundancy paths are not analyzed for the purpose of demonstrating PSVCC on a simple but illustrative model. However, PSVCC is equally viable when modeling extremely complex systems such as large commercial PWRs.

The single RCCL presented here is composed of five major system components: the reactor (RX), a steam generator (S/G), two Reactor Coolant loop Isolation valves (RCI-1/2), and a single Main Coolant Pump (MCP). Figure 2 provides a generic P&ID of the RCCL from which a functional model can be derived. The primary function of this system is to generate heat (via the RX) and transfer that heat to the secondary system (via the S/G) where the heat can be used to generate electrical power. The MCP serves to transport the coolant liquid through the primary system and maintain flow through the RX to ensure proper cooling and prevent core meltdown. The RCI-1/2 serve the purpose of RCCL isolation in the event of a failure scenario such as a primary coolant leak, detection of foreign solid particulate, etc., or maintenance. This case study includes the analysis of the PHM equipment associated with the system, of which there are a total of six potential sensors, described in Table 1. The case study follows the methodology previously presented in the following subsections and specifically analyzes a heat flow failure scenario physically equivalent to a S/G failure.

Step 1: Create a FFIP model of the system

Using the P&ID of the system of interest (Figure 2), a functional block diagram is developed. Figure 3 shows the resulting functional block diagram of the RCCL being analyzed for this case study and Figure 4 shows the FFIP failure model of a heat flow failure initiating event being analyzed in this case study. Other initiating events are not presented here for clarity and brevity.

Step 2: Prospective PHM Equipment

For each function, a list of parameters that will significantly influence the function's probability of failure is identified. A table, such as Table 2, is created to organize this information.

TABLE 2. SIGNIFICANT PARAMETERS BY FUNCTION

Function	Th	Tc	PL	LB1	LB2	PNM
Rx	x	x	x			
S/G	x		x			
MCP	x		x			x
RCI-1	x		x	x		
RCI-2	x		x		x	

From the information in Table 2, the parameters most likely to contribute significantly to function failure are identified. PHM devices specific to these parameters are chosen and placed within the system for modeling and analysis.

PHM device signal feeds are visually indicated on the functional model from each PHM device to any and all functions of the system that have been determined to be significantly influenced by that parameter, as noted on Table 2. The resulting functional model including the prospective PHM instrumentation signal feeds is illustrated in Figure 5. Note that this step is useful for conceptual mapping, but may become too graphically overwhelming when attempting to model very complex systems with a multitude of significant PHM parameters and components. A computer-readable table is all that is required for automated analysis. For the rest of this case study, only the Th, Tc, and PL PHM sensors are analyzed for simplicity although the steps are

TABLE 1. DESCRIPTION OF PHM DEVICES

PHM Device Name	Parameter Monitored	Type of Device	Function Name
Th	Hot leg fluid temperature	Resistance temperature detector	Signal-Sense, Measure
Tc	Cold leg fluid temperature	Resistance temperature detector	Signal-Sense, Measure
PL	RCCL pressure	Linear variable differential transformer	Signal-Sense, Measure
LB1	Leak-by of RCI-1	Flow detector	Signal-Sense, Measure
LB2	Leak-by of RCI-2	Flow detector	Signal-Sense, Measure
PNM	Decibel level of pump operation	Microphone	Signal-Sense, Measure

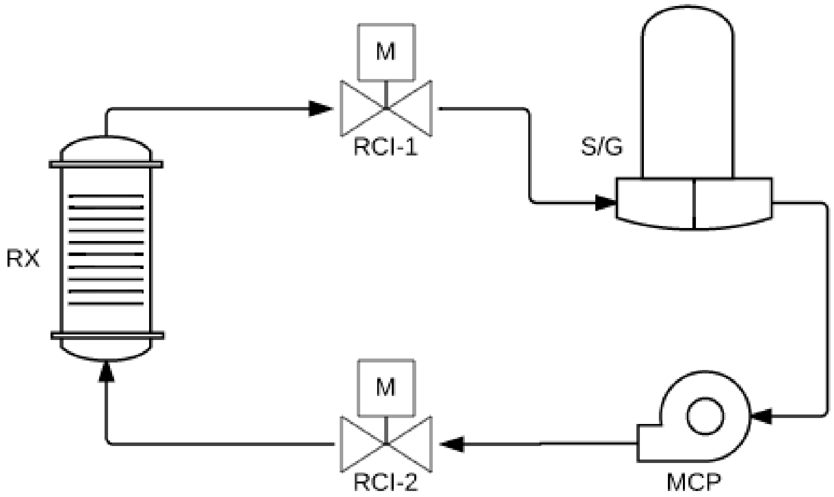


FIGURE 2. P&ID OF THE SIMPLIFIED RCCL OF A GENERIC COMMERCIAL PWR. THE RCI-1/2 ARE NORMALLY OPEN DURING LOOP OPERATION, AND SHUT TO SERVE THE FUNCTION OF LOOP ISOLATION IN THE EVENT OF MAINTENANCE OR FAILURE SCENARIO.

the same and results are similar for analyzing all six potential PHM sensors.

Step 3: System States of Failure and Categories of Concern For each PHM parameter, a range of values are defined for each of the four categories of concern: Normal, Low, High, and Fail. The Normal range should be representative of acceptable parameter values within nominal operating conditions. The Normal range will not be evaluated for failure analysis during the method presented in this paper. This is due to the fact that normal operating conditions are not typically indicative of elevated risk towards impending system failure. Values in the Low range should be representative of conditions that, if maintained for prolonged periods, may lead to system failure. Values in the High range of concern should be representative of conditions that are cause for raised awareness and expeditious corrective action, and are indicative of a short period of time before system failure. Parameter values within the Fail Category of Concern imply that prolonged operations under such conditions will result in imminent system failure. The information for the case study analysis is organized in Table 3. The probability of the initiating event being analyzed resulting in each of the three defined categories is determined (σ-values). These values are also present in Table 3. It should be noted that, while parameter values that directly relate to physical system parameters are useful for system designers to

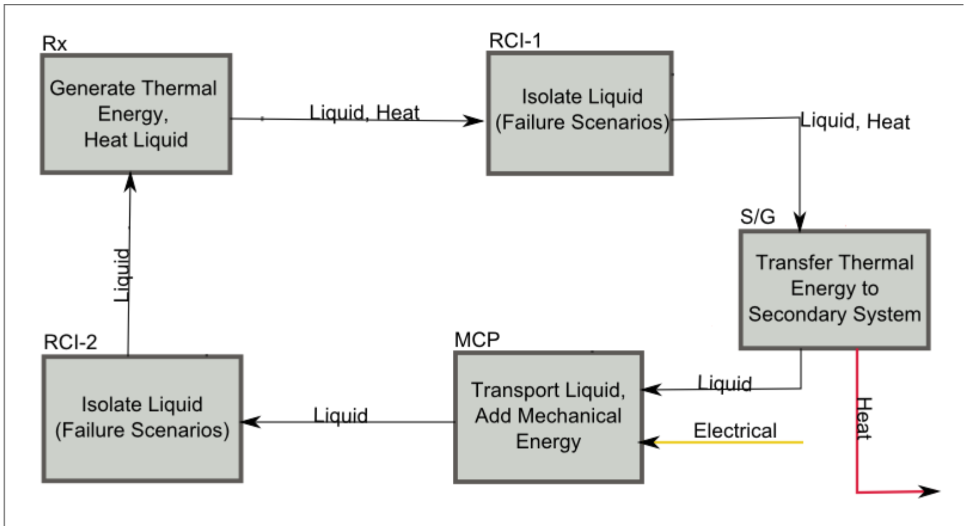

Rx
Generate Thermal Energy, Heat Liquid
Liquid, Heat
RCI-1
Isolate Liquid (Failure Scenarios)
Liquid, Heat
S/G
Transfer Thermal Energy to Secondary System
Liquid
RCI-2
Isolate Liquid (Failure Scenarios)
Liquid
MCP
Transport Liquid, Add Mechanical Energy
Liquid
Electrical
Heat

FIGURE 3. FUNCTIONAL BLOCK DIAGRAM OF THE RCCL SYSTEM (STEP 1).

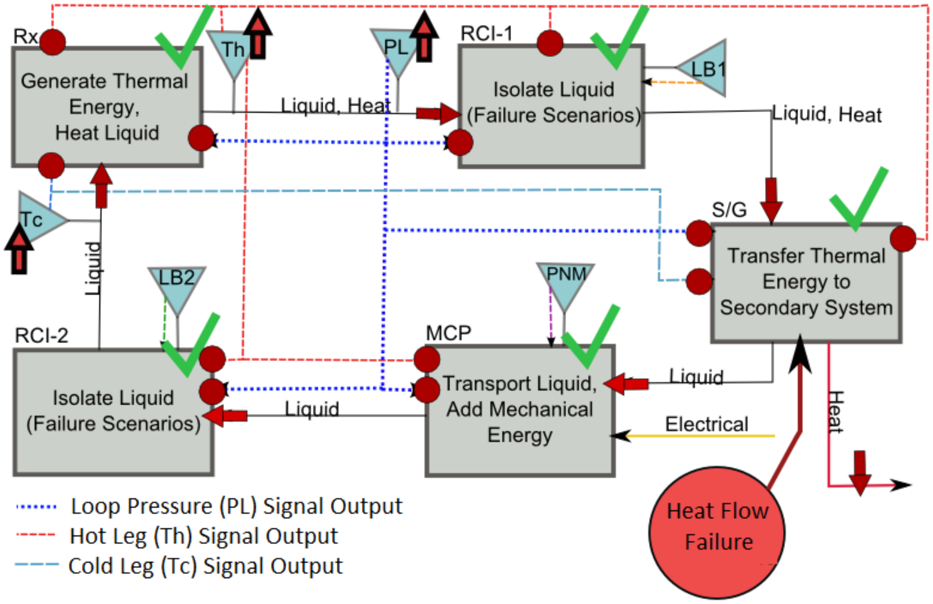

Rx
Th
PL
RCI-1
LB1
Generate Thermal Energy, Heat Liquid
Liquid, Heat
Isolate Liquid (Failure Scenarios)
Liquid, Heat
Tc
S/G
Transfer Thermal Energy to Secondary System
Liquid
LB2
PNM
RCI-2
MCP
Isolate Liquid (Failure Scenarios)
Liquid
Transport Liquid, Add Mechanical Energy
Liquid
Electrical
Heat
Loop Pressure (PL) Signal Output
Hot Leg (Th) Signal Output
Cold Leg (Tc) Signal Output
Heat Flow Failure

FIGURE 4. FFIP FAULT PROPAGATION PATH

more deeply consider the Categories of Concern, in the earliest stages of functional modeling before many of these parameters are set, it is sufficient to only use the Normal, Low, High, and Fail Categories of Concern with representative estimates of σ values.

Step 4: Detector Failure Probabilities (DFP)

DFPs represent the probability of PHM detectors in the system failing to detect PHM parameter changes during a Category of Concern failure event. These values reflect each potential PHM sensor configuration being analyzed for comparison in Step 8. The DFPs used to analyze the case study RCCL system with three PHM devices (Th, Tc, and PL) installed are listed in Table 4 below. Note that similar tables are generated for each potential PHM system configuration (e.g.: Th, Tc; Th, PL; Tc, PL; etc.).

Step 5: Determine "ε" Values The ε values represent the probabilities of various system components failing before plant operators have time to correct the fault by taking a recovery action. The generated ε values for the functional heat flow failure being analyzed in this case study (representative of a gradual fouling of heat transfer surfaces on the S/G U-tubes) are listed in Table 5 below.

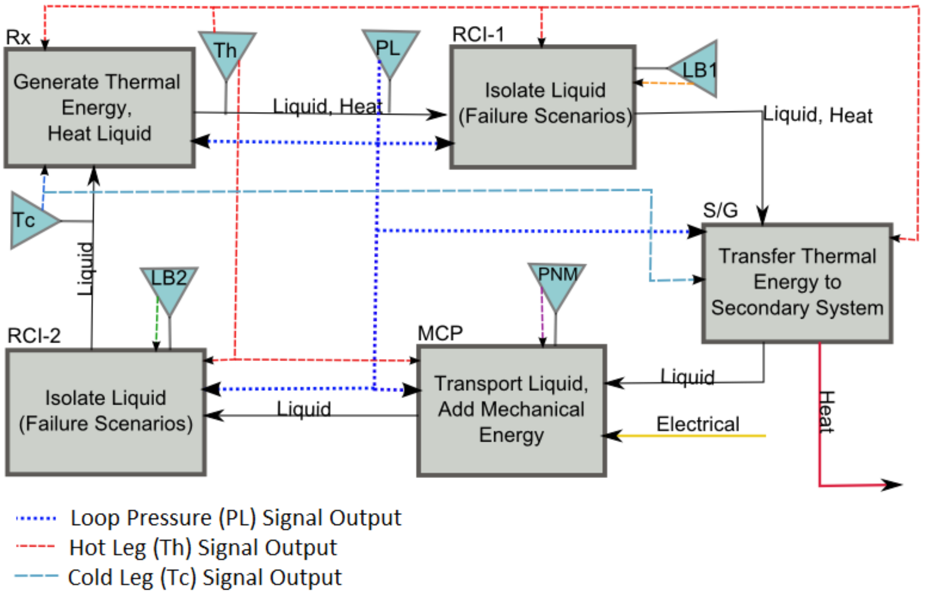

Rx
Generate Thermal Energy, Heat Liquid
Th
PL
Liquid, Heat
RCI-1
Isolate Liquid (Failure Scenarios)
LB1
Liquid, Heat
Tc
S/G
Transfer Thermal Energy to Secondary System
Liquid
LB2
PNM
RCI-2
MCP
Isolate Liquid (Failure Scenarios)
Liquid
Transport Liquid, Add Mechanical Energy
Liquid
Electrical
Heat
Loop Pressure (PL) Signal Output
Hot Leg (Th) Signal Output
Cold Leg (Tc) Signal Output

FIGURE 5. FUNCTIONAL MODEL OF THE RCCL SYSTEM, ILLUSTRATING ONE POTENTIAL CONFIGURATION OF PHM INSTRUMENTATION TAPS AND SIGNAL FEEDS (STEP 2).

TABLE 3. RANGES DEFINING CATEGORIES OF CONCERN AND σ -VALUES

	Category of Concern				
PHM Device	Normal	Low	High	Fail	Units
Th	390-410	370-390; 410-430	350-370; 430-450	$< 350; > 450$	Deg. F
Tc	340-360	320-340; 360-380	300-320; 380-400	$< 300; > 400$	Deg. F
PL	1900-2100	1700-1900; 2100-2300	1500-1700; 2300-2500	$< 1500; > 2500$	psi
LB1	< 0.1	0.1-0.5	0.5-1.0	> 1.0	gph
LB2	< 0.1	0.1-0.5	0.5-1.0	> 1.0	gph
PNM	< 2.0	2.0-4.0	4.0-6.0	> 6.0	$dB > background$
	σ-values	0.7	0.25	0.05	

Step 6: Determine RFF Values

The RFF values represent the probability of an operator's actions or inactions failing to restore the plant to normal operating conditions. Three values are defined per failure mode: one for each Category of Concern (Low, High, Fail). For this case study, the values used to analyze heat flow failure are as follows: $RFF_{LOW} = 0.2, RFF_{HIGH} = 0.25, RFF_{FAIL} = 0.32$.

Step 7: Cut Set Analysis

For illustrative purposes in this case study, only one group of cut sets will be expanded upon in this section in order to demonstrate the process. This group is representative of the failure probabilities of the MCP during a heat flow failure, with three PHM devices installed. Figure 6 provides an example illustrating one of the various cut set flow paths analyzed for this group. Cut set results can be found in Table 7.

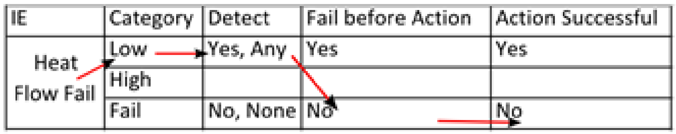
Separate sets of cut sets for this scenario are generated for the following prospective PHM configurations: (Th), (Th,Tc), (Th, PL), (Tc), (Tc, PL), (PL). For each cut set analysis, the DFP used is the direct product of the individual DFPs of the PHM devices within the given configuration. Each configuration and

TABLE 4. DFP: DETECTORS (Th, Tc, PL)

	Category of Concern		
Detectors	Low	High	Fail
Th	0.1	0.02	0.0001
Tc	0.08	0.005	0.0001
PL	0.4	0.2	0.1
All Fail	0.0032	2.00E-05	1.00E-09

TABLE 5. HEAT FLOW FAILURE ε VALUES

	Category of Concern		
Functions	Low	High	Fail
MCP	0.2	0.4	0.85
S/G	0.1 0.3	0.72	
RX	1.00E-07	5.00E-05	2.00E-04
RCI-1	0.0001	0.0005	0.001
RCI-2	0.0002	0.0006	0.002



IE	Category	Detect	Fail before Action	Action Successful
Heat Flow Fail	Low	Yes, Any	Yes	Yes
	High			
	Fail	No, None	No	No

FIGURE 6. EXAMPLE CUT SET FLOW PATH

its corresponding DFP is listed in Table 6.

Step 8: Compare Method Results The results of the various PHM configurations' cut sets are compared with the results from the FFIP analysis and between each other. The results of each PHM configuration are compared to aid in identification of the most useful combination of PHM devices for the system. Results of the case study are presented and discussed in the next section.

5 RESULTS AND DISCUSSION

In the previous section, cut set analysis was performed on the various failure paths of Figure 4 above, with PHM sensors inserted in various configurations. Table 7 presents the case where three PHM sensors have been placed in the system and analyzed for their reduction in system failure probability which now stands at 4.10E-8. For comparison, the FFIP analysis produced a system failure probability of 1.22E-7/yr without any PHM hardware being present.

TABLE 6. DFP VALUES FOR VARIOUS PHM CONFIGURATIONS

	Category of Concern		
PHM Configurations	Low	High	Fail
Th	0.1	0.02	1.00E-04
Th, Tc	0.008	1.00E-04	1.00E-08
Tc	0.08	0.005	1.00E-04
Th, PL	0.04	0.004	1.00E-05
PL	0.4	0.2	0.1
Tc, PL	0.032	0.001	1.00E-05

TABLE 7. CUT SET RESULTS FOR THREE PHM SENSORS

Failure/yr	Cut Sets
4.10E-08	System Failure Probability
1.22E-08	$IE\_Heat\_Flow\_Fail, Cat\_High, MCP\_Fail\_B4$
1.71E-08	$IE\_Heat\_Flow\_Fail, Cat\_Low, MCP\_Fail\_B4$
5.19E-09	$IE\_Heat\_Flow\_Fail, Cat\_Fail, MCP\_Fail\_B4$
4.58E-09	$IE\_Heat\_Flow\_Fail, Cat\_High, Response\_Fail\_(High)$
1.37E-09	$IE\_Heat\_Flow\_Fail, Cat\_Low, Response\_Fail\_(Low)$
2.93E-10	$IE\_Heat\_Flow\_Fail, Cat\_Fail, Response\_Fail\_(Fail)$
2.73E-10	$IE\_Heat\_Flow\_Fail, Cat\_Low, Det\_All\_Fail\_LOW$
6.10E-13	$IE\_Heat\_Flow\_Fail, Cat\_High, Det\_All\_Fail\_HIGH$
6.10E-18	$IE\_Heat\_Flow\_Fail, Cat\_Fail, Det\_All\_Fail\_FAIL$

Once cut set analysis of all potential PHM sensor configurations is complete (in this case study, only three sensors were fully analyzed for simplicity), a comparison can be made between different configurations, as shown in Table 8. It is interesting to note that all but one potential sensor configuration lowers system failure risk by an order of magnitude from the FFIP base case. This is as a result of operator recovery actions or automated system recovery actions occurring successfully once a Category of Concern failure state is identified by the PHM system. The greatest reduction in system failure risk is found in the three PHM sensor configuration (Th, Tc, PL). However, the two sensor configuration (Th, Tc) has very similar system failure risk. A system designer may choose to only install the Th and Tc PHM sensors rather than all three if the cost of the third sensor is high[1]. In a fully computer automated system analysis, a cost-versus-risk-reduction algorithm can be used to determine the tradeoff between sensor configurations and sensor costs.

TABLE 8. SYSTEM FAILURE PROBABILITIES FOR DIFFERENT PHM SYSTEM CONFIGURATIONS

Failure/yr	Configuration
1.22E-07	FFIP Base Case
4.10E-08	Th, Tc, PL
4.50E-08	Th, Tc
7.95E-08	Th, PL
8.21E-08	Tc, PL
8.23E-08	Th
8.45E-08	Tc
1.02E-07	PL

By performing analysis with the PSVCC method presented in this paper, a clearer and more representative picture of system failure risk can be determined in the early phases of complex system design. Including PHM systems in the early stages of analysis allows for intelligent system architecture choices to be made. PRA methods are difficult to use in the earliest phases of design and PRA models are hard to rapidly reconfigure to explore alternative PHM configurations. FFIP and related functional failure methods do not have an explicit method of representing and analyzing PHM systems. Neither PRA nor FFIP represent Categories of Concern failures explicitly or usefully. The method presented in this paper provides system designers with analysis of many potential PHM configurations and resulting system risk reductions while explicitly modeling Categories of Concern failures.

6 CONCLUSIONS AND FUTURE WORK

The PSVCC method presented in this paper provides system designers with a tool to more fully analyze system failure risk in the early phases of complex system design by examining the contribution of PHM systems and recovery actions to overall system reliability. Existing methods such as PRA and FFIP are difficult to use at the earliest stages of design and are unable to explicitly represent PHM systems or recovery actions. The PSVCC method presented here allows system designers to rapidly analyze multiple PHM system configurations and identify the most appropriate configuration for the system. Early knowledge of PHM system configuration will save designers time and money as compared to current systems engineering methods that leave PHM system design until much later in the design process.

Future work includes the development of an automated tool to place PHM sensors in a system functional model and develop automated recovery functions with minimal need for designer input. A fully automated PHM system design and analysis tool has the potential to discover new PHM system configurations and recovery actions that can further reduce system failure risks. While defense in depth strategies and multiple redundant systems are useful for reducing system failure risk, well-designed PHM systems also play an important role in complex system design.

ACKNOWLEDGMENT

This research was partially supported by United States Nuclear Regulatory Commission Grant Number NRC-HQ-84-14-G-0047. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

REFERENCES

[1] Coble, J. B., Ramuhalli, P., Bond, L. J., Hines, J., and Upadhyaya, B., 2012. *Prognostics and health management in nuclear power plants: a review of technologies and applications*. Pacific Northwest National Laboratory.

[2] Pecht, M., 2008. *Prognostics and health management of electronics*. Wiley Online Library.

[3] Goebel, K., Saha, B., Saxena, A., Celaya, J. R., and Christophersen, J. P., 2008. "Prognostics in battery health management". *IEEE instrumentation & measurement magazine,* ***11***(4), p. 33.

[4] Schwabacher, M., 2005. "A survey of data-driven prognostics". In Proceedings of the AIAA Infotech@ Aerospace Conference, pp. 1–5.

[5] Poll, S., Patterson-Hine, A., Camisa, J., Garcia, D., Hall, D., Lee, C., Mengshoel, O. J., Neukom, C., Nishikawa, D., Ossenfort, J., et al., 2007. "Advanced diagnostics and prognostics testbed". In Proceedings of the 18th International

[1] Note that in a complete analysis of the RCCS, all three sensors (Th, Tc, PL) are found to be necessary for the complete suite of initiating events that can impact the RCCS

Workshop on Principles of Diagnosis (DX-07), pp. 178–185.

[6] Saxena, A., Celaya, J., Saha, B., Saha, S., and Goebel, K., 2009. "On applying the prognostic performance metrics".

[7] Coble, J. B., and Hines, J. W., 2008. "Prognostic algorithm categorization with phm challenge application". In Prognostics and Health Management, 2008. PHM 2008. International Conference on, IEEE, pp. 1–11.

[8] Ben-Daya, M., 2009. "Failure mode and effect analysis". In *Handbook of Maintenance Management and Engineering*, M. Ben-Daya, S. O. Duffuaa, A. Raouf, J. Knezevic, and D. Ait-Kadi, eds. Springer London, pp. 75–90.

[9] Stamanis, D. H., 2003. *Failure Modes and Effects Analysis: FMEA from Theory to Execution*, 2nd ed. ASQ Quality Press, Milwaukee, WI.

[10] Robidoux, R., Xu, H., Xing, L., and Zhou, M., 2010. "Automated modeling of dynamic reliability block diagrams using colored petri nets". *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on,* ***40***(2), March, pp. 337–351.

[11] Hamada, M. S., Wilson, A. G., Reese, C. S., and Martz, H. F., 2008. *Bayesian Reliability*. Springer.

[12] Kumamoto, H., 2007. *Satisfying Safety Goals by Probabilistic Risk Assessment*. Springer.

[13] Fleming, K. N., and Silady, F. A., 2002. "A risk informed defense-in-depth framework for existing and advanced reactors". *Reliability Engineering & System Safety,* ***78***, July, pp. 205–225.

[14] Bakolas, E., and Saleh, J. H., 2011. "Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems". *Reliability Engineering & System Safety,* ***96***(1), pp. 184–193.

[15] Zio, E., 2009. "Reliability engineering: Old problems and new challenges". *Reliability Engineering & System Safety,* ***94***(2), pp. 125 – 141.

[16] Modarres, M., Kaminskiy, M., and Krivtsov, V., 1999. *Reliability engineering and risk analysis: a practical guide*. CRC press.

[17] Keller, W., and Modarres, M., 2005. "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor norman carl rasmussen". *Reliability Engineering & System Safety,* ***89***(3), pp. 271 – 285.

[18] Swain, A. D., and Guttmann, H. E., 1983. Handbook of human-reliability analysis with emphasis on nuclear power plant applications. final report. Tech. rep., Sandia National Labs., Albuquerque, NM (USA).

[19] Dougherty, E., and Fragola, J., 1988. "Human reliability analysis".

[20] Swain, A. D., 1990. "Human reliability analysis: need, status, trends and limitations". *Reliability Engineering & System Safety,* ***29***(3), pp. 301–313.

[21] Stone, R. B., and Wood, K. L., 2000. "Development of a functional basis for design". *Journal of Mechanical Design,* ***122***(4), pp. 359–370.

[22] Stone, R. B., Wood, K. L., and Crawford, R. H., 2000. "Using quantitative functional models to develop product architectures". *Design Studies,* ***21***(3), pp. 239–260.

[23] Hirtz, J. M., Stone, R. B., Szykman, S., McAdams, D., and Wood, K. L., 2001. "Evolving a functional basis for engineering design". In Proceedings of the ASME Design Engineering Technical Conference: DETC2001, Pittsburgh, PA.

[24] Hirtz, J., Stone, R. B., McAdams, D. A., Szykman, S., and Wood, K. L., 2002. "A functional basis for engineering design: reconciling and evolving previous efforts". *Research in engineering Design,* ***13***(2), pp. 65–82.

[25] Stone, R. B., Tumer, I. Y., and Stock, M. E., 2005. "Linking product functionality to historic failures to improve failure analysis in design". *Research in Engineering Design,* ***16***(1-2), pp. 96–108.

[26] Hutcheson, R. S., McAdams, D. A., Stone, R. B., and Tumer, I. Y., 2006. "A function-based methodology for analyzing critical events". In Proceedings of the IDETC/CIE.

[27] Kurtoglu, T., and Tumer, I. Y., 2008. "A graph-based fault identification and propagation framework for functional design of complex systems". *Journal of Mechanical Design,* ***130***(5), p. 051401.

[28] Jensen, D., Tumer, I. Y., and Kurtoglu, T., 2009. "Flow state logic (fsl) for analysis of failure propagation in early design". In ASME 2009 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, American Society of Mechanical Engineers, pp. 1033–1043.

[29] Kurtoglu, T., Tumer, I. Y., and Jensen, D. C., 2010. "A functional failure reasoning methodology for evaluation of conceptual system architectures". *Research in Engineering Design,* ***21***(4), pp. 209–234.

[30] Distefano, S., and Puliafito, A., 2009. "Dependability evaluation with dynamic reliability block diagrams and dynamic fault trees". *Dependable and Secure Computing, IEEE Transactions on,* ***6***(1), Jan, pp. 4–17.

[31] Ramachandran, G., and Charters, D., 2011. *QUANT RISK ASSESS FIRE SAFETY*. Taylor & Francis.

[32] Samuels, P., Huntington, S., Allsop, W., and Harrop, J., 2008. *Flood Risk Management: Research and Practice: Extended Abstracts Volume (332 pages) + full paper CD-ROM (1772 pages)*. Taylor & Francis.

[33] Soares, C., 2010. *Safety and Reliability of Industrial Products, Systems and Structures*. A Balkema Book. Taylor & Francis.

[34] Bedford, T., and Cooke, R., 2001. *Probabilistic Risk Assessment: Foundations and Methods*. Cambridge University Press.

[35] Ramp, I. J., and Van Bossuyt, D. L., 2014. "Toward an auto-

mated model-based geometric method of representing function failure propagation across uncoupled systems". In Proceedings of the ASME 2014 International Mechanical Engineering Congress and Exposition IMECE2010, ASME.

[36] O'Halloran, B., Papakonstantinou, N., and Van Bossuyt, D. L., 2015. "Modeling of function failure propagation across uncoupled systems". In Proceedings of the Reliability and Maintainability Symposium.

[37] NRC Staff, 2007. Tutorial on probabilistic risk assessment (pra). Tech. rep., Nuclear Regulatory Commission.