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 at 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 multimodule advanced reactors. The decision-making process integrates online monitoring systems and the associated diagnostic and prognostics tools to continuously account for component health in an integrated probabilistic/deterministic metamodel 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 probabilistically support SCS decisions so that unnecessary trips and challenges to plant safety systems are minimized or prevented. OPRA identifies and ranks the success paths, combinations of non-safety systems and components, with real-time failure data using an event tree/fault tree method. OPRA does not interfere with the safety systems and adds a buffer zone to the existing probabilistic risk assessment domain by minimizing possible transients. In this work, failure scenarios related to feedwater and turbine control valves are analyzed for the Advanced Liquid Metal Reactor Power Reactor Innovative Small Module design at full power. As an alternative to the default shutdown option, four and six success paths (full-power-operation and reduced-power-operation) are defined respectively for the two cases demonstrated within the OPRA framework.

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

1. INTRODUCTION

Operators are responsible for ensuring the safety of a nuclear reactor as a last line of defense. Operators observe important control parameters (e.g., steam generator water level) following the utilization of abnormal operating procedures and emergency operating procedures, and they check whether automatic safety system actuations have occurred when critical actuation criteria are 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 component fault diagnostics. A supervisory control system (SCS) [1] has been introduced for multi-unit advanced small modular reactors that aims to provide real-time decision-making capabilities based on the status of the plant, its systems, and component health to minimize the need for human interventions during normal and abnormal operations and to increase plant availability.

The operational performance risk assessment (OPRA) approach was developed to probabilistically support the decision-making process to minimize challenges to plant safety systems and to minimize, if

* *yigitoglua@ornl.gov*

not prevent, avoidable trips [2]. The term probabilistic risk assessment (PRA) is often used to represent the probabilistic portion of the methodology which focuses on the operational performance. The standard PRA techniques of event trees (ETs) and fault trees (FTs) to model system behavior are used, but the SCS is focused on the success paths of the ETs. Contributors to the paths, or sequences of avoiding trip setpoints, include elements such as the successful implementation of changing the state of a component (e.g., pump started, valve opened) so that SCS operation continues.

The current implementation of the probabilistic part of the OPRA approach relies on the use of fault tree and event tree analyses that are continuously updated with real-time failure data streamed from the online equipment condition monitoring system and the associated prognostics system. In the event of failure or performance degradation of a monitored component (or subsystem), the OPRA approach automatically identifies success paths, relying solely on non-safety systems and components, that lead to acceptable plant states without requiring a safety system initiation. 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. This new metric ranks and eventually prioritizes alternative state navigation trajectories. Rankings from probabilistic and deterministic calculations are then combined using a variant of utility theory.

In this work, failure scenarios related to the turbine control and feedwater control valves are analyzed for the Advanced Liquid Metal Reactor Power Reactor Innovative Small Module (ALMR PRISM) plant at full power. As an alternative to the default shutdown option, full and reduced-power operation success paths 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 (i.e., three reactor modules) is piped to a single turbine generator to form a power block of about 415 MW_e. In the reference plant [3], 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, similar to the GE Hitachi PRISM design. The balance of plant systems included in the ALMR PRISM design are similar to those needed for the currently operating fleet of light water reactors and as modeled in Modelica (Figure 1).

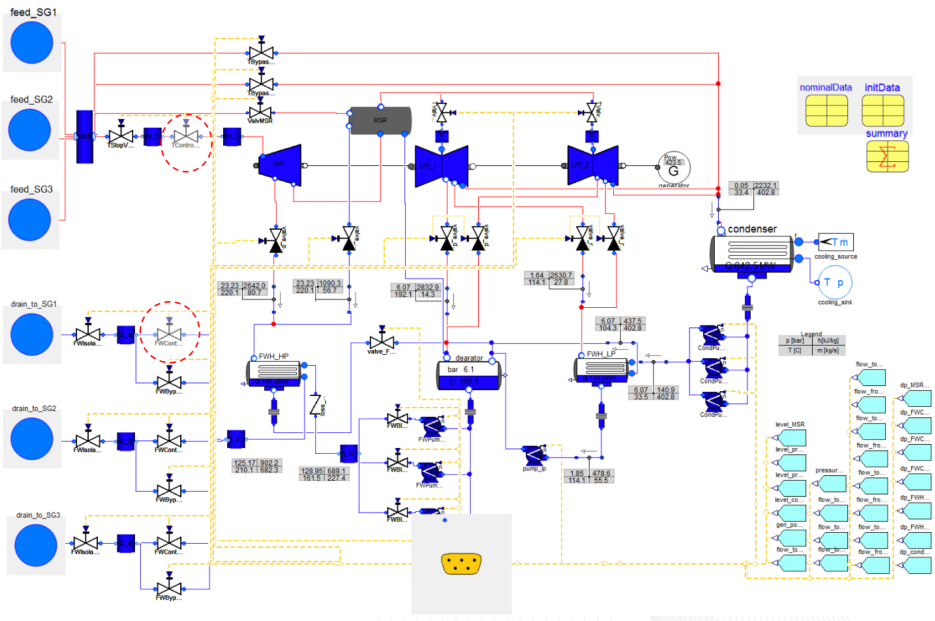

Figure 1: ALMR PRISM Power Conversion System Model Layout

Two possible failure events are considered in this work, and the control options for these two scenarios that reflect the failures/degradations/out-of-service conditions are defined by a senior reactor operator and provided below.

Scenario 1: *Turbine control valve (TCV) drifts in closed direction*

Control options:

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

Scenario 2: *SG 1 feedwater flow control valve (FW FCV) drifts in closed direction*

Control options:

1. Reactor 1 trip on low SG level (i.e., do nothing).
2. Open the SG 1 bypass flow FCV. Shut the main FW FCV.
3. Advise the RO to manually isolate the SG 1 main FW FCV and investigate the 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 the RO to reduce Reactor 1 power, investigate valve logic error, and 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, if the Reactor 2 is not at the full power.
8. Maintain generated power in the short term.
9. Advise the RO to investigate valve logic error and adjust power on Reactor 2.

Based on these 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 or decrease cooling flow to the SGs, resulting in overcooling or 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, ultimately causing a reactor trip.

OPRA receives real-time information from an enhanced risk monitor (ERM) [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 their remaining useful life based on simulated operational data from Modelica.

3. HOW LIKELY IT IS?

An event similar to scenario 2 occurred at the Virgil C. Summer Nuclear Station in South Carolina on January 24, 2008 [5]. The feedwater flow control valve C exhibited feedwater flow oscillations, as indicated by the plant computer and main control board. As the oscillations increased in size, the shift supervisor directed the RO to take manual control of the valve. Feedwater flow was greater than steam flow when manual control was implemented. When the RO decreased flow demand on the manual/auto station, the valve indicated closed, and feedwater flow decreased to zero. Due to a rapidly decreasing

water level in SG C, the shift supervisor directed a manual reactor trip. In SCS, this event is simulated, and the time to trip is compared with the time to place the reactor in a success end state as defined by OPRA. Failure rate data for quantifying the FTs were obtained from the available data source [6] and the selected component failure rates are taken from the ERM in real time. One of the challenges is to incorporate time dependent data in the FTs and update them at every time step to recalculate success probabilities. To meet this challenge, FTs modeled by Reliability Workbench are coupled with Modelica in the SCS, and FTs are automatically updated according to component availabilities.

Another challenge involves broadening consideration of component operability from failed/not failed to include partial levels of system output, such as the flow through a valve. This extension does not fit the binary structure of the ET and FTs. Thus, as represented by different pathways in ET/FT analyses 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 an SG).

In the scenario where the FCV drifts closed, the flow paths between the FCV and the SG headers, between the SGs and the high-pressure turbine, and between the SGs and the condenser are considered in the probabilistic models. Top events in the ET are developed by tracing the flow paths for each SG. The event tree for this scenario, which assumes that the third SG and the associated reactor in the power block are unaffected by the transient, is shown in Figure 3. Failures of components that lie in this flow path, feedwater bypass valves (FWBV), isolation valves, TCV and turbine bypass valves are postulated, along with 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 [6].

4. WHAT ARE THE CONSEQUENCES?

To test and verify the accuracy of the probabilistic models for the SCS, the status of the TCVs and FW FCVs was captured in the ET/FT models. There are five possible end states:

1. **Normal operations:** Both reactors operate within normal operational limits.
2. **Half power:** One of the reactors is manually shut down without actuating the reactor protection system.
3. **Power reduction:** FW or TBV supply flow for 15%–20% percent flow capacity versus main FCVs, 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 is operated normally.
4. **Scram:** This consequence is included to show that SCS does not compromise RPS and, in the worst-case scenario, RPS will activate safety systems to mitigate the incident. A reactor scram could result from a mismatch of the FW flow and steam demand or SG water-level limits.
5. **Manual shutdown:** Both reactors are manually shut down without scram.

Among these end states, normal operations, power reduction, and half power are considered success end states. Control options for scenarios 1 and 2, reflecting the failures, degradations, and out-of-service conditions, are provided in Section 3.

It should be noted that the SCS is part of the non-safety-related instrumentation and control system architecture; that is, it is separate and isolated from the protection system. The SCS does not interfere with protection system functions such as the reactor trips; therefore, the default consequence is always the reactor scram.

4.1. Probabilistic Model of Scenario 1

The ET shown in Figure 2 captures plant operations with 0, 1, or 2 SGs in service; but the current work demonstrates two SGs in operation. Now that the SCS has determined where in the ET the failure occurred, it must reconstruct the ET, so decision options can be identified. The ability to make a decision

requires knowledge of the likelihood of success for different control options given the nature of the failure. Determining the likelihood of success, which requires knowledge of event sequences, necessitates 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.

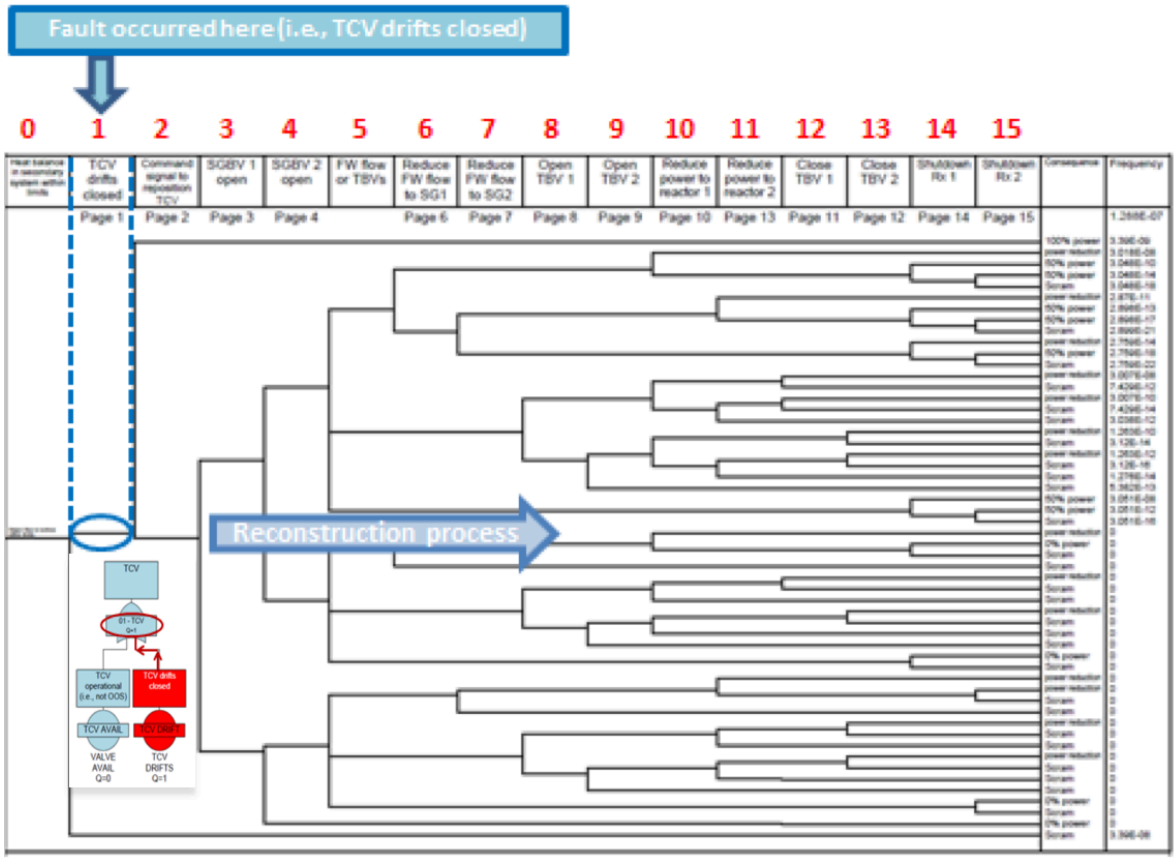

Figure 2: ET for Steam Flow to Turbine with One Operating SG

Once 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 setpoint. Note that this is different from operations that continue producing power. To identify the control options for each sequence of events, the deconstruction process must alternate between the ETs and FTs and must check component status 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 delivered options back to the ET branch where the fault occurred—in this example, ET Branch 1.

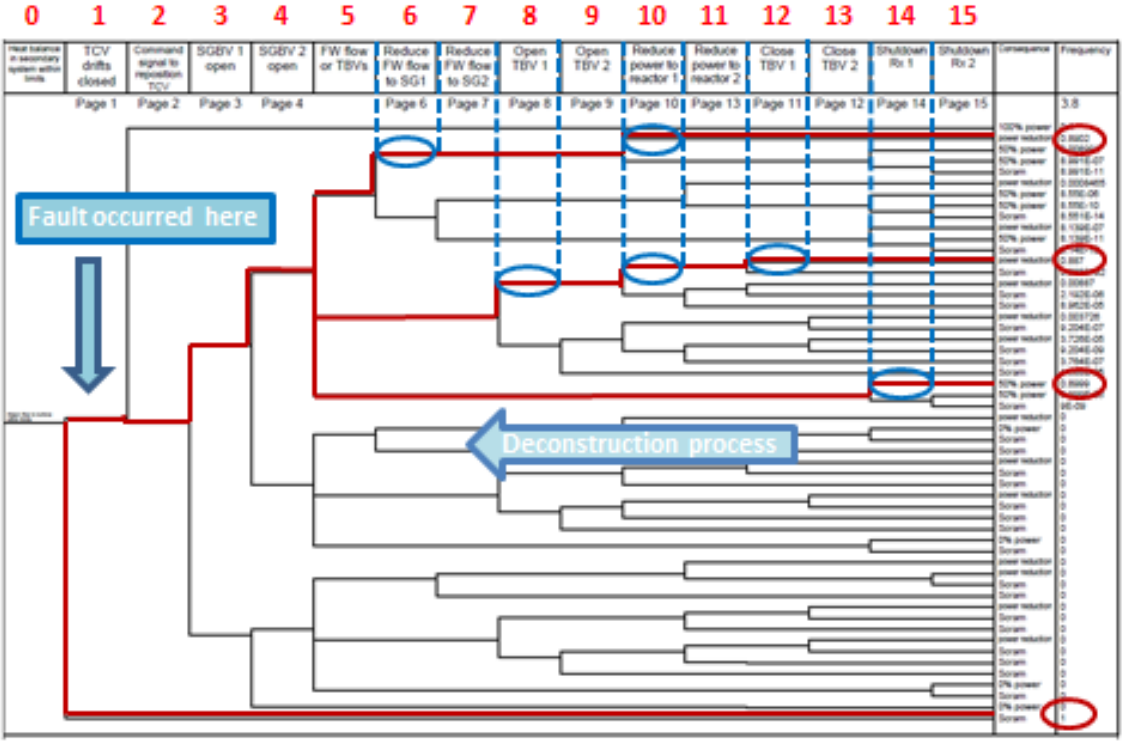

Figure 3: Deconstruction of ET to Identify Decision Options

In deconstructing the ET (Figure 3), the SCS must automatically and autonomously determine that there are five success paths and that 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.

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	Conduct 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 Scenario 2

In scenario where FCV drifts closed [7], the flow paths between the FCV and the SG headers, between the SGs and the HP turbine, and between the SGs and the condenser are considered in the probabilistic models. Top events in the ET are developed by tracing the flow paths for each SG. The ET for this scenario (Figure 4) assumes that the third SG and the associated reactor in the power block are unaffected by the transient. Failures of components that lie in this flow path, FW bypass valves, isolation valves, TCVs, and TBVs, are postulated, and potential control options such as reducing power and increasing steam demand for both units are addressed. Figure 4 illustrates the deconstruction process and availability of the components checked with the ERM and as indicated with green colored basic events in FTs which are available.

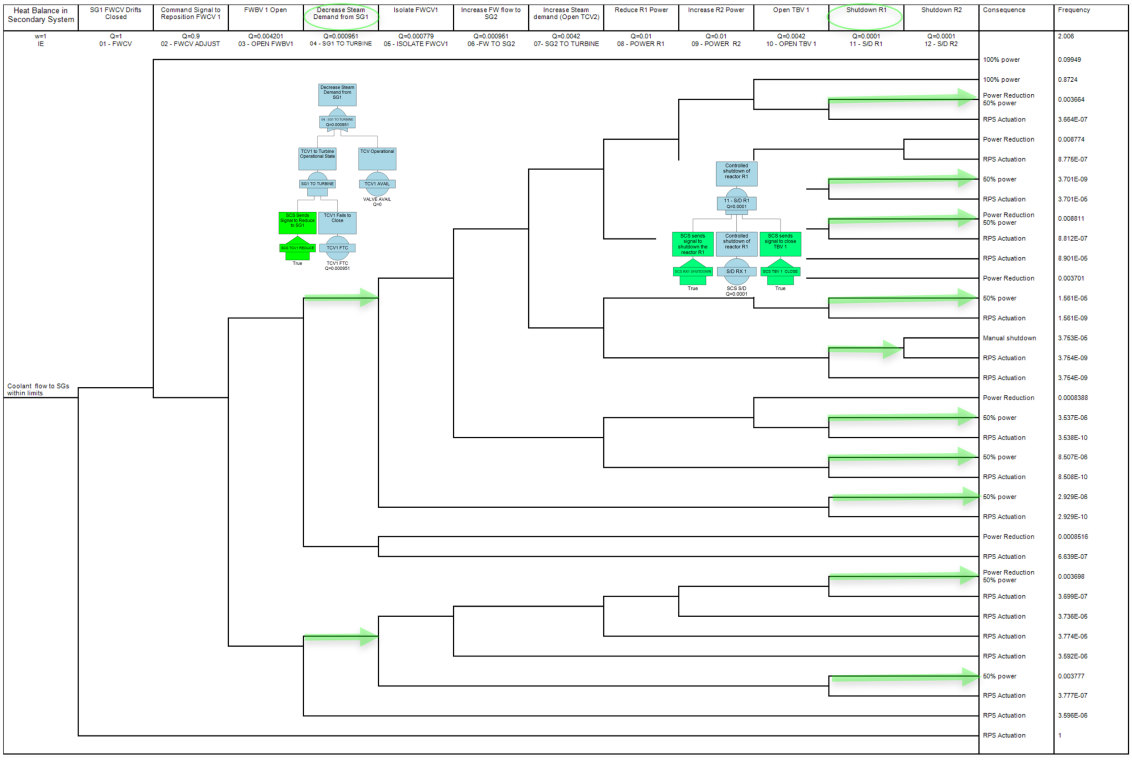

Figure 4: Event Tree for FW FCV drifts in Closed Direction

Table 2 shows six alternative control actions that can be considered in addition to the default RPS system activation and Modelica simulations performed for each alternative control action to determine whether safety limits are reached.

Table 2: Control Options Identified from the Deconstruction Process

Likelihood of success	ET branch sequences	Control options	Consequence
1.0	1	Do nothing	Scram
0.8724	3-10	Conduct normal operations, 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

Utility factor analysis determines the best alternative based on how far in time the system is from a trip setpoint and how fast it is approaching that setpoint.

4. CONCLUSION

Based on the scenarios presented in this paper, it can be concluded that although the SCS does not perform safety-related functions it can reduce the likelihood of RPS activations by identifying and implementing decision alternatives that enable continued plant operations. This work also shows that when an incident occurs (e.g., valve failure), OPRA can provide several control options in addition to automatic RPS activation. These options are simulated by the SCS to estimate future conditions and the success probabilities of alternative actions that are ultimately evaluated by the SCS to identify a preferred course of action.

This risk-informed decision approach will aid the operation of multi-modular systems, potentially reducing operator workload, plant staffing levels, and maintenance costs and help to prevent unplanned outages.

Acknowledgments

This project is funded by the US Department of Energy, Office of Nuclear Energy, under the Instrumentation, Control, and Human-Machine Interface technical area of the Advanced Reactor Technologies 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 (September 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*," Vol. 3, GEFR-00793, UC-87Ta, prepared for US Department of Energy under Contract no. DE-AC03-85NE37937 (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 (September 2016).

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

[6] D. Grabaskas and A. J. Brunett. "*PRISM Balance-of-Plant Analysis Failure Modes and Reliability Data,*" Interim Report, Oak Ridge National Laboratory/Argonne National Laboratory, Argonne, IL (August 2016).

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