OPERATIONAL PERFORMANCE RISK ASSESSMENT IN SUPPORT OF A SUPERVISORY CONTROL SYSTEM

A. Guler, M. Muhlheim, S. Cetiner
Oak Ridge National Laboratory
ayk@ornl.gov, muhlheimmd@ornl.gov, cetinersm@ornl.gov

R. Denning
Research Consultant
denningrs.8@gmail.com

ABSTRACT

A supervisory control system is being developed for multiunit advanced small modular reactors to minimize human interventions during normal and abnormal operations. In the supervisory control system, control action decisions are made based on a probabilistic risk assessment that employs event trees and fault trees. Although traditional probabilistic risk assessment tools are implemented, their scope is extended to normal operations, and the application is reversed to assess the success of non-safety related systems and to enable continued operation of the plant. This extended probabilistic risk assessment approach is called operational performance risk assessment (OPRA). OPRA helps to identify available paths, combine control actions for maintaining plant conditions within operational limits, and to quantify the likelihood of success of these operational trajectories to optimize the selection of alternative actions without activating reactor protection system.

In this paper, a case study of OPRA in a supervisory control system is demonstrated for the Advanced Liquid Metal Reactor (ALMR) Power Reactor Inherently Safe Module (PRISM) design, specifically the power conversion system. The scenario investigated involved a condition in which the feedwater control valve that was observed to be drifting to the closed position. Alternative plant configurations that would allow the plant to continue to operate at full or reduced power were identified using OPRA. Dynamic analyses were performed with a thermal-hydraulic model of the ALMR PRISM system using Modelica to evaluate the magnitude of safety margins. Successful recovery paths for the selected scenario were identified and quantified using the supervisory control system.

Key Words: Operational performance risk assessment, supervisory control system

1 INTRODUCTION

In nuclear power plants, the primary responsibility of the human operator is to ensure the safety of the plant. In the event of an abnormal transient incident, such as a component failure, the operator is responsible for observing important control parameters (flow rates, steam generator water level, etc.), following abnormal operating procedures and emergency operating procedures, and checking to assure that automatic safety system actuations have occurred when critical actuation criteria have been met. In general, the operator does not have the time or information available to examine alternative plant system configurations that would allow continued operation of the plant. With the advent of small modular reactors (SMRs) the role of the operator needs to be reconsidered, particularly in light of advances in autonomous control systems and in component fault diagnostics. From an economic standpoint, it will not be practical

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

to have the number of dedicated operators associated with each unit, which are now required for large nuclear plants. Control room operators will be responsible for the oversight of multiple units. The potential benefits of a supervisory control system (SCS) in reducing the demands on the control room operators and in increasing plant availability need to be explored.

The objective of the SCS [1] is to improve plant availability by automated SCS actions supported monitoring of equipment status, measuring control parameters, predicting outcomes and incorporating this information into a dynamic decision-making module. By reducing the need for operator interventions, the SCS will also reduce the potential for human errors. The dynamic decision module has three elements: 1) probabilistic model event trees (ETs)/fault trees (FTs) to define best risk-informed control options based on real time systems and components operational availability through a dynamic database, operational performance risk assessment (OPRA) [2]; 2) deterministic models to quantify defined control options via a plant simulator; 3) a utility function model to evaluate and rank defined control options (See green box in Fig. 1). This paper, will focus on the probabilistic model.

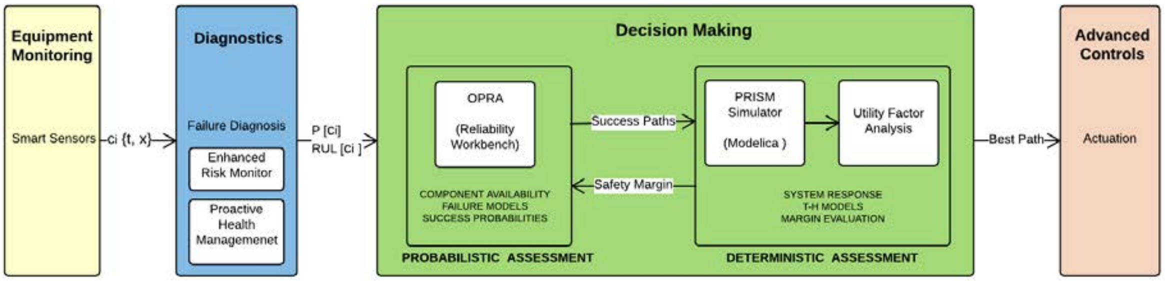

Fig. 1. Supervisory control system modular representation

The likelihood of failure of components/systems (e.g., valves, pumps, feedwater system, etc.) increases with time because of degradation. Equipment monitoring is used to assess the state of equipment, its probability of failure, and its residual lifetime. OPRA dynamically examines alternative heat rejection paths that would enable continued operation at the planned or reduced level of electric output. The likelihood of success of control actions that would result in each alternative configuration is calculated as input to the decision-making algorithm. The challenge is to dynamically control risk by deploying control actions on the spot in response to changing risk indicators.

This paper examines a scenario involving a feedwater control valve (FWCV) is drifting closed to show capabilities of the OPRA approach. Most feedwater control valves use an air operator to position the valve. This requires an air supply, a pressure regulator, a current-to-pressure converter, and the air operator. These air components caused several manual reactor trips because of feedwater oscillations or degradation issues as indicated in several licensee event reports [3, 4, 5]. Some of these issues are captured in the SCS, and alternative success paths are automatically generated to continue operation of the ALMR PRISM reactor at full or reduced power without causing a trip.

The rest of the paper is organized as follows. The ALMR PRISM reactor and power conversion system are briefly introduced in Section 1.1. Section 2 describes scenario and the probabilistic model of the scenario. Results of the analyses are given in Section 3 and conclusions are provided in Section 4.

1.1 ALMR PRISM PLANT

The reference design of ALMR PRISM has nine liquid metal pool type reactor modules. Each module produces 425 MW of thermal power tied to a single steam generator [6]. Steam from three steam generators (three reactor modules) is piped to a single turbine generator to form a power block of about 415 MWe. In a standard plant, there are a total of three power blocks, which have a combined electrical generation capacity of 1,245 MWe. In this paper, it is assumed that one of the steam generators in a power block is always available to limit the ET dimension therefore, two PRISM reactors make up a power block like GE Hitachi PRISM design.

The balance of plant (BOP) systems of the ALMR PRISM design are similar to the currently operating fleet of light water reactors, and modeled in Modelica as shown in Fig. 2 for a single power block.

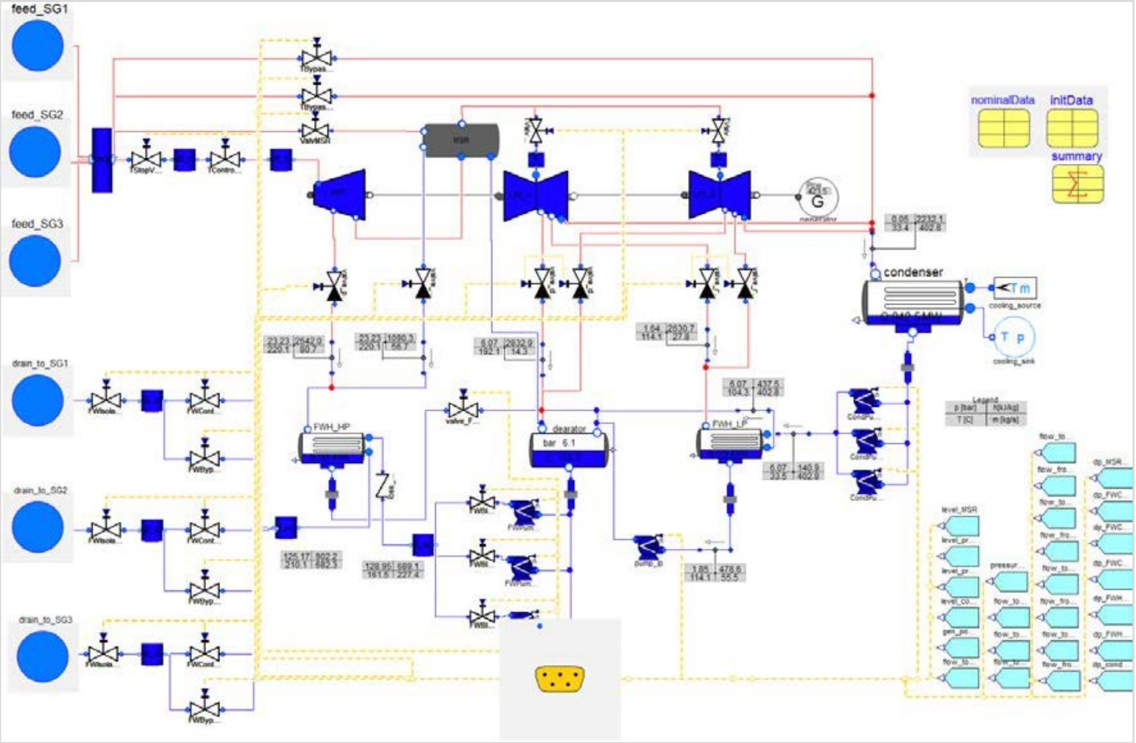

Fig. 2. ALMR PRISM power conversion system model layout.

The PRISM design has the inherent capabilities to override some initiating events without challenging the safety limits of the fuel, clad, or coolant, even under a hypothetical assumption that the reactor shutdown system fails to scram in response to the initiating event. For example, analysis demonstrates that an unprotected transient overpower initiated by accidental full withdrawal of a control rod without scram leads to a power increase that stabilizes at 103% of nominal power. If adequate coolant flow is maintained to provide heat removal, the reactor could continue operation until the power was reduced to the design level. The increase of only 3% in the power level is well within the margin of the heat removal system. The plant control system can accommodate such an increase by reducing the power level of other modules in the same power block [6]. This inherent capability increases the operational margin, and increases the SCS flexibility to adjust overall power in between the blocks without activating the reactor protection system (RPS).

2 OPERATIONAL PERFORMANCE RISK ASSESSMENT

2.1 Scenario and Challenges Addressed

For the selected scenario of steam generator (SG) 1 FWCV drifting in the closed direction, the following control options are defined by an expert operator to avoid challenges to a safety system include:

- Trip reactor 1 on low SG level
- Open SG1 bypass flow control valve (FCV), close main FWFCV
- Advise reactor operator (RO) to manually isolate SG1 main FWFCV; investigate valve logic error
- Decrease steam demand from SG1 by adjusting the SG1 turbine FCV in the closed direction and lowering generated power
- Advise RO to reduce reactor 1 power, investigate valve logic error and consider open SG1 bypass FCV
- Decrease steam demand from SG1 by adjusting the SG1 turbine FCV in the closed direction
- Increase steam demand from SG2 by adjusting the SG2 turbine FCV in the open direction
- Maintain generated power in the short term
- Advise RO to investigate valve logic error and adjust power on reactor 2

OPRA receives real-time information from an enhanced risk monitor [7] (Fig. 1), which uses condition monitoring equipment to determine the current condition of key plant components as time dependent probabilities of failure and projects the future degradation of these components and remaining useful life, based on simulated operational data from Modelica.

One of the challenges is to incorporate time dependent data in the FTs and update it every time step to update success probabilities. To cope with this problem, FTs modeled by Reliability Workbench are coupled with Modelica in the SCS, and are automatically updated according to component availabilities.

The other challenge is to broaden consideration of the operability of the components from failed/not-failed to also consider partial levels of system output, such as the flow through a valve. This extension does not fit the binary structure of the ET/FTs. Thus, as represented by different pathways in the ET/FT for a system, it may be possible to identify multiple plant configurations with the capability to satisfy an operational function, e.g., the rate of water flow to a steam generator.

2.2 Probabilistic Model of the Scenario

In the FCV drifts closed scenario, the flow paths between FCV to the steam generators header, SGs to HP turbine and SGs to condenser are considered in the probabilistic models. Top events in ET are developed by tracing the flow paths for each steam generator. The event tree for this scenario, which assumes that the third steam generator and associated reactor in the power block are unaffected by the transient, is shown in Fig. 3. Failures of components that lie in this flow path, feedwater bypass valves, isolation valves, TCVs and turbine bypass valves, are postulated as well as potential control options such as reducing power and increasing steam demand for both units. Failure rate data for quantifying the FTs were obtained from the available data source [8].

An event similar to the event analyzed in this paper occurred at the Virgil C. Summer Nuclear Station (VCSNS) on January 24, 2008 [4]. The feedwater flow control valve C exhibited oscillations as indicated by the plant computer and on the main control board. As the feedwater flow oscillations increased in size, the shift supervisor directed the operator to take manual control of the valve. Feedwater flow was greater than steam flow when manual control was implemented. When the operator decreased flow demand on the manual/auto station, IFV00498 indicated closed and feedwater flow decreased to zero. Due to a rapidly decreasing water level in Steam Generator C, the Shift Supervisor directed a manual reactor trip. In SCS, this event will be simulated and the time to trip will be compared with the time to place the reactor in a success end state defined by OPRA current focus of this paper is limited with the PRA.

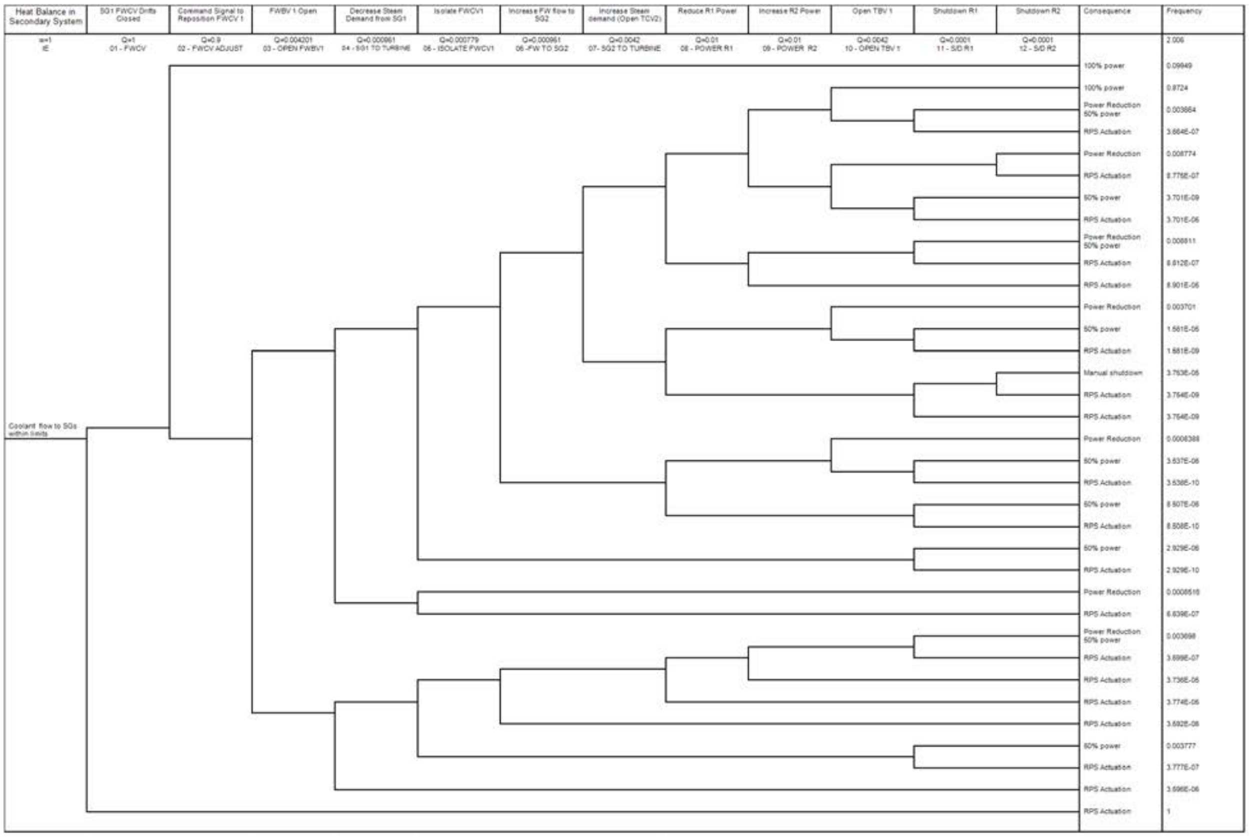

Fig. 3. Event tree for feedwater flow control valve drifts in close direction

Thirteen top events (Q0–Q12) are defined in the ET and represent the four main control options:

- Reactor 1 trip (RPS actuation) on low SG level (Failure branch of the Q1)
- Open SG1 bypass FCV (Q1, Q3, Q5)
  - shut main FWFCV
  - advise SCS to manually isolate SG1 main FW FCV
  - investigate valve logic error
- Decrease steam demand from SG1(Q1, Q3, Q4, Q5, Q8)
  - adjust the SG1 turbine FCV in the closed direction (lowering generated power)
  - advise SCS to reduce reactor 1 power, investigate valve logic error and consider second control option
- Increase steam demand from SG2 (Q1, Q3, Q4, Q5, Q6, Q7, Q9)
  - adjust the SG1 turbine FCV in the closed direction
  - increase steam demand from SG2 (SG2 turbine FCV in the open direction) maintain generated power in the short term
  - advise SCS to investigate valve logic error and adjust power on reactor 2

When TCV 1 drafted in the closed direction "Decrease Steam Demand from SG1", Q4, TBV 1 must be opened to reduce flow and dump steam to the condenser otherwise it will cause a scram because of high water level in SG1.

Q6, "Increase FW Flow to SG2," describes the open FWCV 2 and includes the possibility of the motor for FW Pump 2 operating slightly above the motor rating at 100% power (still operating well below its

115% service factor rating) or some of the FW Pump 1 flow directed to FWCV 2.

Q11 and Q12 represent cold shutdown of reactor 1 and shutdown of reactor 2 respectively. Cold shutdown is normally achieved by automatic or manual initiation of the plant control system (PCS) or RPS to insert all control rods. If an extremely unlikely series of failures (no credible single failure can cause a challenge) has prevented the normal shutdown, then operator action will be required to diagnose the problem and identify actions to bring the reactor to cold shutdown [6].

3 ANALYSIS

For the FWCV failure there are five possible end states:

1. **Normal operations:** Both reactors operate within the normal operational limits.
2. **Half power:** One of the reactors is manually shutdown without actuating the RPS.
3. **Power reduction:** FW or turbine bypass valves supply flow for 15%-20% percent flow capacity versus main flow control valves which can provide 20%-100% flow capacity. Therefore, flow reduction can represent approximately 70% power if power from one of the reactors is reduced and the other one is operated normally.
4. **Scram:** This consequence is included to show SCS does not compromise RPS and in the worst-case scenario RPS will activate the safety systems to mitigate the incident consequences. A reactor scram could happen as a result of a mismatch of the feedwater flow and steam demand or because of SG water level limits.
5. **Manual shutdown:** Both reactors are manually shutdown without scram.

Among these end states; normal operations, power reduction and ½ power are assumed as success end states.

Table I. Event Tree analysis summary

End State	Description	Frequency
Normal Operations	100% Power	9.949E-1
Reduced Power	70%-85% Power	3.063E-2
Half Power	50% Power	1.645E-2
Scram	RPS Actuation	1.000E0
Manual Shutdown	0% Power	3.753E-5

Success end states are selected and sequences deconstructed to determine control action combinations which are summarized in Table II.

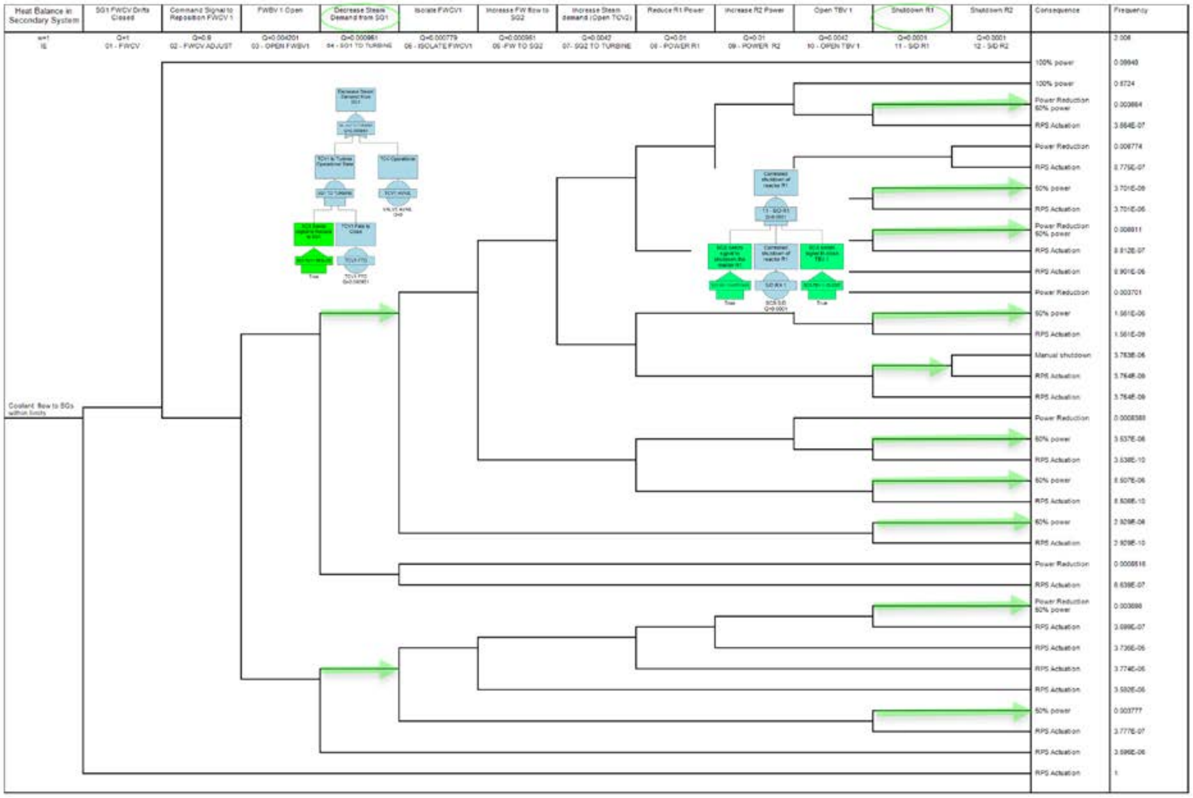

Fig. 4. Event Tree for feedwater flow control valve drifts in close direction

Seven alternative control actions additional to the default RPS system activation are listed in Table II. Modelica simulations run for each alternative to determine whether safety limits are reached or not. The utility factor analysis determines the best alternative based on how far the system is from a trip set point and how fast it is approaching that set point.

Table II. Control options identified from deconstruction process

Likelihood of success	ET Branch sequences	Control options	Consequence
1.0	1	Do nothing	Scram
0.8724	3–10	Normal operation, adjust power with R2	100% Power
0.008811	3–7, 9, 11	Open FWBV, increase R2 power, shutdown R1	Power reduction 65% power
0.008774	3–8, 10, 12	Open FWBV, reduce R1 power, shutdown R2	Power reduction 30% power
0.003777	4, 11	Close TCV1, shutdown R1	Power reduction 50% power
0.003701	3–6, 8, 10	Open FWBV, reduce R1 power, open TBV1	Power reduction 65% power
0.003698	4–9, 11	Close TCV1, open TCV2, increase R2 power, shutdown R1	Power reduction 80% power

The difference between 65% and 80% power reduction is determined by flow control via FW bypass valve or TCV, in the first case FWBV1 open so the max flow rate is limited by FWBV capacity but in the second case, FWCV2 is in its maximum open position and flow reduction will be based on TCV2 maximum opening position. TCV operational limits (30%) are wider than the bypass valves (15%-20%).

4 CONCLUSIONS

The SCS does not perform safety-related functions; however, the SCS can reduce the likelihood of RPS activations by identifying and implementing decision alternatives that enable continued operation of the plant.

In this paper, it has been shown that when an incident occurs such as valve failure, OPRA can provide several control options other than automatic RPS activation, which can be simulated by the SCS to estimate future conditions, the probabilities of success of alternative actions, and used by the SCS to identify a preferred course of action. This risk-informed approach will help operate multimodular systems and potentially reduce operator workload, reduce plant staffing levels, reduce maintenance costs, and avoid unplanned outages.

5 ACKNOWLEDGMENTS

This project was funded by the US Department of Energy's Office of Nuclear Energy under the Instrumentation, Control, and Human-Machine Interface technical area of the Advanced Reactor Technologies program.

6 REFERENCES

1. 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 (Sept. 2014).
2. S. M. Cetiner and 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).
3. Licensee Event Report (LER) 287/2015-001, "Revision 0, for Oconee Nuclear Station (ONS), Unit 3" (March 31, 2015).
4. Licensee Event Report (LER) No. 2008-001-00, "Virgil C. Summer Nuclear Station (VCSNS)," (March 20, 2008).
5. Licensee Event Report (LER) 446/15-002-00, "Reactor Trip Due to Feedwater Flow Controller Malfunction for Comanche Peak Nuclear Power Plant (CPNPP) Unit 2," (Dec. 1, 2015).
6. PRISM Preliminary Safety Information Document, GEFR-00793, UC-87Ta, prepared for US Department of Energy under Contract No. DE-AC03-85NE37937, Vol. 3, (1987).
7. P. Ramuhalli, A. Veeramany, E. H. Hirt, C. A. Bonebrake, G. Dib, and S. Roy, "Summary Describing Integration of ERM Methodology into Supervisory Control Framework with Software Package Documentation," PNNL-25839, (Sept. 2016).
8. D. Grabaskas and A. J. Brunett, "PRISM Balance-of-Plant Analysis Failure Modes and Reliability Data," interim report ORNL, Argonne National Laboratory, Argonne, IL (Aug. 2016).