ORNL/SR-2016/211

Integrated Risk-Informed Decision-Making for an ALMR PRISM

Sacit M. Cetiner
Michael D. Muhlheim
Askin G. Yigitoglu
Randall J. Belles
Richard S. Denning, Consultant

May 2016

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

ORNL/SR-2016/211

Reactor and Nuclear Systems Division

INTEGRATED RISK-INFORMED DECISION-MAKING FOR AN ALMR PRISM

Sacit M. Cetiner
Michael D. Muhlheim
Askin G. Yigitoglu
Randall J. Belles
Richard S. Denning, Consultant

Date Published: May 2016

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

LIST OF FIGURES v
LIST OF TABLES v
ACRONYMS vii
ACKNOWLEDGMENTS ix
ABSTRACT xi
1. INTRODUCTION 1
    1.1 GENERALIZED FRAMEWORK FOR AUTONOMOUS DECISION-MAKING 1
    1.2 AUTONOMOUS DECISION-MAKING FOR SUPERVISORY CONTROL 3
        1.2.1 High-Level Description of the SCS 4
        1.2.2 Metrics for Decision-Making 4
    1.3 SUPERVISORY CONTROL SYSTEM ARCHITECTURE 4
2. PROBABILISTIC MODEL 7
    2.1 ASSUMPTIONS 7
    2.2 WHAT DECISIONS ARE MADE 8
    2.3 HOW DECISIONS ARE MADE 9
    2.4 EXAMPLE 9
3. SYSTEM MODEL 15
    3.1 ALMR PRISM POWER CONVERSION SYSTEM DESIGN DESCRIPTION 15
    3.2 ALMR PRISM POWER CONVERSION SYSTEM MODEL 18
    3.3 ONGOING WORK 20
4. DIAGNOSTICS AND PROGNOSTICS 21
    4.1 SUMMARY OF PNNL'S PROTOTYPIC ERM FRAMEWORK FOR ADVANCED REACTORS 24
    4.2 ERM SOFTWARE FUNCTIONAL DESCRIPTION 25
        4.2.1 Equipment Condition Assessment and Prognostics 25
        4.2.2 Predictive Risk Assessment 25
        4.2.3 Uncertainty Quantification 25
        4.2.4 Supervisory Control Interface 25
    4.3 SUMMARY AND ONGOING WORK 26
5. DOMAIN OF AUTONOMOUS CONTROL 27
    5.1 RELATIONSHIP TO TECHNICAL SPECIFICATIONS AND LCOs 27
    5.2 KEY OPERATIONAL TRANSIENTS 27
6. CONCLUSIONS AND FUTURE WORK 31
    6.1 ONGOING WORK 31
7. REFERENCES 33

LIST OF FIGURES

Figure 1. Elements considered within the generalized framework for autonomous decision-making. 2
Figure 2. Illustration of a conceptual state space formed by arbitrary state variables x1 and x2. 3
Figure 3. The proposed framework for autonomous decision-making adopted for supervisory control systems. 5
Figure 4. Functional architecture of the SCS with the generalized decision-making framework..... 6
Figure 5. Power conversion system for the ALMR PRISM. 8
Figure 6. ET for steam flow to turbine with one steam generator in operation (Scenario 1)..... 10
Figure 7. ET showing both reactors operating at 100%..... 11
Figure 8. ET after TCV 1 fails with both reactors operating at 100%. 12
Figure 9. FTs capture component failures and carry SCS command options. (OOS = out of service)..... 13
Figure 10. An end-to-end simplified system diagram of an ALMR PRISM power block [13]..... 16
Figure 11. ALMR PRISM primary and secondary sodium transport systems [14]..... 17
Figure 12. ALMR PRISM steam supply system and recirculation loop mass and energy balances [15]..... 17
Figure 13. ALMR PRISM PCS flow diagram [16]. 18
Figure 14. ALMR PRISM PCS model developed for the SCS..... 19
Figure 15. A typical nodalization example of a horizontal feedwater heater in RELAP5..... 20
Figure 16. Considerations and steps to achieving an enhanced risk monitor [20]..... 22
Figure 17. Schematic showing the integration of PHM systems with ERMs and their functionality within the hierarchy of a supervisory control system for advanced reactors [24] 23

LIST OF TABLES

Table 1. ALMR PRISM heat transport system design values 28
Table 2. List of reactor trip variables and associated safety functions 28

ACRONYMS

AL	analytical limit
°C	degree Centigrade
ALMR	advanced liquid-metal reactor
ART	Advanced Reactor Technologies
BOP	balance-of-plant
CDF	core damage frequency
DOE	US Department of Energy
ECA	equipment condition assessment
EM	electromagnetic
ERM	enhanced risk monitor
ESFAS	engineered safeguards features actuation system
ET	event tree
FCV	flow control valve
FT	fault tree
FW	feedwater
GDC	General Design Criteria
ICHMI	Instrumentation, Controls, and Human-Machine Interface
IHTS	intermediate heat transport system
IHX	intermediate heat exchanger
kg/s	kilogram per second
LCO	limiting condition of operation
LSSS	limiting safety system setting
m	meter
m^3/s	cubic meters per second
MAUT	multi-attribute utility theory
MPa	mega Pascals
MSIV	main steam isolation valve
MWe	megawatt electric
n/cm^2s	neutrons per centimeter squared per second
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operation and maintenance
ORNL	Oak Ridge National Laboratory
PCS	power conversion system
PHM	prognostic health management
PNNL	Pacific Northwest National Laboratory
POF	probability of failure
PRA	probabilistic risk assessment
PRISM	Power Reactor Inherently Safe Module
PSID	Preliminary Safety Information Document
R&D	research and development
RO	reactor operator
RPS	reactor protection system
SCS	supervisory control system
SG	steam generator

SGS	steam generator system
SL	safety limit
SMR	small modular reactor
SSC	systems, structures, and components
TBV	turbine bypass valve
TCV	thermal control valve
TRANSFORM	*TRANsient Simulation Framework of Reconfigurable Models*
TS	Technical Specification

ACKNOWLEDGMENTS

This project is funded by the US Department of Energy, Office of Nuclear Energy, under the Instrumentation, Control, and Human-Machine Interface (ICHMI) technical area of the Advanced Reactor Technologies (ART) program.

ABSTRACT

Decision-making is the process of identifying decision alternatives, assessing those alternatives based on predefined metrics, selecting an alternative (i.e., making a decision), and then implementing that alternative. The generation of decisions requires a structured, coherent process, or a decision-making process. The overall objective for this work is that the generalized framework is adopted into an autonomous decision-making framework and tailored to specific requirements for various applications. In this context, automation is the use of computing resources to make decisions and implement a structured decision-making process with limited or no human intervention. The overriding goal of automation is to replace or supplement human decision makers with reconfigurable decision-making modules that can perform a given set of tasks rationally, consistently, and reliably.

Risk-informed decision-making requires a probabilistic assessment of the likelihood of success given the status of the plant/systems and component health, and a deterministic assessment between plant operating parameters and reactor protection parameters to prevent unnecessary trips and challenges to plant safety systems.

The probabilistic portion of the decision-making engine of the supervisory control system is based on the control actions associated with an ALMR PRISM. Newly incorporated into the probabilistic models are the prognostic/diagnostic models developed by Pacific Northwest National Laboratory. These allow decisions to incorporate the health of components into the decision–making process. Once the control options are identified and ranked based on the likelihood of success, the supervisory control system transmits the options to the deterministic portion of the platform.

The deterministic portion of the decision-making engine uses thermal-hydraulic modeling and components for an advanced liquid-metal reactor Power Reactor Inherently Safe Module. The deterministic multi-attribute decision-making framework uses various sensor data (e.g., reactor outlet temperature, steam generator drum level) and calculates its position within the challenge state, its trajectory, and its margin within the controllable domain using utility functions to evaluate current and projected plant state space for different control decisions. The metrics that are evaluated are based on reactor trip set points.

The integration of the deterministic calculations using multi-physics analyses and probabilistic safety calculations allows for the examination and quantification of margin recovery strategies. This also provides validation of the control options identified from the probabilistic assessment. Thus, the thermal-hydraulics analyses are used to validate the control options identified from the probabilistic assessment.

Future work includes evaluating other possible metrics and computational efficiencies, and developing a user interface to mimic display panels at a modern nuclear power plant.

1. INTRODUCTION

This report documents the development of the probabilistic model of a candidate advanced liquid-metal reactor (ALMR) that mimics the actions of a plant operator given a component failure. This model will be coupled with the deterministic portion of the autonomous risk-informed decision-making process within a supervisory control system (SCS). Newly incorporated into the probabilistic models are prognostic/diagnostic models developed by Pacific Northwest National Laboratory (PNNL). These allow decisions to incorporate the health of components into the decision–making process. Once the control options are identified and ranked based on the likelihood of successfully avoiding a reactor trip set point, the SCS transmits the options to the deterministic portion of the platform. The deterministic, probabilistic, and diagnostic tool sets are based on the ALMR Power Reactor Inherently Safe Module (PRISM) design.

Probabilistic risk assessments (PRAs) for nuclear power plants (NPPs) do not evaluate how to avoid a transient, but rather quantify a plant's response to a transient. The metric of interest for these PRAs (i.e., Level-1 PRAs) is the core damage frequency (CDF) and large early release fractions. The paradigm used in the development of an SCS is the measure of the likelihood of successfully avoiding a trip set point and the resulting plant transient. Avoiding the trip set points means that plant parameters such as temperature, pressure, flow, power-flow ratios, and steam generator water levels are maintained within operational limits so that challenges to safety systems are avoided.

To measure how to maintain a plant within operational limits requires a metric for the operational state that reflects a probabilistic analysis of the plant based on maintaining and/or controlling the heat balance from the reactor core to the ultimate heat sink, and reflects the success of maintaining that heat balance. That is, rather than failure space, the SCS is concerned with success space; and rather than challenging a safety system, the unit of measure is defined as the likelihood of avoiding a trip set point, which avoids challenges to the safety systems.

A "risk-informed" approach represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus attention on design and operational issues commensurate with their importance to the likelihood of success [1, 2]. A "risk-informed" approach enhances the traditional deterministic approach by (1) allowing explicit consideration of a broader set of potential challenges to safety; (2) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment; (3) facilitating consideration of a broader set of resources to defend against these challenges; (4) explicitly identifying and quantifying sources of uncertainty in the analysis; and (5) enabling better decision-making by providing a means to test the sensitivity of the results against key assumptions [3].

Detailed descriptions of the decision-making framework and the SCS architecture have been reported in previous status reports [4, 5]. The following sections are provided as background information.

1.1 GENERALIZED FRAMEWORK FOR AUTONOMOUS DECISION-MAKING

The SCS must automatically respond to plant challenges such as equipment failures, must account for equipment being out of service, and must decide what action to take to return the plant to a stable state in real time.

"Automation" refers to the use of computing resources to perform repeatable tasks based on a predetermined set of rules and actions.

"Autonomy," on the other hand, refers to the use of computing resources to make decisions and implement a structured decision-making process with limited or no human intervention. The overriding

goal of autonomy is to replace or supplement human decision makers with reconfigurable decision-making modules that can perform a given set of tasks reliably. (It is assumed that the tasks to be performed are the proper tasks to be undertaken, given the circumstances.)

Decision-making is the process of identifying and choosing alternatives based on an agreed-upon set of metrics and preferences established by the decision maker. Indirectly implied in decision-making is that there are options to be considered. Each option offers a different approach or trajectory to move from a given state or condition to a desired state or condition.

The generation of consistent decisions requires that a structured, coherent process be defined, which immediately leads to a decision-making framework. The generalized framework for autonomous decision-making can be adopted and tailored to specific requirements for various applications.

This section provides an outline of the generalized decision-making framework that was presented and described in greater detail in previous reports. It also summarizes the key concepts of a risk-informed decision-making process for an SCS.

Ultimately, the objective of a decision-making process is to consider uncertainties and to evaluate options for the current component and system status. Hence it is quite possible that evaluation and assessment steps will require the consideration of multiple attributes of a system, components or elements of a system, or their future states. This is especially true for large-scale, complex systems such as NPPs.

While there are minor differences in the literature about the necessary and sufficient steps for decision-making, the decision-making process for the SCS is based on the following fundamental elements:

1. identification: define alternatives

2. evaluation: assess alternatives

3. resolution: generate a single solution or a single trajectory, and collect and order those steps needed to finalize an action

4. action: execute the action(s)

These elements, as illustrated in Figure 1, define the generalized autonomous decision-making framework.

Figure 1. Elements considered within the generalized framework for autonomous decision-making.

1.2 AUTONOMOUS DECISION-MAKING FOR SUPERVISORY CONTROL

Based on General Design Criteria (GDC) 1 [6], GDC 13 [7], and 10 CFR 50.55a(a)(1) [8], the control systems in NPPs should be "appropriately designed and of sufficient quality to minimize the potential for challenges to safety systems" and "capable of maintaining system variables within prescribed operating ranges" [9]. The plant control systems in general and the reactor control system in particular are designed to maintain the plant in its normal operating conditions.

The purpose of the control system is to maintain system variables—such as reactor power, coolant flow rate, power-to-flow ratio, reactor outlet temperature, coolant level, and turbine status—within prescribed operating ranges. Exceeding a control system set point results in a plant transient and a challenge to plant mitigating systems, including a potential challenge to plant safety systems.

The simplest way to define this new metric—likelihood of avoiding a trip set point—is by calculating the proximity of the system state at any given time to its trip set points, which is called the "challenge surface." The challenge surface represents the controllable domain, beyond which a safety system actuation is warranted by the design of the plant. The challenge surface is illustrated with the red line in Figure 2. The goal of the SCS is to avoid challenging a safety system.

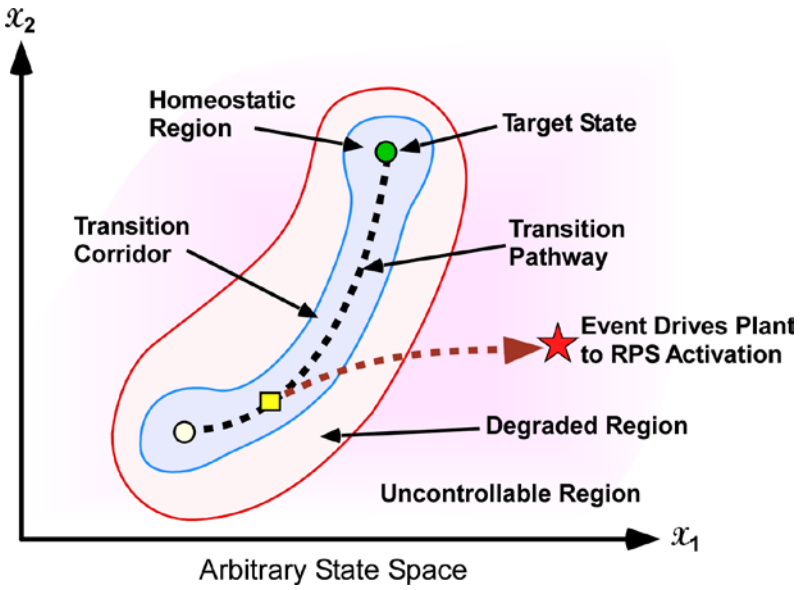

Figure 2. Illustration of a conceptual state space formed by arbitrary state variables x_1 and x_2.

The safety system domain is the domain outside the challenge surface of the plant state space. The safety system domain is illustrated in fading purple in Figure 2. Because this region represents the safety functions (e.g., protection system functions), it is outside the scope and capabilities of the control system.

Operation anywhere within the homeostatic region is considered normal. The plant control systems employ appropriate feedback control strategies, provided that the system parameters are maintained within the homeostatic region. Thus, a plant's integrated control system maintains the balance of plant parameters given the minor fluctuations in system variables that are ever present.

Should operation be driven into the degraded region through equipment failures or degradations, the control objectives become (1) maintain continuous and uninterrupted delivery of the principal products of the system, if possible; (2) prevent or minimize equipment damage; and (3) preclude initiation of the plant safety and protection systems. Transitioning into the degraded region may require faster response control

options to maintain system variables within the challenge surface. It is within this region that operators—and now the SCS—respond to plant threats to return the plant to within accepted parameters.

If a system variable transitions into the uncontrollable region, it enters the domain of the protection system, which is independent of and isolated from the control system. Reducing the likelihood of entering the uncontrollable region reduces the number of challenges to safety systems and the number of plant transients.

1.2.1 High-Level Description of the SCS

The SCS shall comply with the following high-level requirements:

1. The SCS shall be implemented as a non-safety–related system.

2. The SCS shall follow all the applicable rules and regulations regarding the separation and isolation of safety- and non-safety-related systems.

3. The SCS shall not perform any safety-related function.

4. The SCS shall not interfere with the functionality and operation of any safety system.

5. The SCS shall not override operator directives.

These requirements are enforced to define the domain of operation of the SCS. Implementing the SCS as a non-safety–related system avoids placing an undue regulatory burden on the vendor and the owner—especially considering the complexity of the system.

The fundamental assumption that goes into the design of the SCS is that, should the SCS fail to act during a transient, then the safety system will independently initiate and bring the plant to a nominal or acceptable shutdown state.

1.2.2 Metrics for Decision-Making

An SCS is required to support human decision-making under normal operating conditions and to make autonomous decisions. All of the possible states that the plant can assume constitute the controllable domain. The boundary of the controllable domain is primarily defined by the trip set points of the reactor protection system (RPS) or the engineered safeguards features actuation system (ESFAS). This domain is illustrated in light blue and orange in Figure 2.

The metric “probability of departure from controllable domain” provides an indication of the proximity of the plant state to the challenge surface. While there might be numerous ways to define this probability metric, it can be simply defined as a function of the distance between the current plant state and the closest point on the challenge surface. The closer the plant gets to the surface, the higher the probability of protection system actuation. Higher-order moments of the states can also be considered, such as the rate of approach.

1.3 SUPERVISORY CONTROL SYSTEM ARCHITECTURE

The architecture for autonomous decision-making implements the general framework using two methods. In the first method, the probabilistic method is implemented using PRA techniques to identify decision options. In the second method, the deterministic portion is implemented using utility theory to evaluate

the alternatives identified by the probabilistic portion and to generate a single solution, or the resolution of the autonomous decision-making process. These methods are shown in Figure 3. The cost function for finding the optimal or desired decision is determined by the evaluation metric. Additional constraints, such as regulatory rules and operating guidelines, can be enforced in the deterministic evaluation phase.

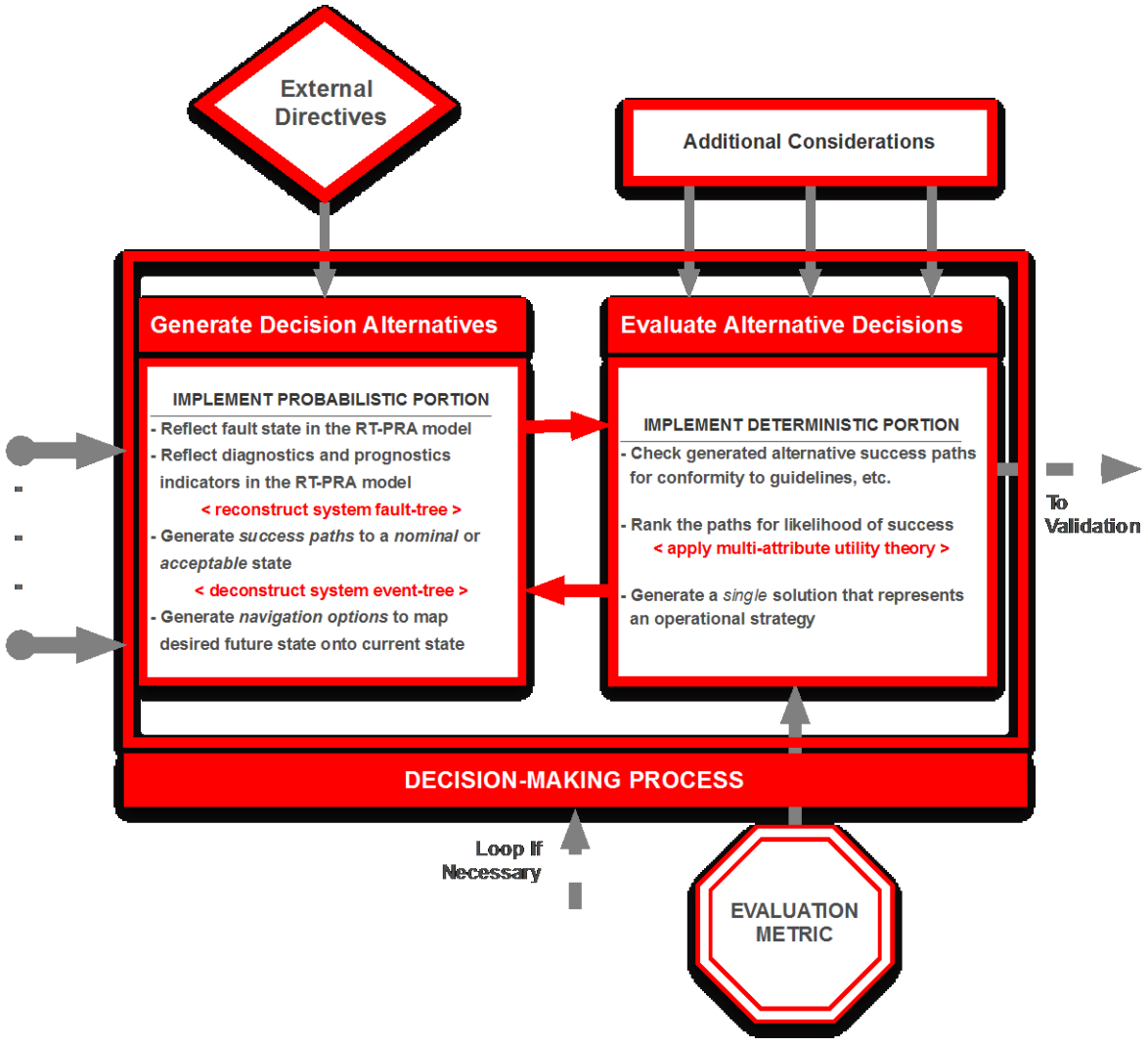

Figure 3. The proposed framework for autonomous decision-making adopted for supervisory control systems.

Figure 4 shows the functional architecture of the SCS and illustrates how the decision-making block in Figure 3 relates to the overall architecture.

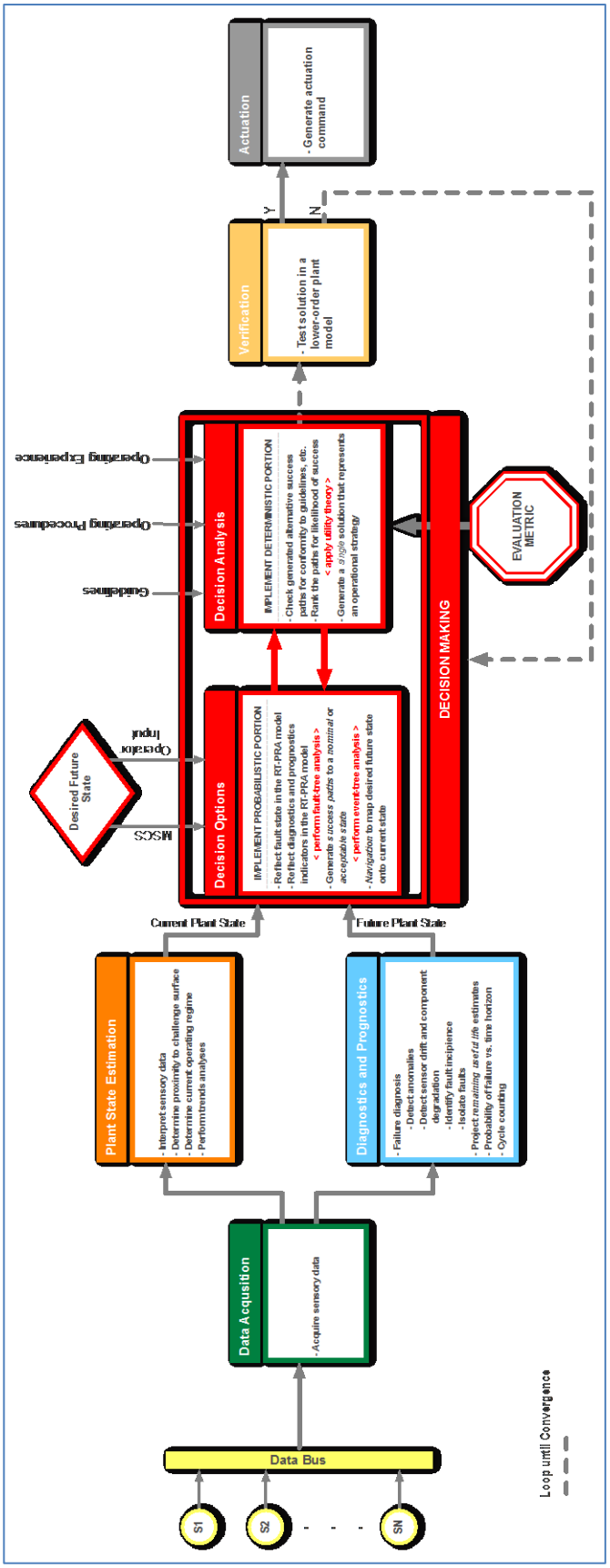

Figure 4. Functional architecture of the SCS with the generalized decision-making framework.

2. PROBABILISTIC MODEL

The probabilistic assessment portion of the risk-informed decision-making framework provides the control options for successfully avoiding trip set points given the status of the plant/systems and the likelihood of success for each of those options. The feasibility of creating the probabilistic portion of the decision-making engine was detailed in a previous milestone report [5]. This report details how the capabilities identified in that report were used to develop the probabilistic control portion of an SCS for the ALMR PRISM.

The probabilistic decision-making engine acts on failed component information, as well as sensor and state information, to identify and rank control restoration actions. A list of possible actions is ranked based on the potential for success based on real-time plant equipment and state information.

Based on plant operating status, component health, and equipment failures, the decision-making capabilities for the SCS use probabilistic analyses to identify a set of control options. These options, if implemented, should prevent the actuation of the protection system. The possibility for one or more outcomes, based on component health and plant status, distinguishes probabilistically informed decision-making implemented in real time from more traditional decision-making.

The probabilistic portion of the decision-making algorithm ranks the likelihood of success of each decision path based on the current system/plant status and component health. Based on the likelihood of the success metric under these conditions, the decision-making algorithm automatically chooses the top candidate control options as decision alternatives for the execution of the corresponding set of corrective actions. Selecting any of the control options would allow operations to continue by maintaining system status within the acceptable region. These actions and selection processes are the same as those an operator would be expected to perform.

The difference between a probabilistically-informed and a probabilistically-based decision-making algorithm is that a probabilistically-based algorithm would simply select the option with the greatest likelihood of success without any other factors being considered. However, this may not be the best choice based on other criteria. For example, the most likely option for avoiding a trip set point probabilistically could be to manually shut down the reactor; but deterministic factors such as reduced generation of heat (i.e., power reduction) might re-rank this option to the least favorable of the choices.

Once the control options are identified and ranked, the SCS transmits the options to the deterministic portion of the platform (see Chapter 3).

The deterministic decision-making framework is intended to provide the necessary interfaces for the probabilistic portion, and to generate a resolution, i.e., a single solution, of the decision-making process.

2.1 ASSUMPTIONS

Typically, limiting conditions for operations (LCOs) and surveillance requirements relate to the system trains or components that are modeled in the system fault trees of a PRA [10]. These are the Level-1 PRAs that model safety and safety-related systems. The risk from challenges to and failures of these systems is measured by the CDF. However, for the SCS, the metric of interest is the likelihood of avoiding a trip set point; and the systems modeled, in what Oak Ridge National Laboratory (ORNL) defines as the Level-0 PRA, are non-safety systems.

The SCS under development is for the ALMR PRISM. The probabilistic portion of the SCS for the secondary cooling system was developed (Figure 5). The "initiating events" for the event tree (ET) models are "successfully maintaining the heat balance from the reactor core to the ultimate heat sink." The ET branches capture the logic of the equipment/components in the systems, and the fault trees (FTs) capture the operational states of those components (e.g., operating, maintenance, failed, or degraded). Thus, the ET/FT models capture the component/system/plant statuses of components working properly, in a degraded state, out-of-service, or failing. The Level-0 PRA provided is for a plant at 100% power.

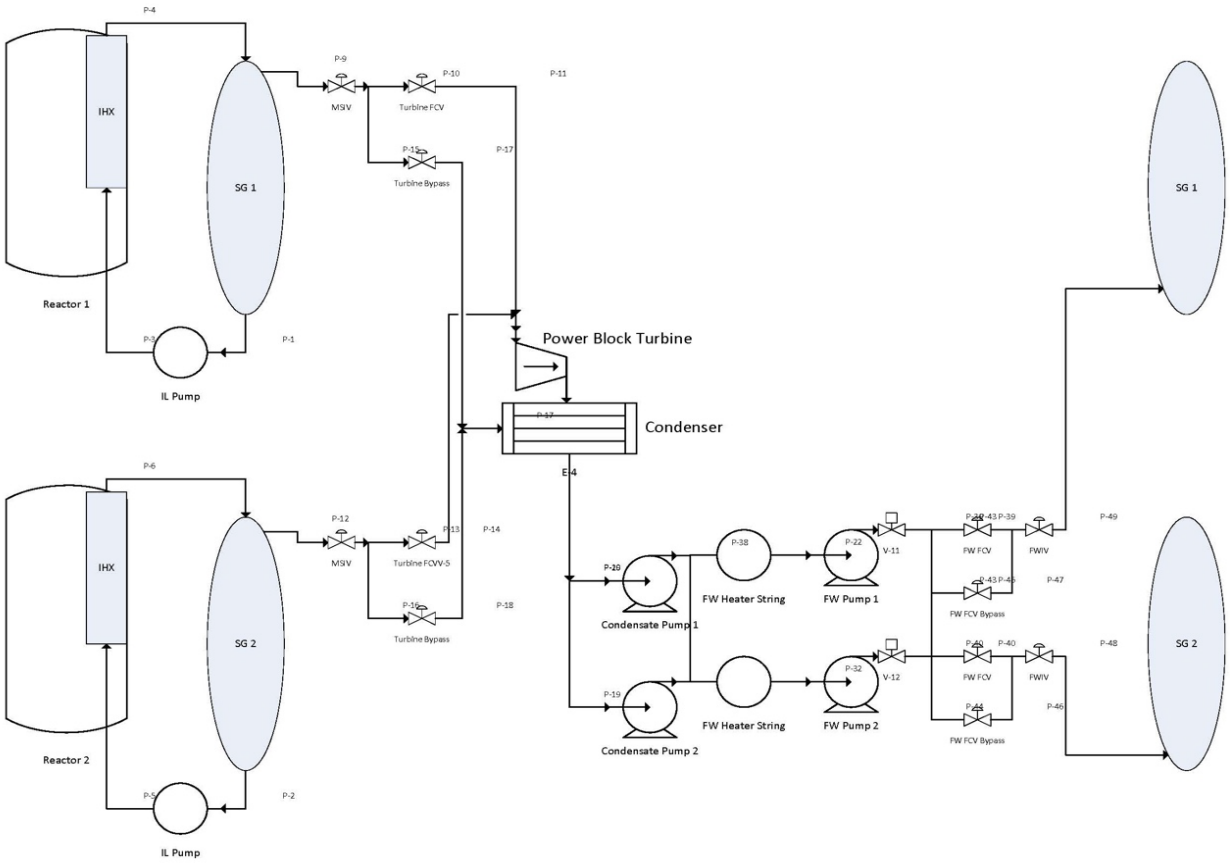

Figure 5. Power conversion system for the ALMR PRISM.

2.2 WHAT DECISIONS ARE MADE

The accuracy of the probabilistic models were tested and verified based on the status of the turbine control valves (TCVs) and feedwater (FW) flow control valves (FCVs). The scenarios for the failures/degradations/out-of-service conditions for these valves are provided below.

Scenario 1: *TCV from reactor 1 drifts in closed direction*
Options:

1. Reactor trip on steam generator (SG) high-water level
2. Open the turbine bypass valve to compensate in the short term—Advise reactor operator (RO) to reduce reactor 1 power/correct TCV logic error
3. If reactor 2 is not at 100%, open reactor 2 TCV—Advise RO to reduce reactor 1 power/correct TCV logic error

4. Decrease FW flow to SG 1—Advise RO to reduce reactor 1 power/correct TCV logic error

Scenario 2: *SG 1 FW FCV drifts in closed direction*
Options:

1. Reactor 1 trip on low SG level
2. Open SG 1 bypass FCV, shut main FW FCV
3. Advise RO to manually isolate SG1 main FW FCV; investigate valve logic error
4. Decrease steam demand from SG 1 by adjusting the SG 1 turbine FCV in the closed direction and lowering generated power
5. Advise RO to reduce reactor 1 power/ investigate valve logic error /consider option 2
6. Decrease steam demand from SG 1 by adjusting the SG 1 turbine FCV in the closed direction
7. Increase steam demand from SG 2 by adjusting the SG 2 turbine FCV in the open direction
8. Maintain generated power in the short term
9. Advise RO to investigate valve logic error and adjust power on reactor 2

Scenario 3: *SG 1 FW FCV drifts in open direction*
Options:

1. Reactor 1 trip on high SG level
2. Attempt to shut main FW FCV and open SG 1 bypass FCV
3. Advise RO to manually isolate SG1 main FW FCV
4. Report valve logic error
5. Increase steam demand from SG 1 by adjusting the SG 1 turbine FCV in the open direction
6. Decrease steam demand from SG 2 by adjusting the SG 2 turbine FCV in the closed direction
7. Advise RO to investigate valve logic error and adjust power on reactor 1

2.3 HOW DECISIONS ARE MADE

Two ETs were developed to reflect the proper heat balance in the secondary cooling system:

1. Steam flow to turbine within limits
2. Cooling flow to SGs within limits.

A TCV drifting closed would reduce steam flow to the turbine. FW FCVs drifting open or closed would increase/decrease cooling flow to the SGs, resulting in overcooling/undercooling of the primary system. Failing to increase steam flow or decrease FW flow would result in a heat imbalance in the secondary cooling system and a reactor trip.

2.4 EXAMPLE

The ET for the operational decisions associated with Scenario 1 above, which is based on the steam flow to the turbine being within proper limits, is provided in Figure 6. The ET captures plant operations with 0, 1, or 2 SGs in service.

An equipment failure, or increased likelihood of failure as predicted using diagnostics and prognostics, may be reflected in more than one ET branch. For example, if TCV 1 fails, its failure is noted for both “SG 1 and 2 in operation” and “SG 1 in operation.” Decision-making options include opening/closing the turbine bypass valves to dump heat to the condenser; reducing power; manually shutting down the reactor; and, if a controlled shutdown fails, then initiating a plant scram via the RPS.

The underlying FTs for the ET branches capture the component states, including their failure modes, their being out of service, or their being available for service but not in service (important for switching TCVs, and so on).

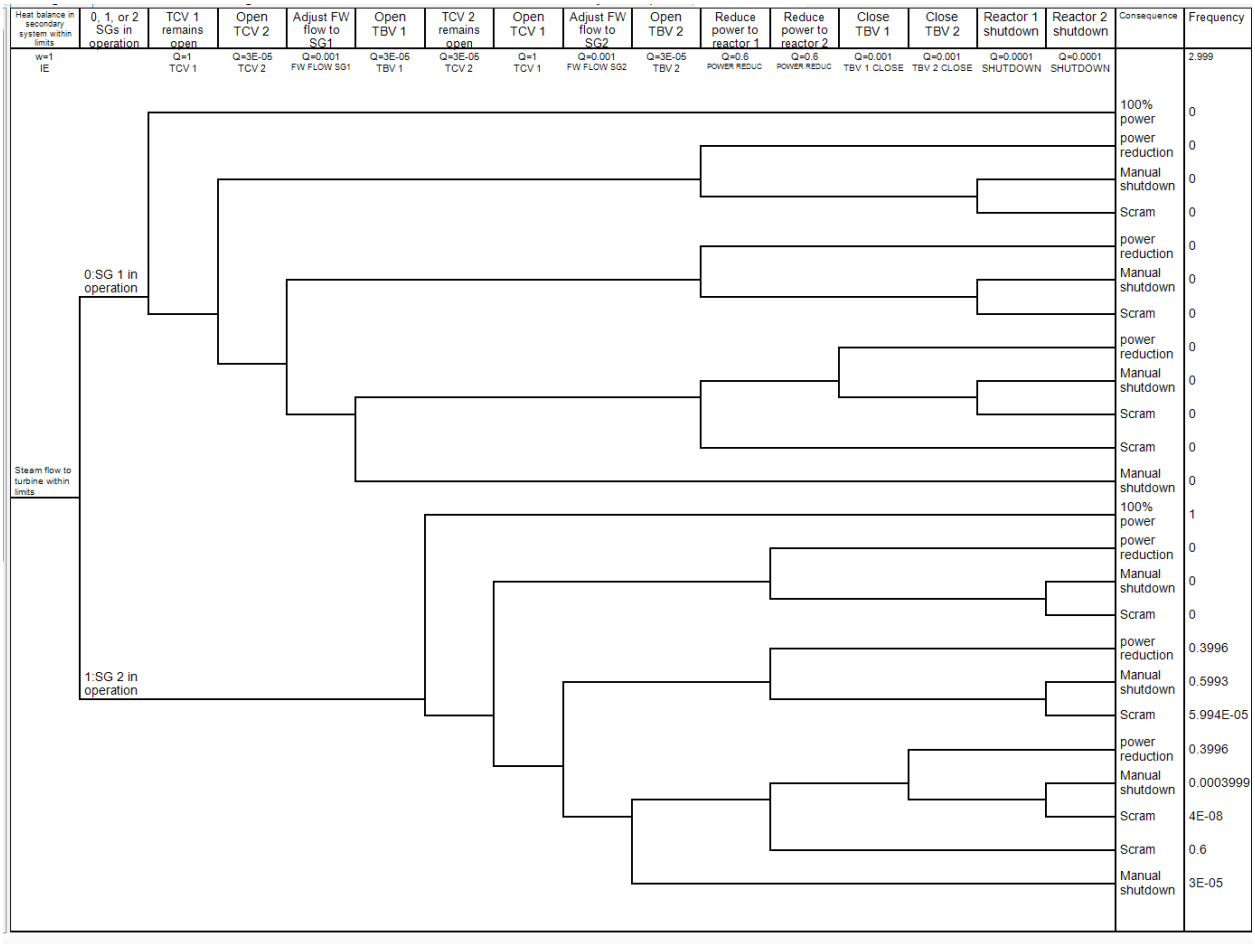

Figure 6. ET for steam flow to turbine with one steam generator in operation (Scenario 1).

FT/ET models were created to identify and rank acceptable control actions in the order of likelihood of success. ET/FT models measure the likelihood of successfully controlling the heat balance in the secondary system given the operation of one or two reactors.

The probabilistic model is based on the simplified ALMR PRISM balance-of-plant (BOP) model and accurately represents redundancies to identify alternate heat rejection paths. This model does not follow the conventional PRA FT/ET construction guides for failures but uses the success paths of the ET branches. The ultimate objective of the SCS is to keep the normal heat-rejection path open to maintain operations within limits. The objectives are to maintain steam flow to the turbine generator and FW flow to the SGs. The linked FTs track the status (including health) of the components. A components failure or unavailability is transmitted by the SCS to the FT, which then transmits that information to the ET. Figure 7 shows the success paths with both reactors operating at 100% power.

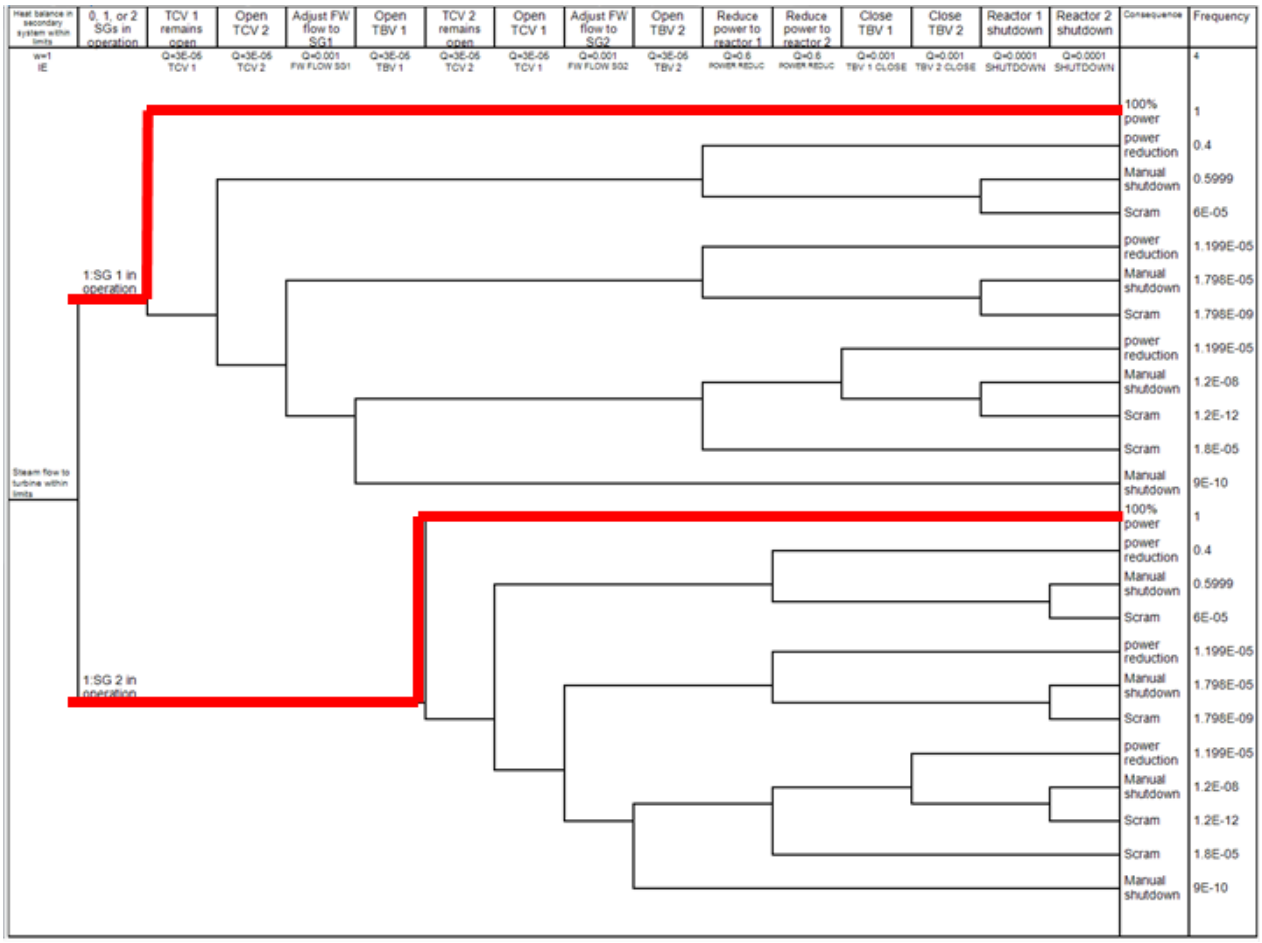

Figure 7. ET showing both reactors operating at 100%.

The initiating event for Scenario 1 is that TCV 1 fails while both reactors are operating at 100%. The following are the decision-making options based on the likelihood of success (Figure 8):

1. Decrease FW flow to SG1, shut down reactor 1.
2. Decrease FW flow to SG1, reduce reactor power.
3. Open turbine bypass valve (TBV), reduce power, close TBV.

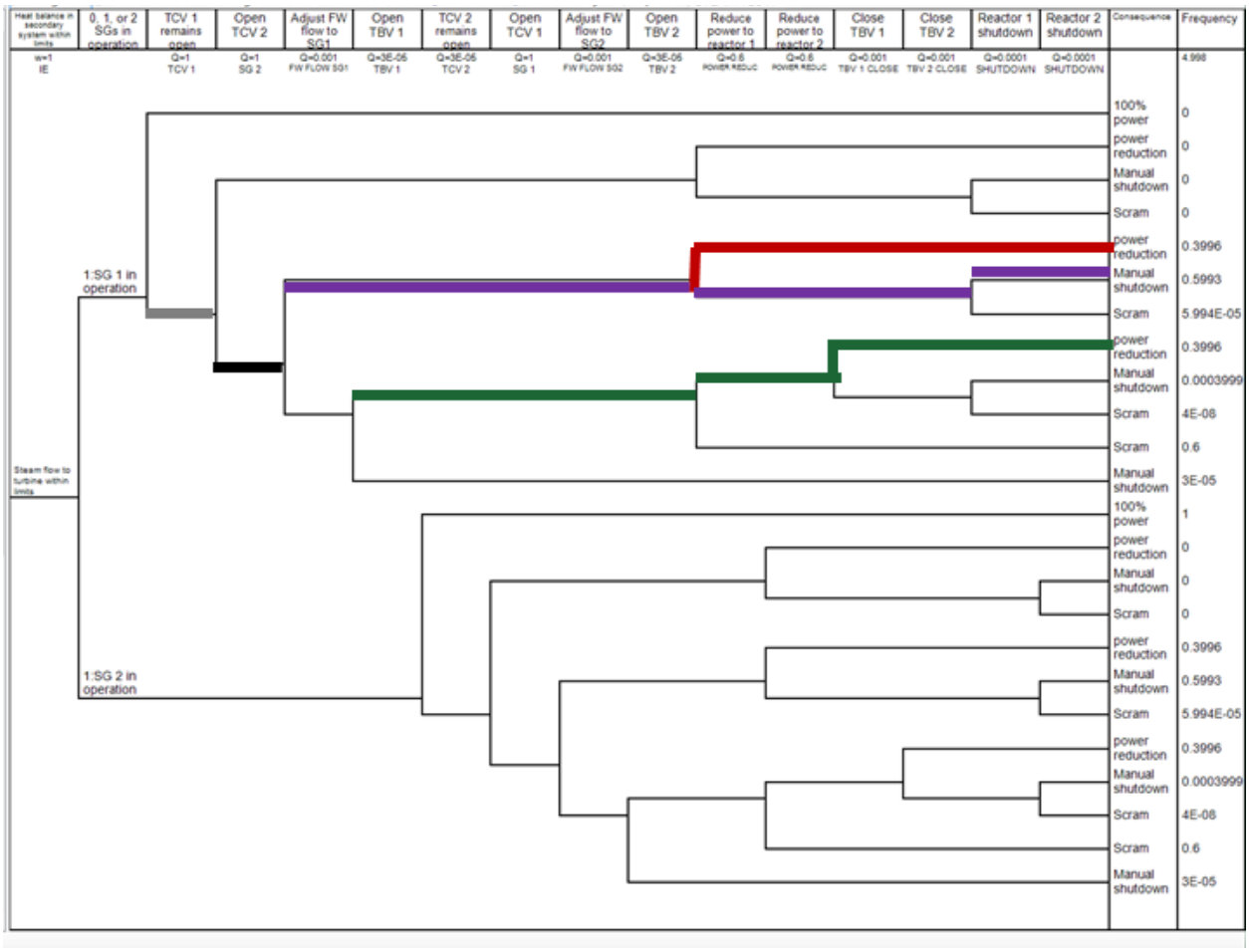

Figure 8. ET after TCV 1 fails with both reactors operating at 100%.

FTs account for equipment degradation, fault, and out-of-service conditions as well as associated SCS actions (Figure 9). FTs capture

- availability of component
- component health
- control option(s)
- component failures
- maintenance (out of service)

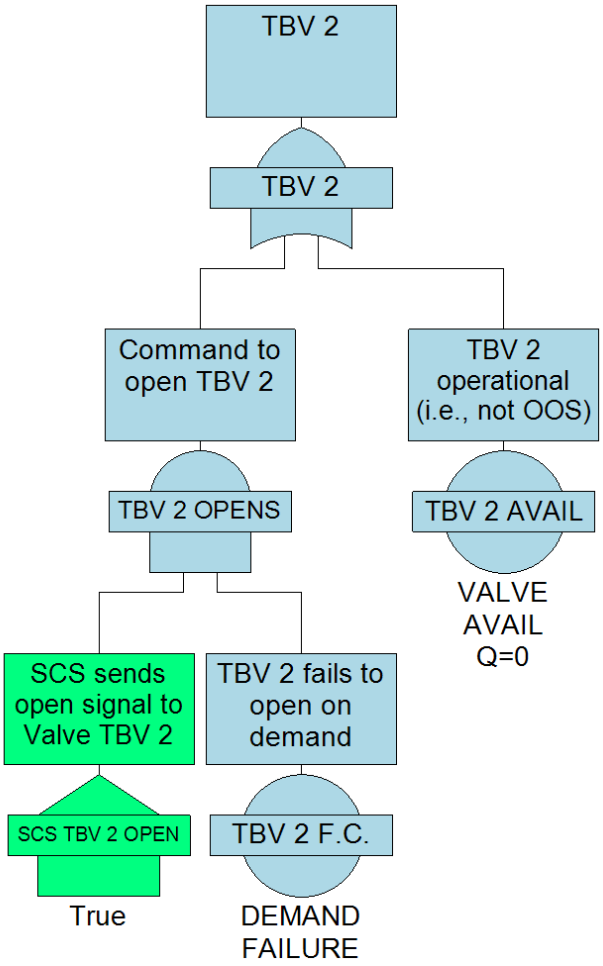

Figure 9. FTs capture component failures and carry SCS command options. (OOS = out of service).

3. SYSTEM MODEL

The system model is based on the design specifications provided in the ALMR PRISM Preliminary Safety Information Document (PSID) [11]. A sufficiently detailed system model is essential in evaluating the impact of set of control actions identified as a result of the decision-making algorithm, and ultimately assessing whether the action set is acceptable for execution.

This report provides a detailed account on the modeling activities for the ALMR PRISM power conversion system (PCS). Modeling for the other key systems was accomplished under a separate project, which delivered an end-to-end simulation toolkit *TRANSient Simulation Framework of Reconfigurable Models* (TRANSFORM). The necessary details of the deterministic decision-making analysis needed to accomplish the objectives of this task required that more complex system features be captured in the ALMR PRISM PCS model.

3.1 ALMR PRISM POWER CONVERSION SYSTEM DESIGN DESCRIPTION

The ALMR PRISM plant reference design uses nine standard reactor modules, which provide a combined thermal power output of 3,825 MW(t). Each reactor module is a 425-MW(t) pool-type liquid metal reactor design connected to its own intermediate heat transport system (IHTS) and steam generator system (SGS). Steam from three SGs is piped to a single turbine/generator to form a power block of about 415 MW(e). Each reference plant contains three power blocks with a combined electrical generation capacity of 1,245 MW(e). A simplified end-to-end system diagram is shown in Figure 10, and a diagram for the primary and secondary sodium transport systems is shown in Figure 11.

Each reactor module is equipped with two intermediate heat exchangers (IHXs) that connect to a common IHTS with a single SG. The existing TRANSFORM toolset has a fairly detailed model of the ALMR PRISM primary heat transport system, IHX, IHTS, and SGS. This project enhanced the SGS model for fidelity and significantly improved the PCS model to create an analogous model to the probabilistic model. Figure 12 provides mass and heat balance data for the ALMR PRISM SGS and the PCS under steady state conditions.

A high-level flow diagram for the ALMR PRISM PCS is shown in Figure 13. Near-saturated steam is supplied from three SGs to the turbine high-pressure section through a common header. The steam exhausted from the high-pressure turbines is directed to the two low-pressure turbines via moisture separators and single-state reheaters. Steam from the low-pressure turbines is then exhausted to a condenser. Condensate from the condenser is piped to a manifold and pumped by three 33%-capacity condensate pumps to a series of FW heaters. The condensate flows through two 50%-capacity low-pressure FW heater trains consisting of four heaters per train. Then the condensate is discharged to a deaerator, from which FW is pumped by three 33%-capacity FW booster pumps in series with three 33%-capacity FW pumps. After passing through a single high-pressure FW heater, the FW is then discharged to the three SG drums. FW from each SG drum is recirculated by a 100%-capacity pump through the associated SG. Steam from the three drums is piped to a manifold and is used to supply the turbines.

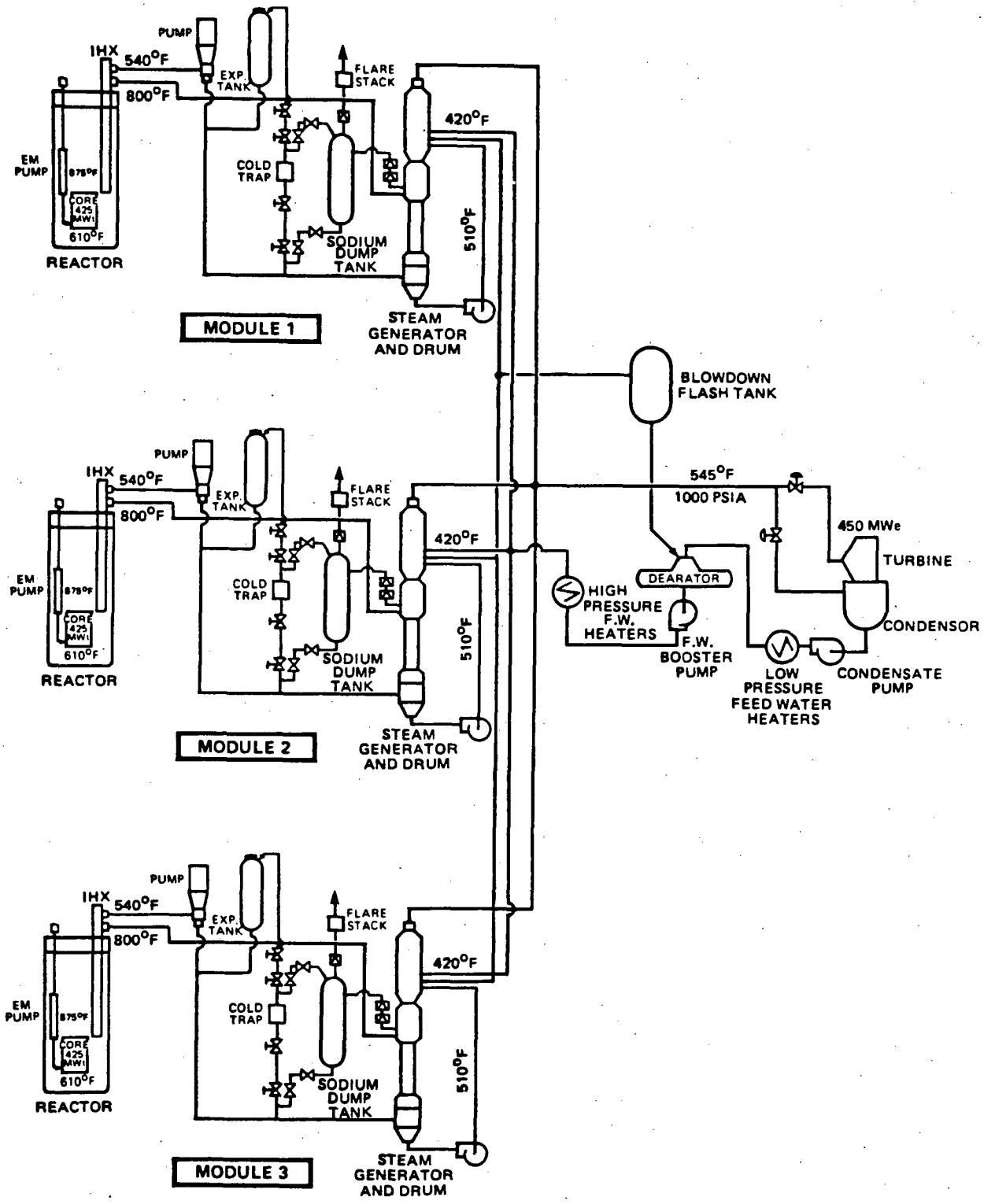

Figure 10. An end-to-end simplified system diagram of an ALMR PRISM power block [11].

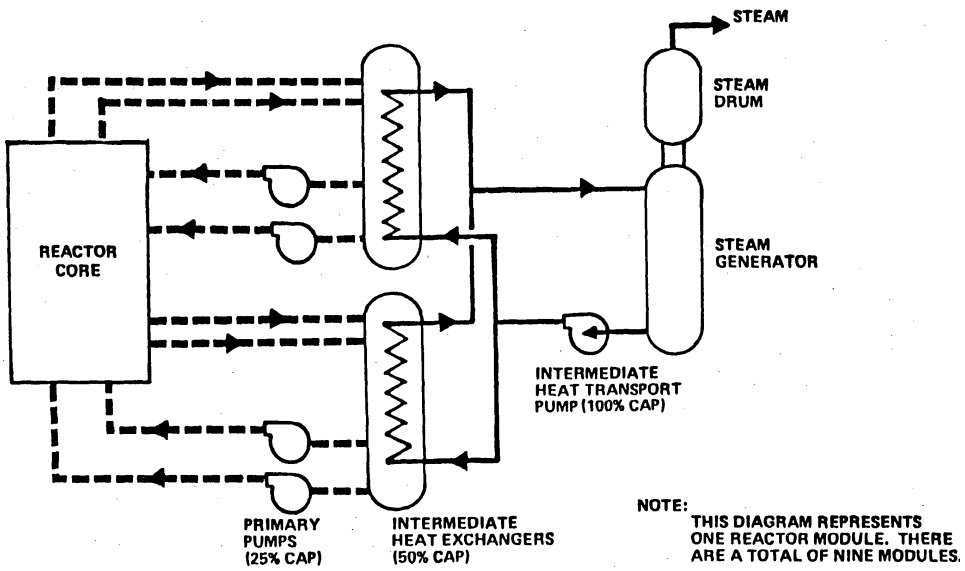

Figure 11. ALMR PRISM primary and secondary sodium transport systems [11].

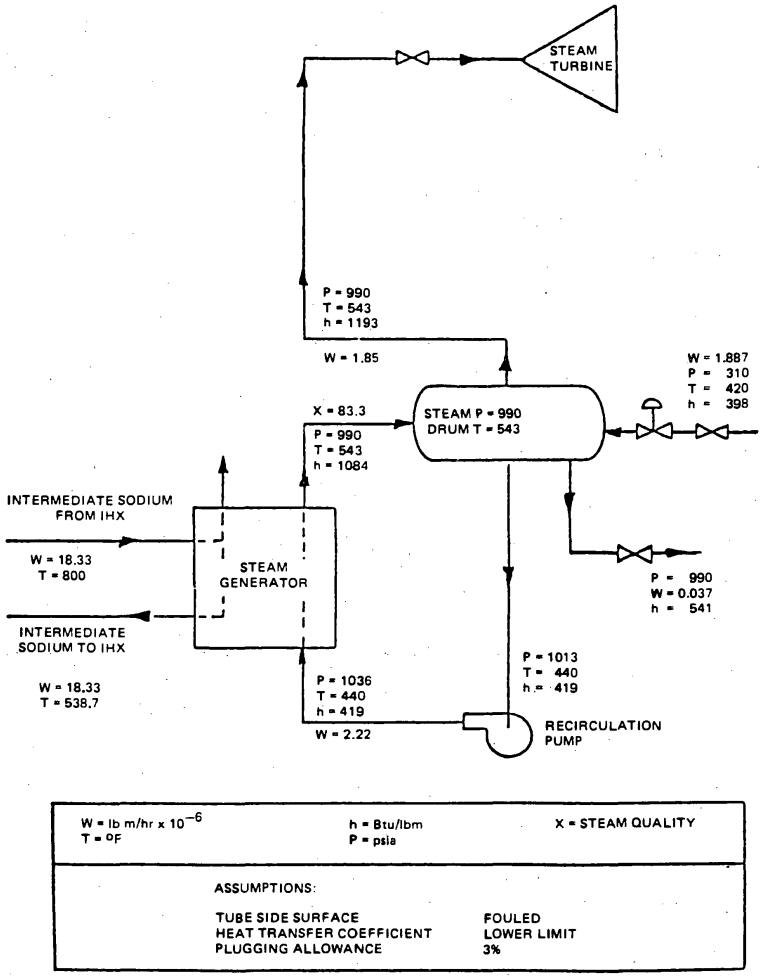

Figure 12. ALMR PRISM steam supply system and recirculation loop mass and energy balances [11].

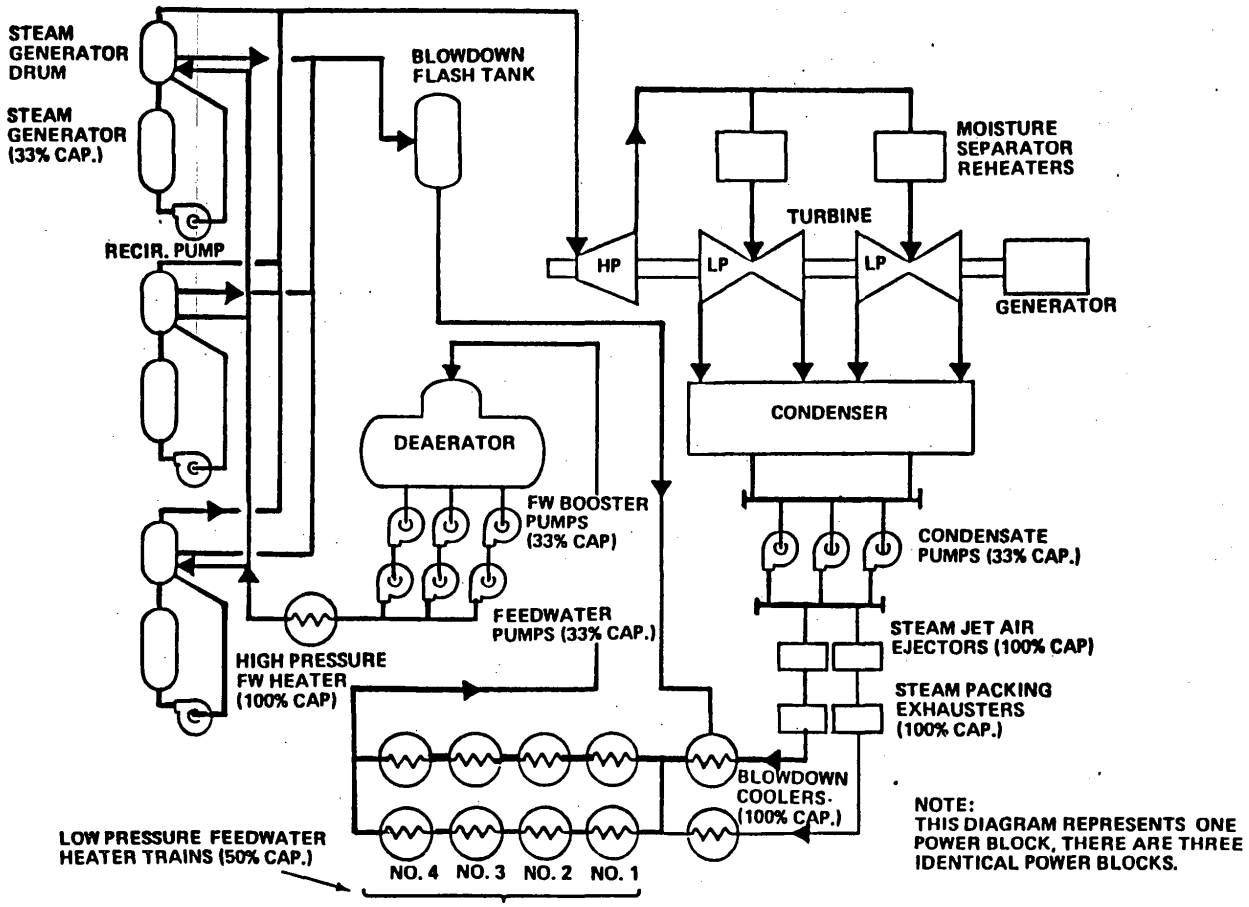

Figure 13. ALMR PRISM PCS flow diagram [11].

3.2 ALMR PRISM POWER CONVERSION SYSTEM MODEL

The simplified PCS model developed for the supervisory control project in Modelica is shown in Figure 14. This model contains high-pressure and low-pressure turbines, a generator, a condenser, a condensate pump, a low-pressure FW heater, a deaerator, a booster pump, and a high-pressure FW heater. Essentially, this model combines four low-pressure FW heaters into a single FW heater. This simplification was needed to match the system model to the probabilistic model developed according to the diagram in Figure 6. Currently, a redundant condensate path has not been implemented, but it will be added as part of the ongoing modeling effort.

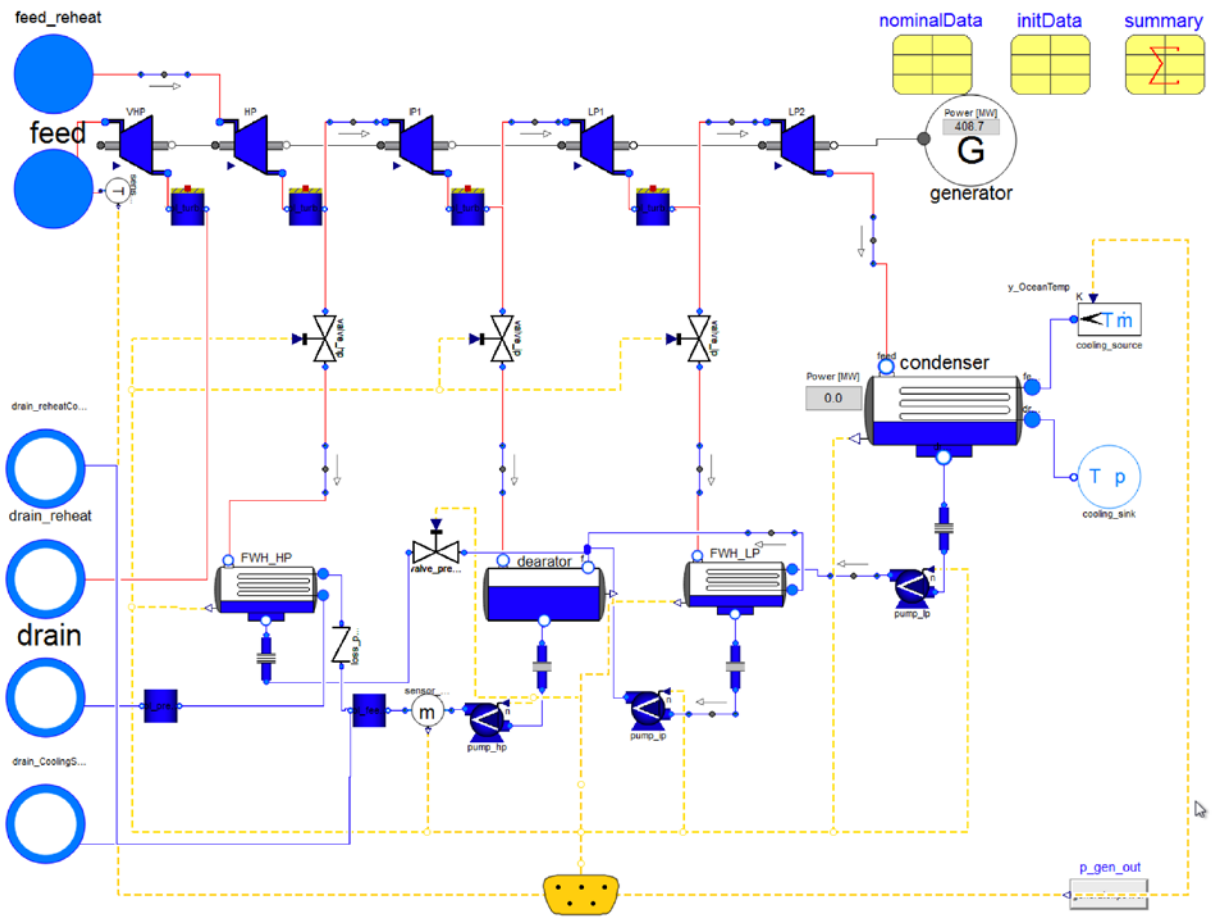

Figure 14. ALMR PRISM PCS model developed for the SCS.

The PCS model in Figure 14 provides the necessary interfaces to manipulate the turbine FVCs, the low-pressure and high-pressure FW FCVs, recirculation flow control set points, and low-pressure and high-pressure FW pump controller set points. Currently, the main steam isolation valve (MSIV) has not been modeled. The primary function of the MSIV is to redirect the main steam to the condenser in the event of a turbine or reactor trip. It is a safety-related component, and functionally it is isolated from the SCS. However, including the MSIV is essential to demonstrate a key trip function in the event of a trip set point violation. The MSIV will be developed and added into the model as part of the ongoing modeling effort.

The FW heater model closely resembles that of a RELAP5 FW nodalization scheme, as shown in Figure 15. While the FW flows on the tube side of a horizontal shell-and-tube heat exchanger and is slowly heated up, the extracted steam flows on the shell side and condenses. Because of the condensation, the shell side has a mixture of saturated water and steam. The water level is typically tracked by a dedicated control system for proper operation of the component. These control features are considered to be important, even though their importance has not been demonstrated yet, in providing the SCS with ample options for decision-making.

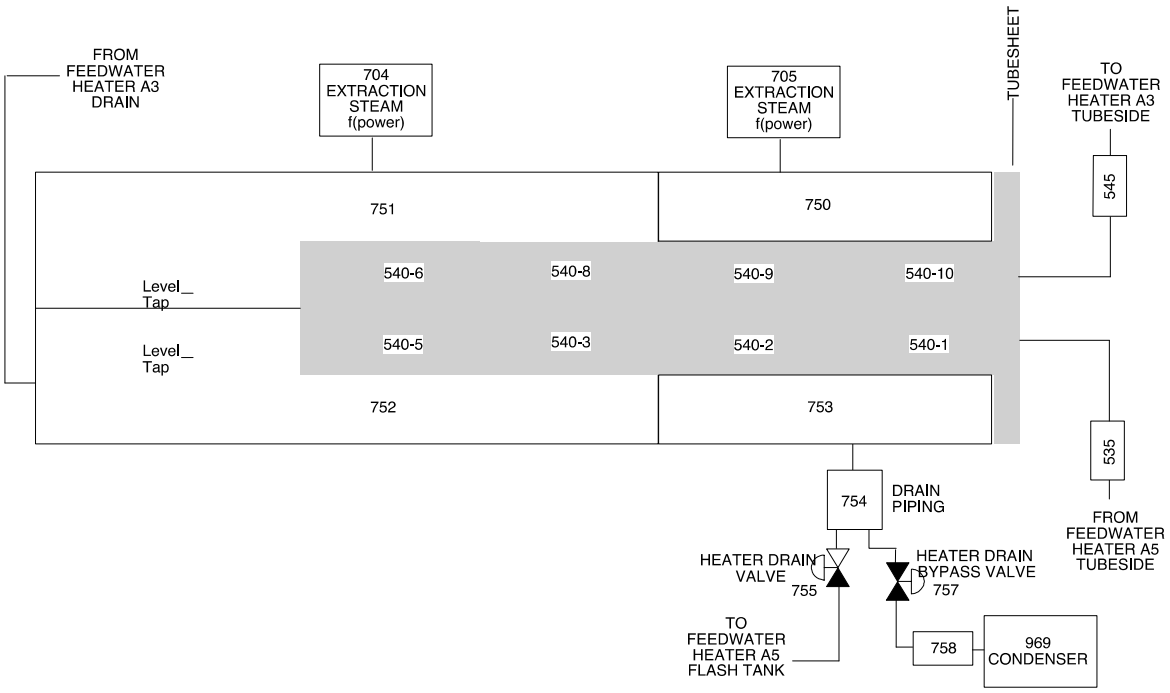

Figure 15. A typical nodalization example of a horizontal feedwater heater in RELAP5.

It should be noted that the ALMR PRISM PSID provides significant details for major plant structures, systems, and components. However, the design data for the turbine side are rather sketchy, as no detailed information is provided for the sizes of components such as FW heater heat exchangers, pumps, and valves. A detailed design of the ALMR PRISM PCS is not part of the project scope. Hence, the ORNL team is using the available data in the ALMR PRISM PSID and filling in the missing data with minimal design work and engineering judgement. Therefore, component sizing is expected to be suboptimal. However, although the suboptimal configuration affects the overall thermodynamic efficiency of the system, it should have limited impact on the dynamic response of the system.

3.3 ONGOING WORK

The key ALMR PRISM PCS components are now adequately represented in the model. Details are being added particularly for the demonstration of key decision-making capabilities, such as choosing between multiple control options.

4. DIAGNOSTICS AND PROGNOSTICS

A requirement of deterministic decision-making is knowledge of the physical behavior of a system, i.e., the time evolution of physical variables for a known disturbance. A system is said to be deterministic if its future state does not involve random behavior. Hence, a deterministic model is a representation of a system behavior that will produce the same set of outputs for a given set of inputs and for the same initial state. Typically, the deterministic behavior of a system is represented by a set of differential, difference, or algebraic equations.

The deterministic decision-making framework is intended to provide the necessary interfaces for the probabilistic portion, and to generate a resolution, i.e., a single solution, of the decision-making process.

Within the supervisory control framework, knowledge of component condition and expected time-to-failure is useful for

- Proactive decision-making and control to ensure that incipient failures of some components do not result in unanticipated shutdowns

- Improved control decision-making based on the potential for component failures as a result of specific supervisory control decisions.

The challenging environments in advanced reactors, such as sodium-cooled fast reactors and high-temperature reactors, and their small modular counterparts, increase the possibility of degradation of safety-critical active and passive components. They also pose a challenge for the deployment and extended operation of advanced reactors. However, the new designs also provide the opportunity to introduce new technologies to increase performance and safety, offer opportunities for advanced diagnostics to identify potential component degradation, and provide improved economics.

Traditional approaches to detecting and managing degradation may have limited applicability to advanced reactors, given the expectation of longer operating periods and potential difficulties with inspection and testing access to critical components because of integrated and compact designs. Addressing the need for operation and maintenance (O&M) decision support based on enhanced situational awareness will require techniques to integrate advanced plant configuration information, equipment condition information, and predictive risk monitors [12].

Critical to decision-making based on component condition is the ability to determine the potential risk to continued operation of the plant. Ideally, the risk estimate is predictive in nature and incorporates the probability of component failure over time given the degradation state of the component at the present time. Existing risk models, such as the PRA, provide a static representation (point-in-time estimate) of the system risk given the current plant configuration (e.g., equipment availability, operational regime, and environmental conditions). Technologies for characterizing predictive risk (enhanced risk monitors, or ERMs) take into account plant-specific normal, abnormal, and deteriorating states of systems, structures, and components (SSCs) in the estimation of current and future risk to safe and economic operation.

Essentially, ERMs are risk monitors that incorporate time-dependent failure probabilities from prognostic health management (PHM) systems to dynamically update the risk metric of interest. However, a key question in the deployment of PHM is the ability to carry out unsupervised, yet risk-informed decisions based on the information provided by the PHM system. PNNL's ERM methodology would contribute to the diagnostic and prognostic portion of the supervisory control decision-making capabilities by anticipating future changes in the condition of key components and associated key risk metrics.

Rather than include generic aging models (for example, linear aging models in which the failure probability increases linearly over time), PNNL's general approach to achieving ERM (Figure 16) uses the condition of the component to calculate the failure probability. These equipment condition assessment (ECA) data are used to predict the condition (along with confidence levels in the prediction) at some point in the future (prognostics). The predicted condition, in the form of a probability of failure (POF), is integrated into risk monitors, resulting in an ERM.

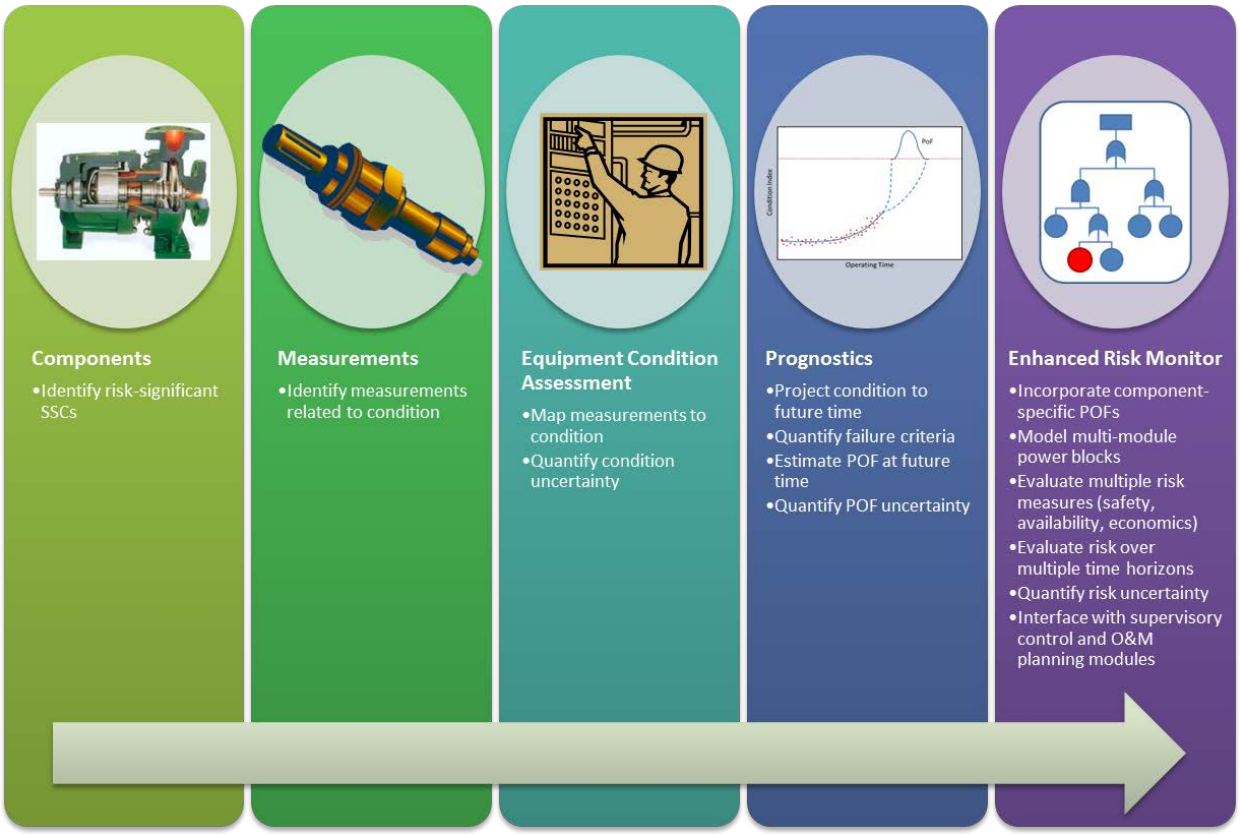

Figure 16. Considerations and steps to achieving an enhanced risk monitor [13].

Both ECA and prognostics may be applied to the monitoring of many components and subsystems within an advanced reactor. However, doing so increases the amount of information that must be aggregated before it is used with risk monitors and in plant supervisory control actions. Figure 17 shows a possible scenario for the aggregation: each PHM module is associated with a risk monitor, resulting in predictive estimates of the subsystem health and the associated risk metrics. This information is used to augment data used for supervisory control and plant-wide coordination of multiple modules by providing the incremental risk incurred, due to aging or other degradation, and demands placed on components that support mission requirements.

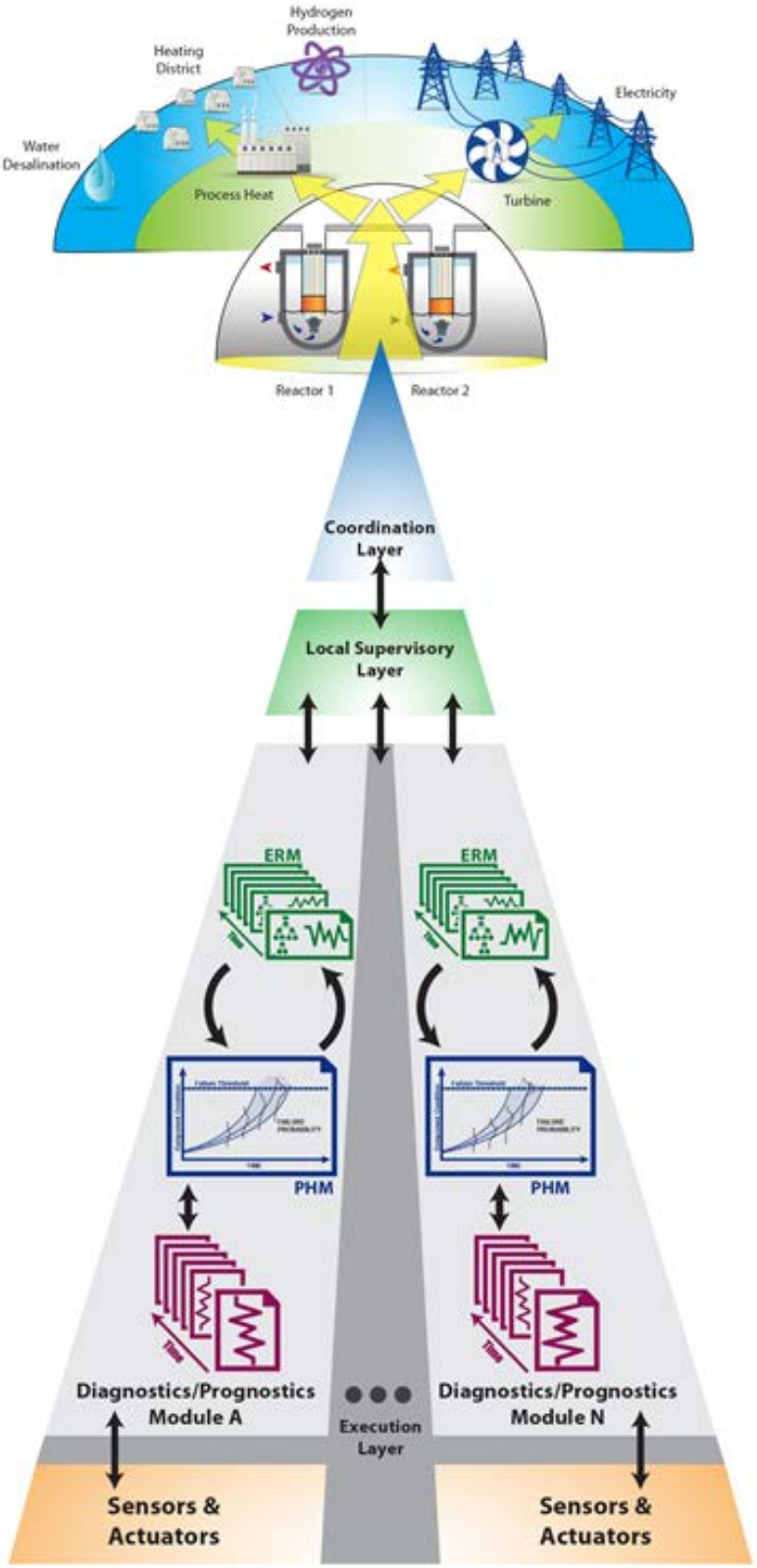

Figure 17. Schematic showing the integration of PHM systems with ERMs and their functionality within the hierarchy of a supervisory control system for advanced reactors [14]

4.1 SUMMARY OF PNNL'S PROTOTYPIC ERM FRAMEWORK FOR ADVANCED REACTORS

This section briefly describes the PNNL methodology for prototypic ERMs that integrate ECA for dynamic characterization of system risk. Details of PNNL's methodology are documented in previous Advanced Reactor Technologies reports [12, 13, 15, 16] and are summarized here for convenience.

ERMs require the integration of two sets of technologies—risk monitors and ECA/prognostics. ECA process measurements (e.g., flow, temperature, and pressure) or performance measurements (e.g., pump efficiency) are used to identify departures from normal operation and characterize the condition in terms of various condition indices. Health monitoring, as part of PHM, would provide condition indicators for key equipment using online, in situ sensors and measurements to support the detection and identification of incipient failure and to reflect evolving degradation. This is particularly important for SSCs proposed for use in advanced reactor designs that differ significantly from those used in the operating fleet of light water reactors (or even in light water reactor–based small modular reactor designs), as operational characteristics for the SSCs based on operating experience may not be fully available.

PNNL has developed a prototypic ERM methodology that incorporates a PRA model of the plant. Based on predictive estimates of component failure over time, time-dependent risk metrics such as the CDF may be computed and analyzed. Additionally, alternative risk metrics that quantify the normalized cost of repairs, replacements, or other O&M actions may be computed through an economic risk model.

PNNL's ERM methodology substitutes the assumption of static failure rates in risk monitors with component-specific time-dependent versions that are evaluated based on the current condition of the equipment [12, 13, 17]. This ERM approach tracks the actual condition of the component to predict the change in failure probability over time. This realistic profile of failure probability is used to develop a predictive estimate of the operational risk. The approach allows for an SCS to leverage these estimates of component condition and predictive risk for plant-wide coordination of multiple modules. A typical application would be to mitigate incremental risk incurred from aging and operational demands placed on mission-supporting components.

The ERM methodology also allows computation of the economic risks of actions such as deferring a maintenance activity given the current component condition and future anticipated degradation. Such an integration of safety and economic risk metrics provides a convenient mechanism for assessing the impact of O&M decisions on the safety and economics of the plant.

This prototypic methodology has been evaluated [14] using a hypothetical PRA model, generated using a simplified design of a liquid-metal-cooled advanced reactor. Component failure data, from an industry compilation of failures of components similar to those in the simplified advanced reactor model, were used to initialize the PRA model. The changes in CDF over time were computed and analyzed by using a time-dependent POF, which grows from the initial probability when equipment is in like-new condition to a maximum POF before a scheduled maintenance action to restore or repair the component to "as-new" condition. Uncertainties were incorporated and propagated through the calculations to provide an estimate of uncertainty bounds in the component failure probabilities, as well as in the predictive risk metrics.

4.2 ERM SOFTWARE FUNCTIONAL DESCRIPTION

Functionally, the three key elements that make up the ERM software are

1. ECA and prognostics
2. predictive risk assessment
3. uncertainty quantification

4.2.1 Equipment Condition Assessment and Prognostics

The core function of this module is to estimate the probability of failure of selected components at future times, given measurements that are sensitive to the current condition of these components. This module, therefore, is dependent on the availability of appropriate sensor measurements, which may be indirect assessments (such as process measurements) or direct assessments (such as vibration) of component condition.

The module also depends on the availability of one or more models of degradation accumulation and growth that account for the specific failure modes of interest. For example, pumps can fail as a result of erosion caused by cavitation or of seal failure. Diagnostic models that relate the measured quantities to one of these failure modes, and corresponding models that describe the growth of the degradation until failure of a component to perform its function, are both required. Such models may be adapted from existing data and models in the literature or derived specifically using laboratory and field experiments.

4.2.2 Predictive Risk Assessment

The core function of this module is to estimate the risk (in the form of CDF and economic risk) at future times given the predicted probabilities of failure. The module is therefore dependent on the availability of information from the ECA/prognostic module described earlier. This module is also dependent on the availability of appropriate risk models. Research to date has used PRA models for the CDF calculation and a hypothetical economic model for the economic risk calculation. The risk assessment is itself done in an iterative fashion, with each iteration using an updated POF.

The PRA and economic models, in turn, depend on information about initial component failure probabilities. As described earlier, these are derived from available information about failure probabilities of similar components.

4.2.3 Uncertainty Quantification

This module uses the previous two modules and provides an estimate of the uncertainty in the POF and predicted risks, based on user-provided information about the sources of uncertainty. Essentially, this module uses the input uncertainties and the prognostic and risk assessment modules to calculate output uncertainties.

4.2.4 Supervisory Control Interface

Functionally, the interface for the ERM with the SCS is shown in Figure 4, within the block labeled “Diagnostics and Prognostics.” The ECA/prognostics module provides the necessary information to implement this block, which is a critical input to the decision-making block within the supervisory control framework. In this initial stage of the integration, the information from the predictive risk assessment is not expected to be used. However, future stages of integration are likely to use it within the “Decision Making” block shown in Figure 4.

4.3 SUMMARY AND ONGOING WORK

ERMs are capable of providing predictive estimates of the POFs of monitored components, as well as the associated predictive risk to system operation. Such information is likely to be of value to supervisory control algorithms, as knowledge about potential failures can be used to make operational decisions. The ERM framework developed by PNNL consists of three major functional modules that use sensor measurements and provide predictive estimates of component failure probabilities, operational risk, and the associated uncertainties. Functionally, these modules may be integrated with the supervisory control framework to provide the necessary diagnostic and prognostic information upon which the control decisions are made. In addition, information on risk to system operation is likely to be of value in the decision-making process; however, it is expected that such information will not be used at the initial stages of integration and testing.

Ongoing activities to integrate the ERM with the supervisory control framework, and evaluate the combined technology, are organized around three shared scenarios within a reference plant design. These scenarios focus on valve failures and provide a simple mechanism for integrating and testing the ERM. Additional scenarios will be incorporated as necessary in the future.

5. DOMAIN OF AUTONOMOUS CONTROL

The desired outcome of the decision-making process is to prevent the system variables from meeting or exceeding a trip set point value. The deterministic decision-making process is used to capture the physical behavior of a system, i.e., the time evolution of physical variables for a known disturbance. That is, the deterministic decision-making framework provides the necessary interfaces for the probabilistic portion to validate the choices for avoiding a trip set point. Combined, the deterministic/probabilistic process generates a resolution, i.e., a single solution, of the decision-making process.

5.1 RELATIONSHIP TO TECHNICAL SPECIFICATIONS AND LCOs

Section 182a of the Atomic Energy Act requires applicants for NPP operating licenses to include Technical Specifications (TSs) as part of the license (42 U.S.C. § 2232). The licensee provides TSs to maintain the operational capability of SSCs that are required to protect the health and safety of the public. The Nuclear Regulatory Commission (NRC) regulatory requirements related to the content of the TSs are found in 10 CFR § 50.36, "Technical specifications" [18]. This regulation also requires the TS to include LCOs and defines LCOs as the lowest functional capability or performance levels of equipment required for safe operation of the facility. The regulation requires that when an LCO is not met, the licensee shall shut down the reactor or follow any remedial actions permitted by the TS until the condition can be met.

Protective instruments are provided with set points at which specific actions are either initiated, terminated, or prohibited. Set points correspond to certain provisions of TSs that are incorporated into the facility operation license. NRC Regulatory Guide RG 1.105, Rev. 3 [19] describes a method acceptable to NRC staff of complying with NRC regulations for ensuring that set points for safety-related instrumentation are initially within and remain within TS limits. RG 1.105 designates the allowable value for a trip set point as the limiting safety system setting (LSSS). In association with the trip set point and LCOs, the LSSS establishes the threshold for protective system action to prevent acceptable limits being exceeded during design basis accidents. The LSSS therefore ensures that automatic protective action will correct the abnormal situation before a safety limit is exceeded.

ISA-67.04.01-2006 provides the relationship between trip set points, analytical limits (ALs), and safety limits (SLs) [20]. Trip set points are chosen to ensure that a trip or safety actuation occurs before the process reaches the AL. The AL is the value of a given process variable at which the safety analysis models the initiation of the instrument channel protective action. Performance of the safety analyses with conservative ALs demonstrates that the established SLs and other acceptance criteria are not exceeded during normal plant transients, anticipated operational occurrences, and other design basis transients. SLs are chosen to maintain the integrity of these physical barriers. SLs can be defined in terms of directly measured process variables such as pressure or temperature. The SLs or LCOs are included in the facility TSs.

A plant's TSs contain the restrictions the operators consult during operation and are a chapter of the plant's Final Safety Analysis Report. All of the plant's operating procedures are checked against the TSs.

5.2 KEY OPERATIONAL TRANSIENTS

The deterministic decision-making module incorporates the physical behavior (current and projected) of the system. To achieve that capability, the utility variables must be selected so that the projected physical behavior of the system can be factored into the decision-making with the probabilistically-ranked options from the PRA calculation. This is best accomplished by linking the desired utility attributes to key process variables, i.e., the ones that provide insight about the status of the system. A partial list of system design variables for ALMR PRISM and their nominal steady-state values are shown in Table 1.

Table 1. ALMR PRISM heat transport system design values

Variable	Description	Nominal value	Unit
$\dot{Q}_{R_X}$	Reactor thermal power	425	MWt
$T_{R_{Xo}}$	Reactor outlet temperature	468.3	ºC
$T_{R_{Xi}}$	Reactor inlet temperature	321.1	ºC
ΔT_{R_X}	Reactor temperature difference	147.2	ºC
ω_p	Primary coolant mass flow rate (total)	2016	kg/s
$\omega_{p,\,disc}$	Primary pump discharge volumetric flow rate*	0.66	m^3/s
h_p	Primary pump head	96.3	m
T_{hl}	Intermediate hot leg temperature	426.67	ºC
ω_i	Intermediate coolant mass flow rate (total)	2268	kg/s
$\omega_{i,\,disc}$	Intermediate pump discharge volumetric flow rate	2.6	m^3/s
h_i	Intermediate pump head	95.7	m
$\dot{Q}_{SG}$	Steam generator thermal power**	432	MWt
$T_{SG,o}$	Steam generator outlet temperature	285	ºC
$p_{SG,\,o}$	Steam generator outlet pressure	6.895	MPa
$T_{SG,\,fw}$	Steam generator feedwater temperature	216	ºC
ω_{SG}	Steam flow rate	233.5	kg/s

* Volumetric flow rate per pump; total of four pumps.
** Including pump heating from primary loop, intermediate loop, and steam generator pumps (~ 6.82 MWt).

The selection criteria for utility variables must address the safety envelope of the controls domain. The fundamental objective of the SCS is to maintain the plant state within the controllable domain. In its simplest form, exceeding the trip variables initiates an RPS and/or ESFAS actuation. Reactor safety functions and associated trip variables are listed in Table 2.

Table 2. List of reactor trip variables and associated safety functions

	Safety function	Monitored variable	Type
Flux	Monitor for insertion of reactivity (threshold function of operating power level)	Reactor core neutron flux	TRIP
Flow	Monitor for loss of flow*	Primary loop sodium level	TRIP
		Primary loop EM pump discharge pressure	
Temperature	Monitor for loss of heat sink	Reactor core outlet temperature	TRIP
		Cold pool temperature	
Level	Monitor for loss of sodium	Primary loop sodium level	TRIP
Pressure	Monitor for electromagnetic pump outlet duct failure	Primary loop electromagnetic pump discharge pressure	TRIP

* The loss-of-flow measurement is indirect using the electromagnetic pump discharge pressure as an indicator of the primary loop flow rate.

However, the SCS tries to confine the plant state within an even tighter domain. Similarly, to incorporate a broader snapshot of the plant state, additional utility attributes must be linked with key process variables.

ALMR PRISM RPS actuates on the following trip variables [11]:

1. measured reactor core neutron flux (φ)
2. reactor core outlet temperature ($T_{R_{Xo}}$)
3. cold pool temperature ($T_{pool,cold}$)
4. pump discharge inlet pressure (p_{disc})
5. primary loop sodium level (y_{PHTS})

In addition to the RPS trip variables identified in the ALMR PRISM PSID [11], the following additional variables were identified as other important decision variables:

1. reactor core coolant temperature difference (ΔT_{R_X})
2. intermediate loop sodium level (y_{IHTS})
3. steam generator drum level (y_{SG})
4. steam generator FW inlet flow rate (ω_{fw})

To maintain consistency among the attributes, the utility variables are derived from the process variables through a simple linear transformation:

$$x_i = \frac{p_i - (p_i)_{min}}{(p_i)_{max} - (p_i)_{min}}$$

where x_i is the utility variable for the *i*th attribute, and p_i is the process variables linked to x_i; subscripts min and max are the minimum and maximum values each process variable is allowed to take. For safety-related variables, i.e., trip variables, these values are based on the set points of their processes from plant TSs.

6. CONCLUSIONS AND FUTURE WORK

This report documents the technical accomplishments for incorporating ERMs into the supervisory control decision-making framework. Furthermore, it expands the use of probabilistic decision-making through an application in the BOP systems of the ALMR PRISM power block. Similarly, the BOP systems are also captured in a systems model implemented in Modelica.

Previously, it was demonstrated that FTs and ETs, if constructed in a distinct way, can be used to automatically identify available decision options and to generate a state trajectory (i.e., a set of corrective actions) to move the system from a troubled state to an acceptable state. The capability was shown with the challenge problem based on a simple hydraulic network.

FT/ET models were developed for a simplified version of the ALMR PRISM BOP systems, which include a high-pressure and a low-pressure turbine, a reheat stage, a condenser, a low-pressure FW heater, a high-pressure FW heater, a deaerator, two SGs, and various pumps and valves. The FT/ET models also accurately capture the redundancies in the BOP.

6.1 ONGOING WORK

Work is ongoing toward a fully integrated demonstration of supervisory control decision-making capabilities on an end-to-end ALMR PRISM system model, including a detailed BOP representation.

The project team is working to expand the complexity of the BOP model to include three SGs to match the specifications of the ALMR PRISM power block. Efforts are ongoing for both the probabilistic model and the systems model.

ORNL is working with PNNL on ERMs. Future work will include the identification of failure modes of key plant components, specifically certain BOP components. The ERM module will then generate critical diagnostics and prognostics information regarding component health.

The technical basis and the computational framework to accomplish the deterministic decision-making function for the SCS were also previously reported. The framework uses utility theory as the mathematical method of performing the deterministic part of the integrated decision-making function. Utility theory offers a unifying measure that takes into account the value and potential consequences of individual control actions, which are reflected in the combined utility of a decision alternative.

Integrated decision-making requires the identification and calibration of utility attributes and utility functions. The utility functions are determined based on the trip set points and other constraints that define the operational space of the SCS.

7. REFERENCES

1. Nuclear Regulatory Commission, *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, RG 1.174, Rev. 2, US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, May 2011.
2. Nuclear Regulatory Commission, *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, RG 1.200, Rev. 2, US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, March 2009.
3. Nuclear Regulatory Commission, *Risk-Informed Security Regulations Workshop*, sponsored by the US Nuclear Regulatory Commission's Office of Nuclear Regulatory Research and Office of Nuclear Security and Incident Response, Albuquerque, N.M., September 14–15, 2010.
4. S. M. Cetiner, M. D. Muhlheim, G. F. Flanagan, D. L. Fugate, and R. A. Kisner, *Development of an Automated Decision-Making Tool for Supervisory Control System*, ORNL/TM-2014/363 (SMR/ICHMI/ORNL/TR-2014/05), Oak Ridge National Laboratory, Oak Ridge, TN, September 2014.
5. S. M. Cetiner, M. D. Muhlheim, *Implementation of the Probabilistic Decision-Making Engine for Supervisory Control*, ORNL/SPR-2015/140, Oak Ridge National Laboratory, Oak Ridge, TN, March 2015.
6. 10 CFR 50, *Domestic Licensing of Production and Utilization Facilities*, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 1, "Quality Standards and Records," Jan. 1, 2016 edition.
7. 10 CFR 50, *Domestic Licensing of Production and Utilization Facilities*, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 13, "Instrumentation and Control," Jan. 1, 2016 edition.
8. 10 CFR 50, *Domestic Licensing of Production and Utilization Facilities*, 10 CFR 50.55a(a)(1), "American Society of Mechanical Engineers (ASME)," Jan. 1, 2016 edition.
9. Nuclear Regulatory Commission, *Standard Review Plan*, NUREG-0800, Rev. 5, Chapter 7.7, "Control Systems," March 2007.
10. Nuclear Regulatory Commission, *An Approach for Plant-Specific, Risk-Informed Decision-making: Technical Specifications*, RG 1.177, Rev. 1, May 2011.
11. *PRISM Preliminary Safety Information Document*, GEFR-00793, UC-87Ta, prepared for US Department of Energy under Contract No. DE-AC03-85NE37937 (December 1987).
12. J. B. Coble, G. A. Coles, R. M. Meyer and P. Ramuhalli, "Incorporating Equipment Condition Assessment in Risk Monitors for Advanced Small Modular Reactors," *Chemical Engineering Transactions* **33**:913–918.
13. P. Ramuhalli, E. H. Hirt, G. A. Coles, C. A. Bonebrake, B. J. Ivans, Jr., D. W. Wootan, M. R. Mitchell, *An Updated Methodology for Enhancing Risk Monitors with Integrated Equipment Condition Assessment*, PNNL-23478 Rev. 0 (SMR/ICHMI/PNNL/TR-2014/01), Pacific Northwest National Laboratory, July 2014.
14. P. Ramuhalli, E. H. Hirt, A. Veeramany, C. A. Bonebrake, W. J. Ivans, Jr, G. A. Coles, J. B. Coble, X. Liu, D. W. Wootan, M. R. Mitchell, and M. F. Brass, *Prototypic Enhanced Risk Monitor Framework and Evaluation - Advanced Reactor Technology Milestone: M3AT-15PN2301054*, PNNL-24712, Pacific Northwest National Laboratory, Richland, WA, 2015.

15. J. B. Coble, G. A. Coles, P. Ramuhalli, R. M. Meyer, E. J. Berglin, D. W. Wootan and M. R. Mitchell, *Technical Needs for Enhancing Risk Monitors with Equipment Condition Assessment for Advanced Small Modular Reactors*, PNNL-22377 Rev. 0; SMR/ICHMI/PNNL/TR-2013/02, Pacific Northwest National Laboratory, Richland, Washington, 2013.
16. P. Ramuhalli, G. A. Coles, J. B. Coble and E. H. Hirt, *Technical Report on Preliminary Methodology for Enhancing Risk Monitors with Integrated Equipment Condition Assessment*, PNNL-22752, Rev. 0; SMR/ICHMI/PNNL/TR-2013/05, Pacific Northwest National Laboratory, Richland, Washington, 2013.
17. Coble, J. B., Ramuhalli, P., Bond, L. J., Hines, J. W., and Upadhyaya, B. R., *Prognostics and Health Management in Nuclear Power Plants: A Review of Technologies and Applications*, PNNL-21515, Pacific Northwest National Laboratory, Richland, Washington, 2012.
18. 10 CFR 50, *Domestic Licensing of Production and Utilization Facilities*, 10 CFR 50.36, "Technical Specifications," January 1, 2016 edition.
19. Nuclear Regulatory Commission, *Setpoints for Safety-Related Instrumentation*, RG 1.105, Rev. 3, December 1999.
20. American National Standards Institute/International Society of Automation, ANSI/ISA-67.04.01-2006 (R2011), *Setpoints for Nuclear Safety-Related Instrumentation*, reaffirmed October 13, 2011.