A New Layer to the PRA: Operational Performance Risk Assessment

Askin Guler Yigitoglu[*a], Michael D. Muhlheim [a], Sacit M. Cetiner [a], Richard S. Denning[b]

[a]Oak Ridge National Laboratory, Oak Ridge, TN, USA
[b]Research Consultant, Columbus, OH, USA

Abstract: A supervisory control system (SCS) concept developed by Oak Ridge National Laboratory provides automated risk-informed decision-making capabilities with the ultimate goal of significantly boosting plant availability while reducing dependency on human resources for multi-module advanced reactors. The decision-making process integrates online-monitoring systems, and the associated diagnostic and prognostics tools to continuously take into account the component health in an integrated probabilistic/deterministic meta model to capture the system behavior during a select set of postulated anticipated operational occurrence scenarios. The operational performance risk assessment (OPRA) approach is introduced to support SCS decisions probabilistically to minimize/prevent unnecessary trips and challenges to plant safety systems. OPRA identifies and ranks the success paths, combination of the non-safety systems and components, with the real-time failure data using event tree/fault tree method. OPRA does not interfere with the safety systems and adds a buffer zone to the existing probabilistic risk assessment (PRA) domain by minimizing the possible transients. In this work, failure scenarios of feedwater and turbine control valves are analyzed for ALMR PRISM (Power Reactor Innovative Small Module) design at full power. As an alternative to the default shutdown option, five and seven success paths (full and reduced power operation) are defined respectively within the OPRA framework.

Keywords: Supervisory Control System, Decision-making, Operational PRA

1. INTRODUCTION

Operator is responsible to ensure the safety of a nuclear reactor as a last line of the defense. Important control parameters (e.g., steam generator water level) are observed by operators, 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. With the advent of small modular reactors, the role of the operator needs to be reconsidered, particularly in light of advances in autonomous control systems and in component fault diagnostics. The supervisory control system (SCS) [1] has been introduced for multi-unit advanced small modular reactors and aims: to provide real-time decision-making capabilities based on the status of the plant/systems and component health, to minimize human interventions during normal and abnormal operations, and also to increase plant availability. The SCS is part of the non-safety-related instrumentation and control system architecture, that is, separate and isolated from the protection system, and as such, it does not interfere with protection system functions, such as the reactor trips.

* *yigitoglua@ornl.gov*

The operational performance risk assessment (OPRA) approach was developed as the probabilistic part of the decision-making process to minimize challenges to plant safety systems and prevent—or at least minimize—avoidable trips [2]. The current implementation of the probabilistic part of the OPRA approach relies on fault and event trees that are continuously updated with real-time failure data streamed from the online equipment condition monitoring system and the associated prognostics system. Given a failure or performance degradation of a monitored component (or subsystem), the OPRA approach automatically identifies success paths that lead to acceptable plant states without requiring a safety system initiation relying solely on non-safety systems and components.

The operational decision alternatives, i.e., plant state navigation trajectories, generated by the probabilistic analyses are tested in an integrated system model of the plant to calculate a new metric, called proximity to trip setpoints, to rank and eventually prioritize alternative state navigation trajectories. Rankings from probabilistic and deterministic calculations are then combined using a variant of the utility theory.

In this work, failure scenarios of the turbine control and feedwater control valves are analyzed for the Advanced Liquid Metal Reactor (ALMR) Power Reactor Innovative Small Module (PRISM) plant at full power. As an alternative to the default shutdown option, four success paths (full and reduced power operation) are defined within the OPRA framework.

2. WHAT CAN GO WRONG?

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 [3]. Steam from three steam generators (three reactor modules) is piped to a single turbine generator to form a power block of about 415 MW_e. In a standard plant, there are a total of three power blocks, which have a combined electrical generation capacity of 1,245 MW_e. 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 (See Figure 1).

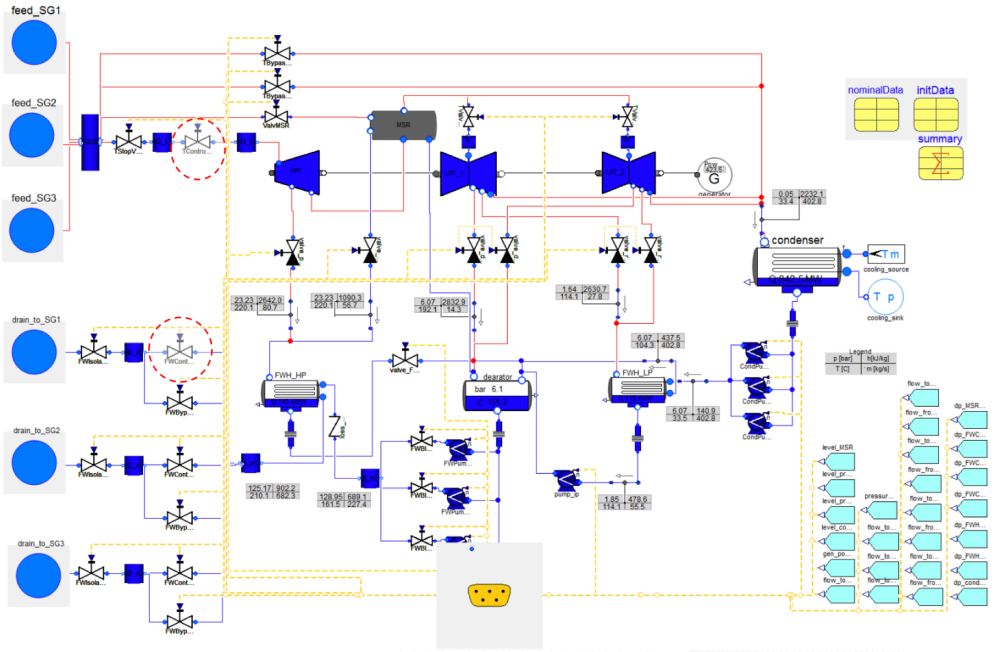

Figure 1: ALMR PRISM Power Conversion System Model Layout

Two possible failure events are considered and the control options for these two scenarios reflecting the failures/degradations/out-of-service conditions are provided below.

Scenario 1: *TCV drifts in closed direction*
Control options:

1. Reactor trip on steam generator (SG) low-water level (i.e., do nothing)
2. Successfully reposition TCV
3. Open the turbine bypass valve to compensate in the short term—Advise reactor operator (RO) to reduce reactor power/correct TCV logic error
4. If reactor 2 (1) is not at 100%, open reactor 2 SGBV—Advise RO to reduce reactor 1 (2) power/correct TCV logic error
5. Decrease FW flow to SG 1 (2)—Advise RO to reduce reactor 1 (2) power/correct TCV logic error

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

Based on the two scenarios, two ETs and corresponding FTs were developed to reflect the proper heat balance in the secondary cooling system: (1) steam flow to turbine within limits; and (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.

OPRA receives real-time information from an enhanced risk monitor [4] (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.

3. HOW LIKELY IT IS?

A similar event described in Scenario 2, occurred at the Virgil C. Summer Nuclear Station (VCSNS) on January 24, 2008 [5]. 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. Failure rate data for quantifying the FTs were obtained from the available data source [6].

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].

4. WHAT ARE THE CONSEQUENCES?

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 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.

To test and verify the accuracy of the probabilistic models for the SCS, the status of the turbine control valves (TCVs) and feedwater (FW) flow control valves (FCVs) were captured in the ET/FT models.

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. The control options for Scenario 1 and Scenario 2 reflecting the failures/degradations/out-of-service conditions are provided in the previous section.

4.1. Probabilistic Model of the Scenario 1

The ET for the operational decisions associated with Scenario 1, which is based on the steam flow to the turbine being within proper limits, is provided in Figure 2. The ET captures plant operations with 0, 1, or 2 SGs in service and this demonstration problem is showing two SGs in operation. Now that the SCS knows where in the ET the failure occurred, it must reconstruct the ET so that any decision options can be identified. The ability to make a decision requires knowledge of the likelihood of success for the different control options given the failure that just occurred. Determining the likelihood of success, which requires knowledge of the event sequences, requires that the SCS reconstruct the ET/FT models. The sequences with the greatest likelihood of success can then be selected.

In reconstructing the probabilistic model from the data, the SCS must recognize that the fault TCV DRIFT is input into Gate “01-TCV” in the FT. That is, the SCS maps the basic event to the gate.

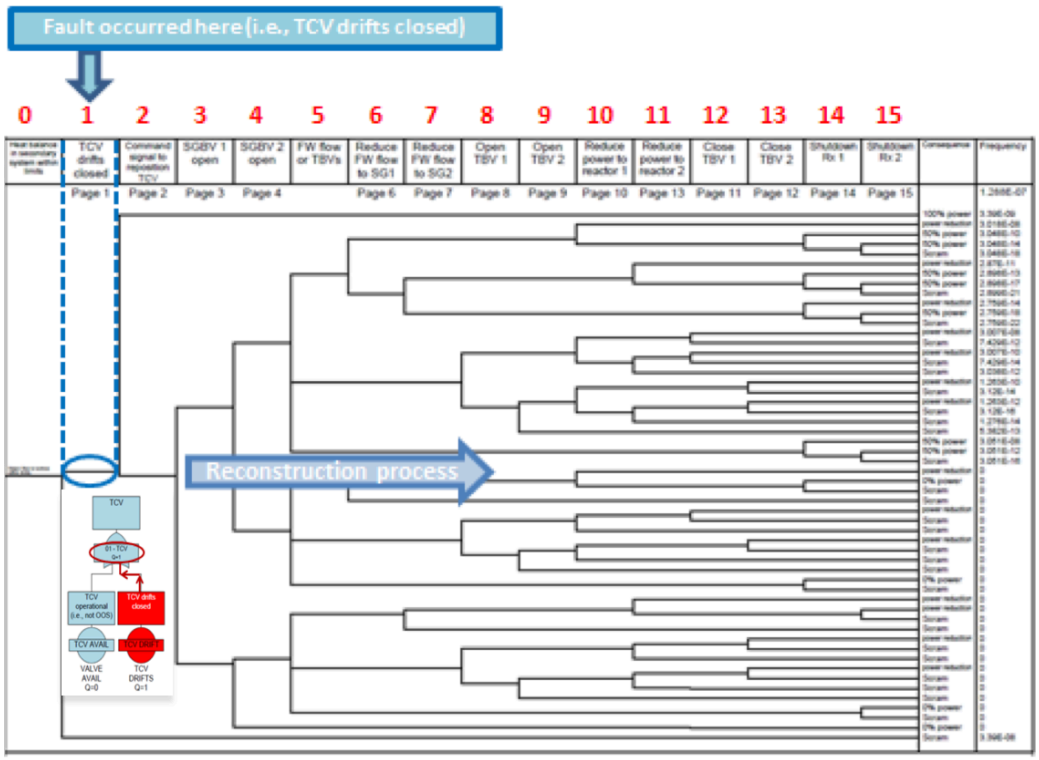

Figure 2: ET for steam flow to turbine with one steam generator in operation

Now that the SCS has *reconstructed* the ET with the fault properly accounted for in the FT and ET, it must now *deconstruct* the ET to identify the control options for successfully maintaining system operation. The reconstructed ET shows there are four viable control options based on probability for avoiding a trip setpoint. The deconstruction process is used to first determine those actions that if taken, would avoid a trip set point. Note that this is different than operations to continue producing power. To identify the control options for each sequence of events, the deconstruction process must alternate between the ET and FTs, and check the status of the components to ensure they are available if needed or to acknowledge that they are unavailable. In this example, the deconstruction starts with ET Branch 15 and deconstructs the ET, branch by branch, until it has collected, reviewed, and identified options back to the ET branch where the fault occurred—in this example ET Branch 1.

In deconstructing the ET (Figure 3), the SCS must automatically and autonomously determine that there are five success paths, and each success path has potential control commands at the success/failure branch points on the ET. Thus, the success paths with decision points are provided in Table 1.

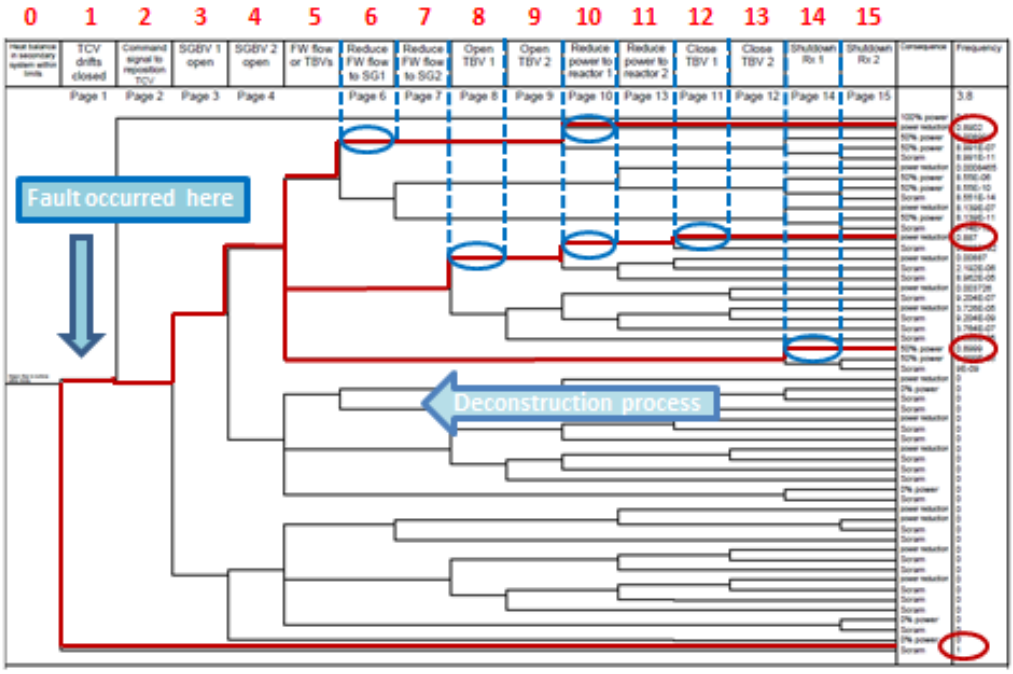

Figure 3: Deconstruction of ET to identify decision options

The SCS automatically and autonomously determined that there are five success paths, and each success path has potential control commands at the success/failure branch points on the ET.

Table 1: Control options identified from deconstruction process

Likelihood of success	ET Branch sequences(s)	Control option	Consequence
1.0	1	Do nothing	Scram reactors
0.8999	14	Controlled shutdown of Rx1	50% power
0.8902	6—10	Reduce FW flow—reduce power	Power reduction
0.887	8—10—12	Open TBV—reduce power—close TBV	Power reduction
0.1	2	Successfully reposition TCV	100% power

4.2. Probabilistic Model of the Scenario 2

In the FCV drifts closed scenario [7], 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. 4. 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.

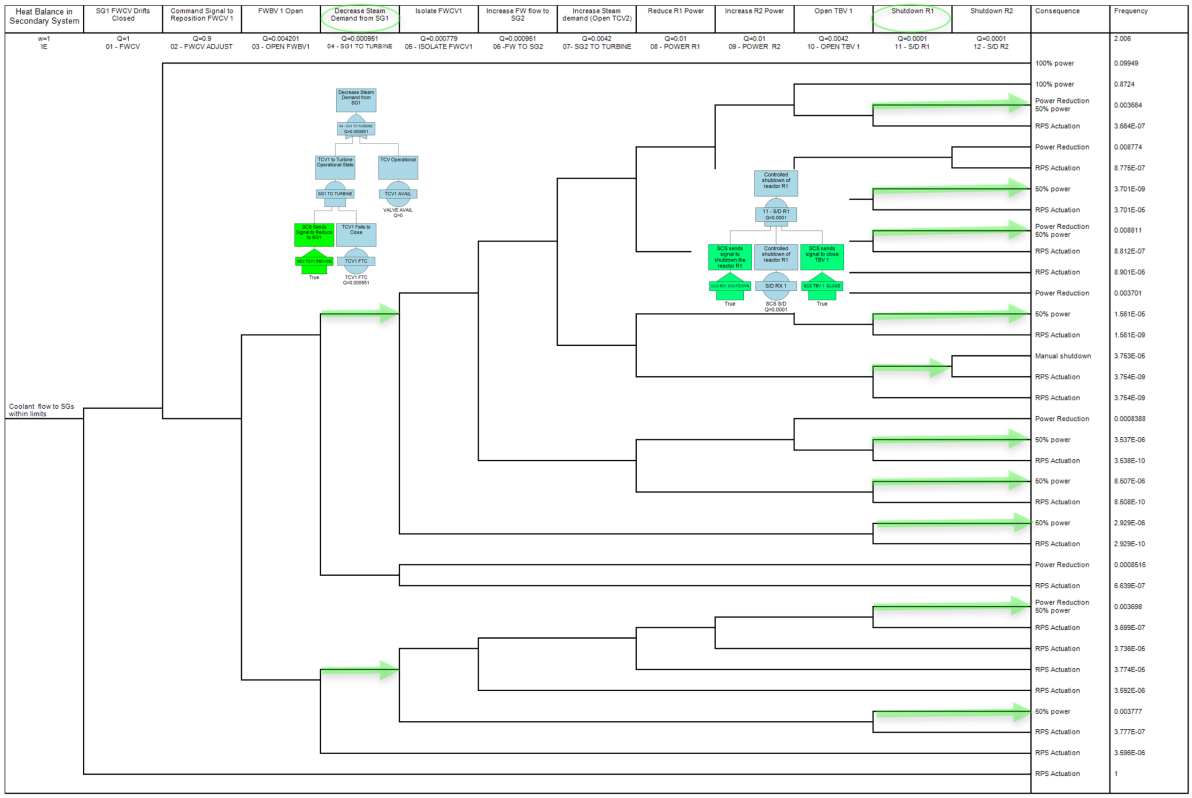

Figure 4: Event Tree for feedwater flow control valve drifts in close direction

Seven alternative control actions additional to the default RPS system activation are listed in Table 2. Modelica simulations run for each alternative to determine whether safety limits are reached or not.

Table 2: 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 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.

4. CONCLUSION

Based on the case studies, it can be concluded that 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. It has been also 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 decision approach will help operate multi-modular systems and potentially reduce operator workload, reduce plant staffing levels, reduce maintenance costs, and avoid unplanned outages.

Acknowledgements

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.

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] PRISM Preliminary Safety Information Document, GEFR-00793, UC-87Ta, prepared for US Department of Energy under Contract No. DE-AC03-85NE37937, Vol. 3, (1987).

[4] 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).

[5] Licensee Event Report (LER) No. 2008-001-00, "Virgil C. Summer Nuclear Station (VCSNS)," (March 20, 2008).

[6] 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).

[7] A. Guler, M. Muhlheim, S. Cetiner, R. Denning, "*Operational Performance Risk Assessment in Support of a Supervisory Control System*", in Proceeding of 10th International Conference on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2017), San Francisco, CA, (2017).