Oak Ridge National Laboratory

A New Layer to the PRA: Operational Performance Risk Assessment

Askin Guler Yigitoglu
Advanced Reactor Engineering
Reactor and Nuclear Systems Division
Co-authors: M. D. Muhlheim, S. Cetiner, and R. Denning

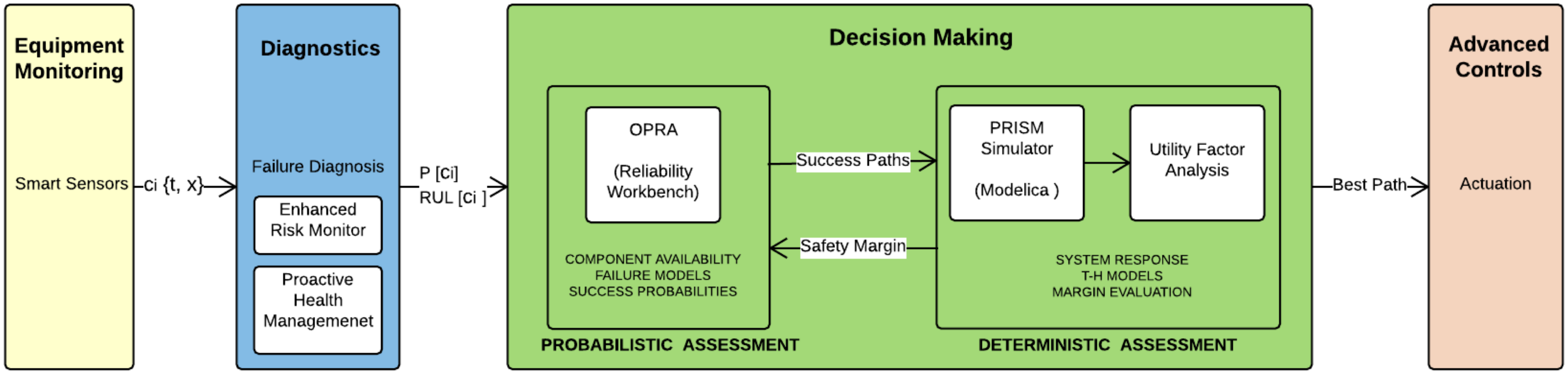
PSAM 14, Los Angeles, California
September 20, 2018

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

Introduction to the Supervisory Control System

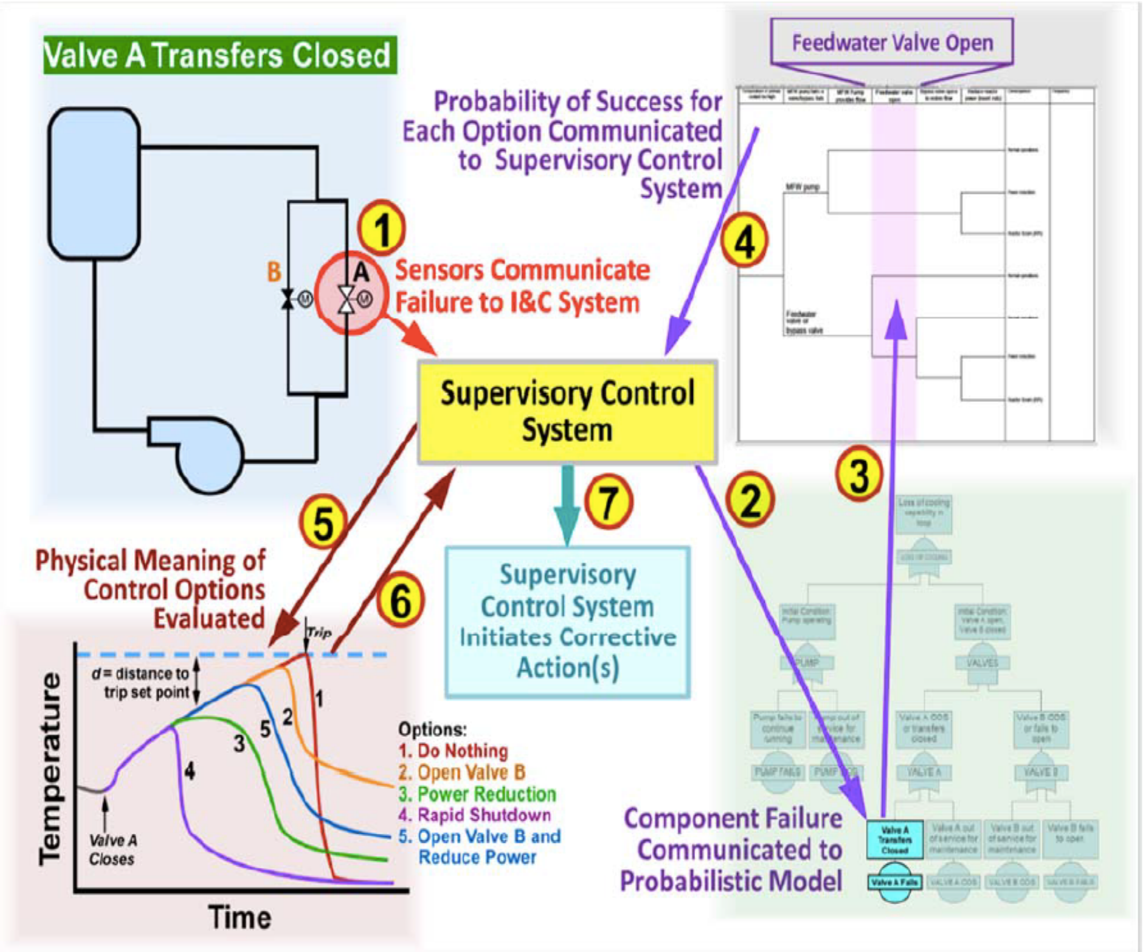
- Proposed for multi-unit advanced small modular reactors:
  - to provide real-time decision-making capabilities based on the status of the plant/systems and component health
  - to minimize human interventions during normal and abnormal operations
  - to increase plant availability



Risk-Informed Decision Making

Control action decisions are made based on a probabilistic risk assessment via event trees (ETs) and fault trees (FTs) but

- scope applies to <u>normal operations</u>
- application is reversed to assess the <u>success of non-safety related system</u>
- top events in ETs represents system components and control actions instead of safety systems
- SCS command signals added to the FTs

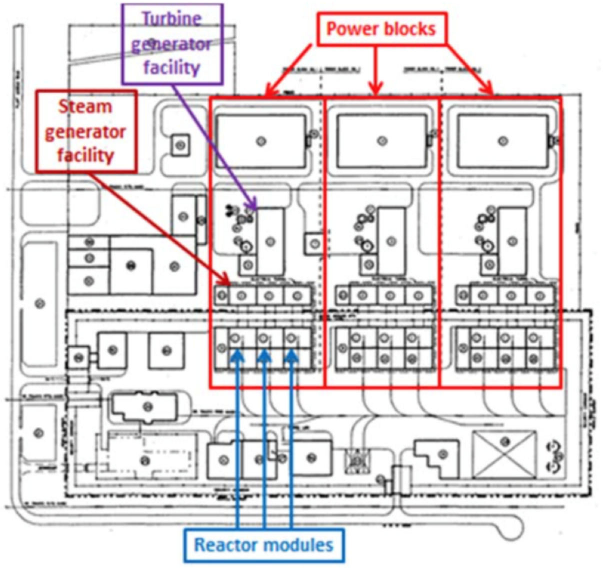


Operational Performance Risk Assessment

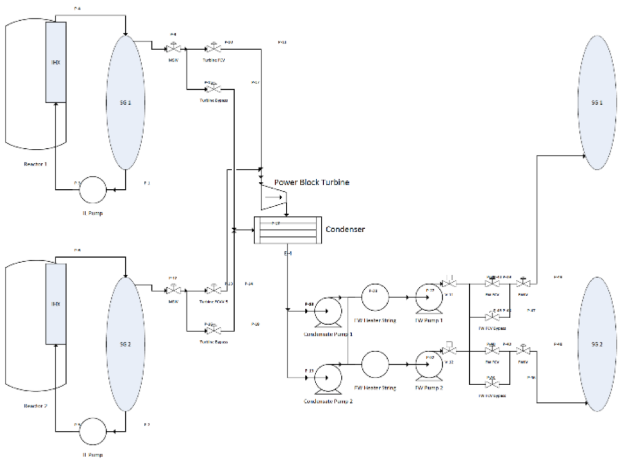
Demonstration: The balance of plant (BOP) of the Advanced Liquid Metal Reactor (ALMR) Power Reactor Inherently Safe Module (PRISM) design is selected for proof of concept

Assumptions:

- Most components of the BOP system are in operation in full power
- Typical manual actions in current fleet will be handled via SCS in PRISM reactor
- One of the SGs in a power block is always available
- In the worst-case scenario RPS will activate the safety systems to mitigate incident consequences

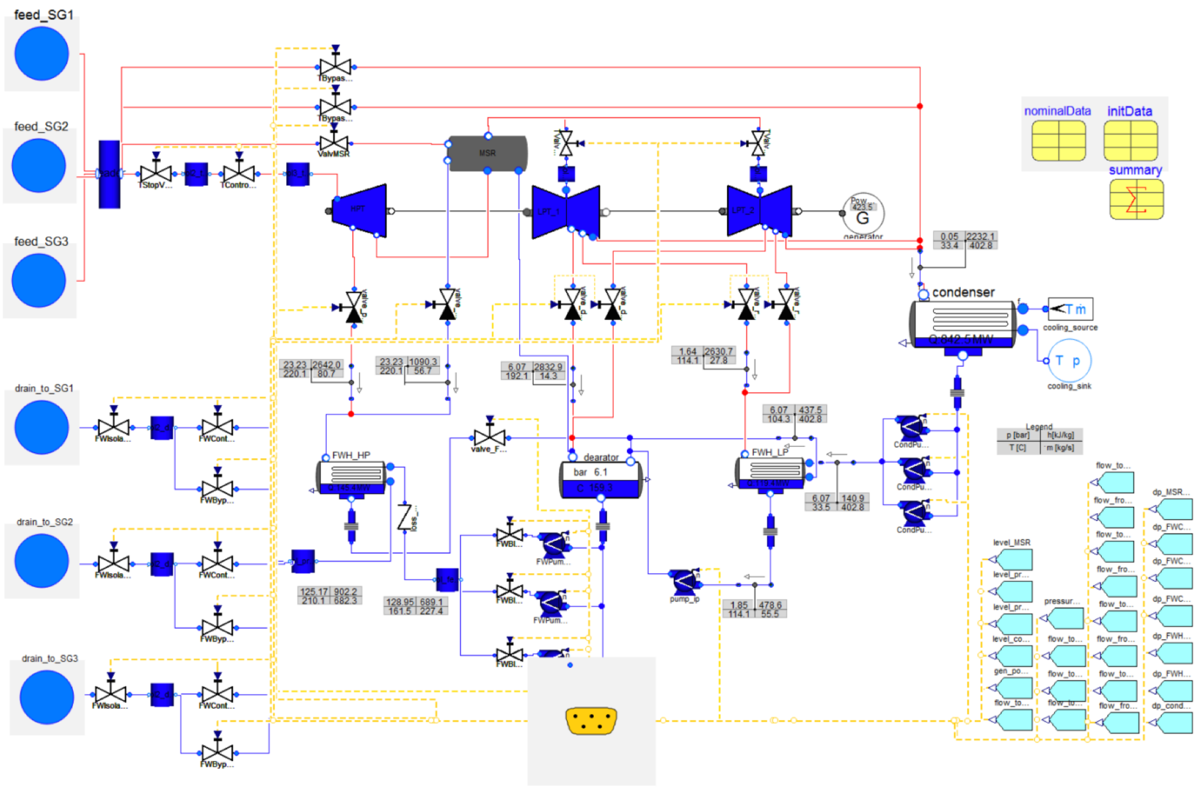


ALMR PRISM PSID Appendix G



ALMR PRISM Simplified Power Block Diagram

What can go wrong?



ALMR PRISM Power Conversion System Model for a Single Power Block

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

1. Reactor trips 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 trips 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.

How likely it is?

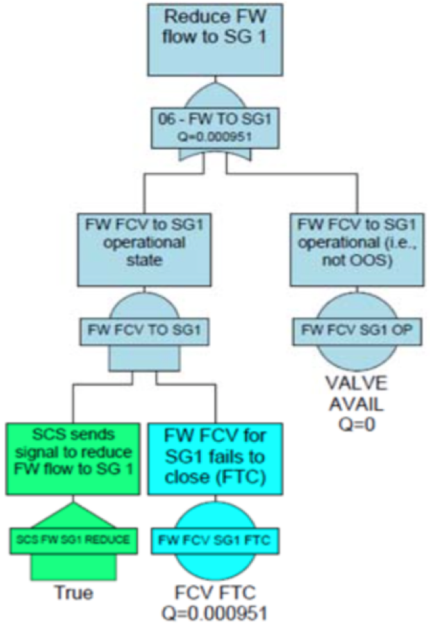
- ETs and FTs were developed to reflect the proper heat balance in the secondary cooling system
- FCVs (mostly air operated valves) caused several manual reactor trips due to
  - **Feedwater flow oscillations**
    - ➢ Duke Energy event occurred at Oconee Nuclear Station (ONS), Unit 3, in which the unit was manually tripped on January 31, 2015
    - ➢ Virgil C. Summer Nuclear Station (VCSNS) on January 24, 2008
  - **Degradation issues**
    - ➢ Comanche Peak Nuclear Power Plant (CNPP) Unit 2 on December 1, 2015

Air-operated valve reliability data (U.S. Nuclear Regulatory Commission, 2007)

Failure mode	Events	Demands or hours	Mean failure probability or rate[2]
FTO	73	173,117	-
FTC	63	173,117	-
FTO/C	146	173,117	9.51E-04
FC[1]	266	1,171,601,352 h	2.49E-07
SOP[1]	140	1,171,601,352 h	1.31E-07
ILS[1]	113	1,171,601,352 h	9.69E-08
ELS[1]	64	1,171,601,352 h	5.51E-08

[1]Reactor-year hours

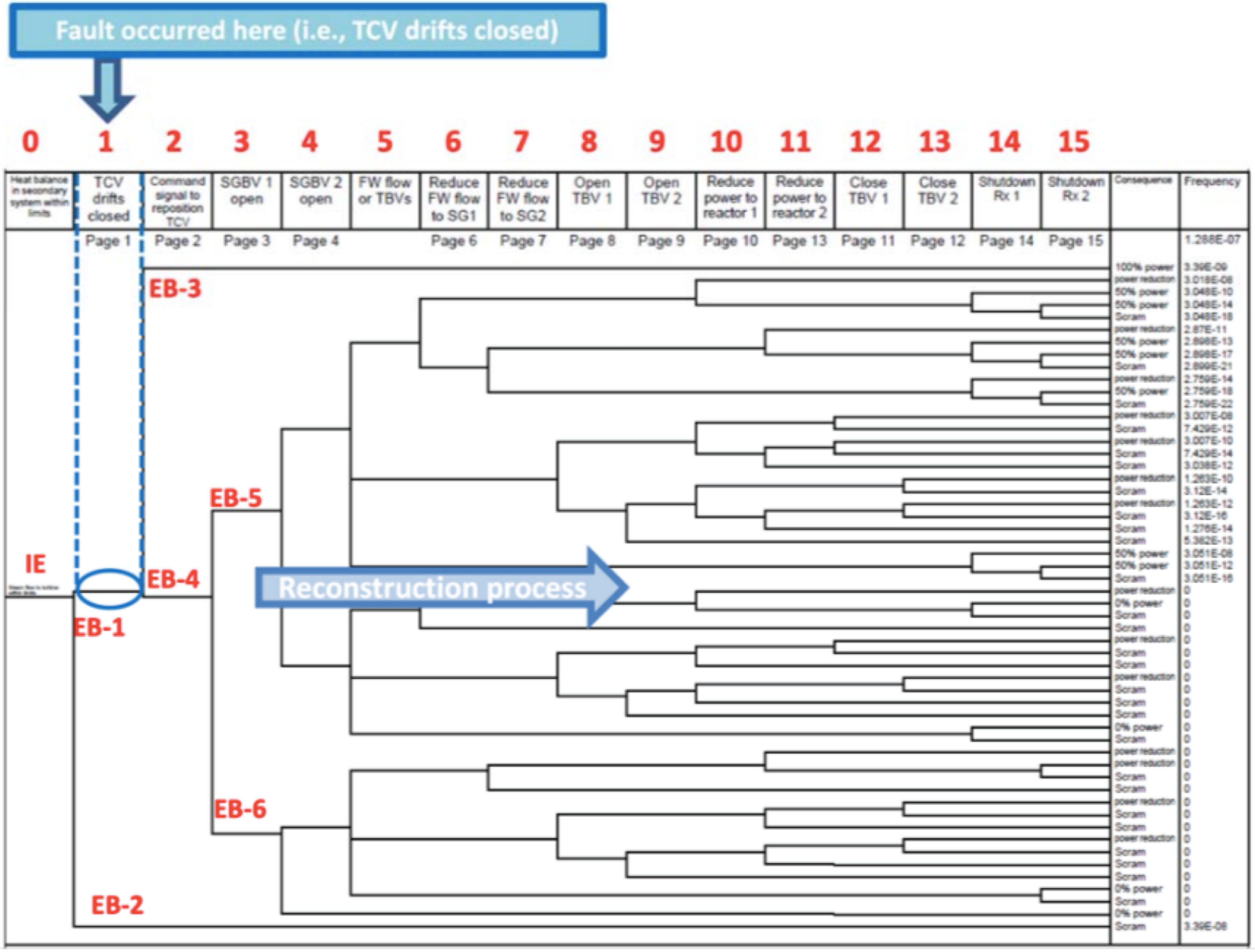
[2]Mean values for FTO and FTC not reported



What are the consequences?

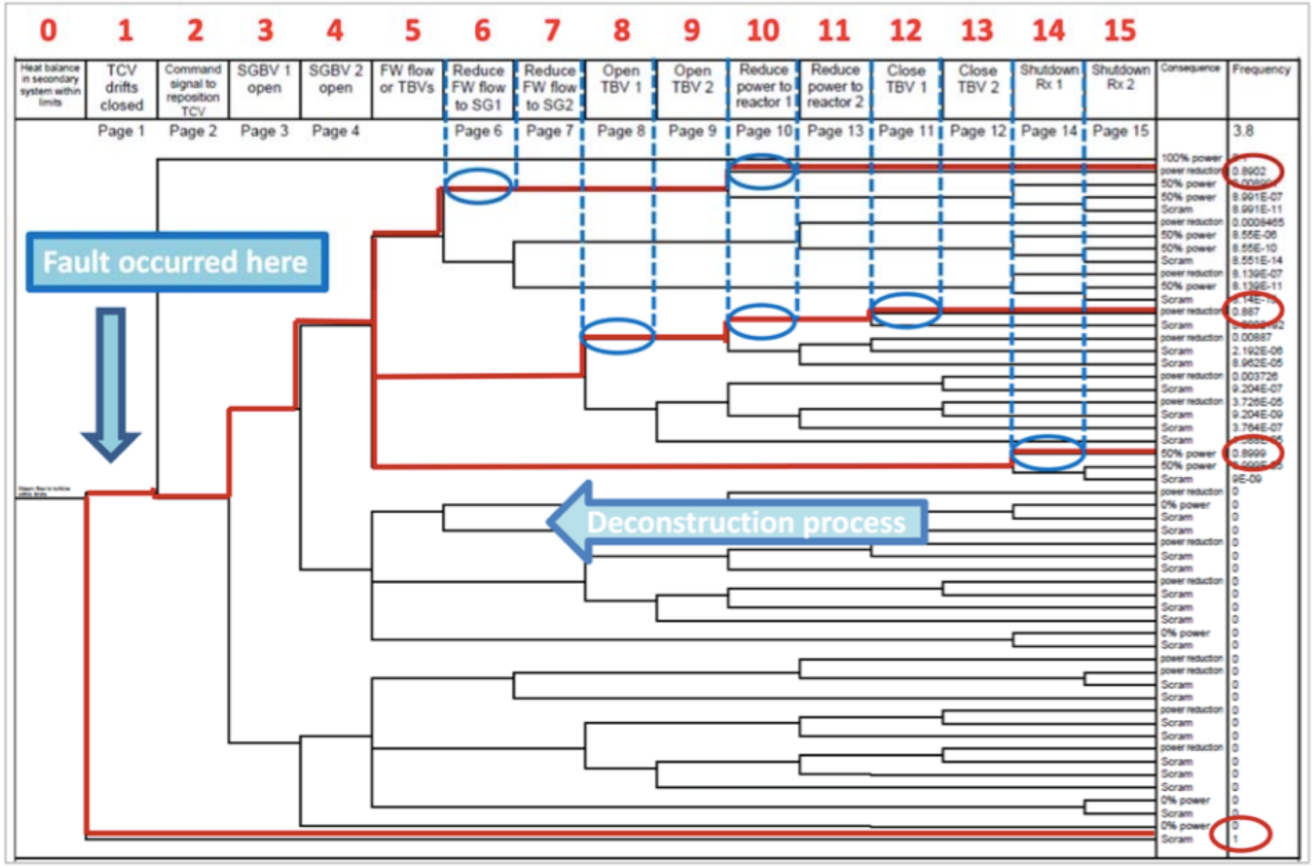
- **Normal operations:** Both reactors operate within normal operational limits.
- **Half power:** One of the reactors is manually shut down without actuating the reactor protection system.
- **Power reduction:** FW or TBV supply flow for 15%–20% percent flow capacity versus main FCVs, which can provide 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.
- **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.
- **Manual shutdown:** Both reactors are manually shut down without scram.

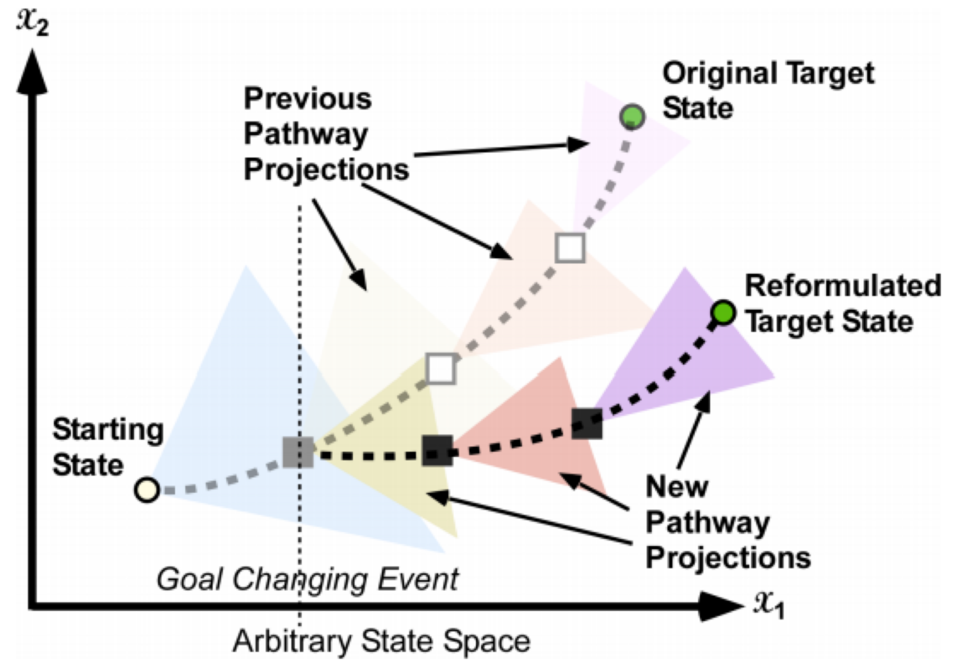
Probabilistic Model of the TCV Drifts in Closed



OAK RIDGE National Laboratory

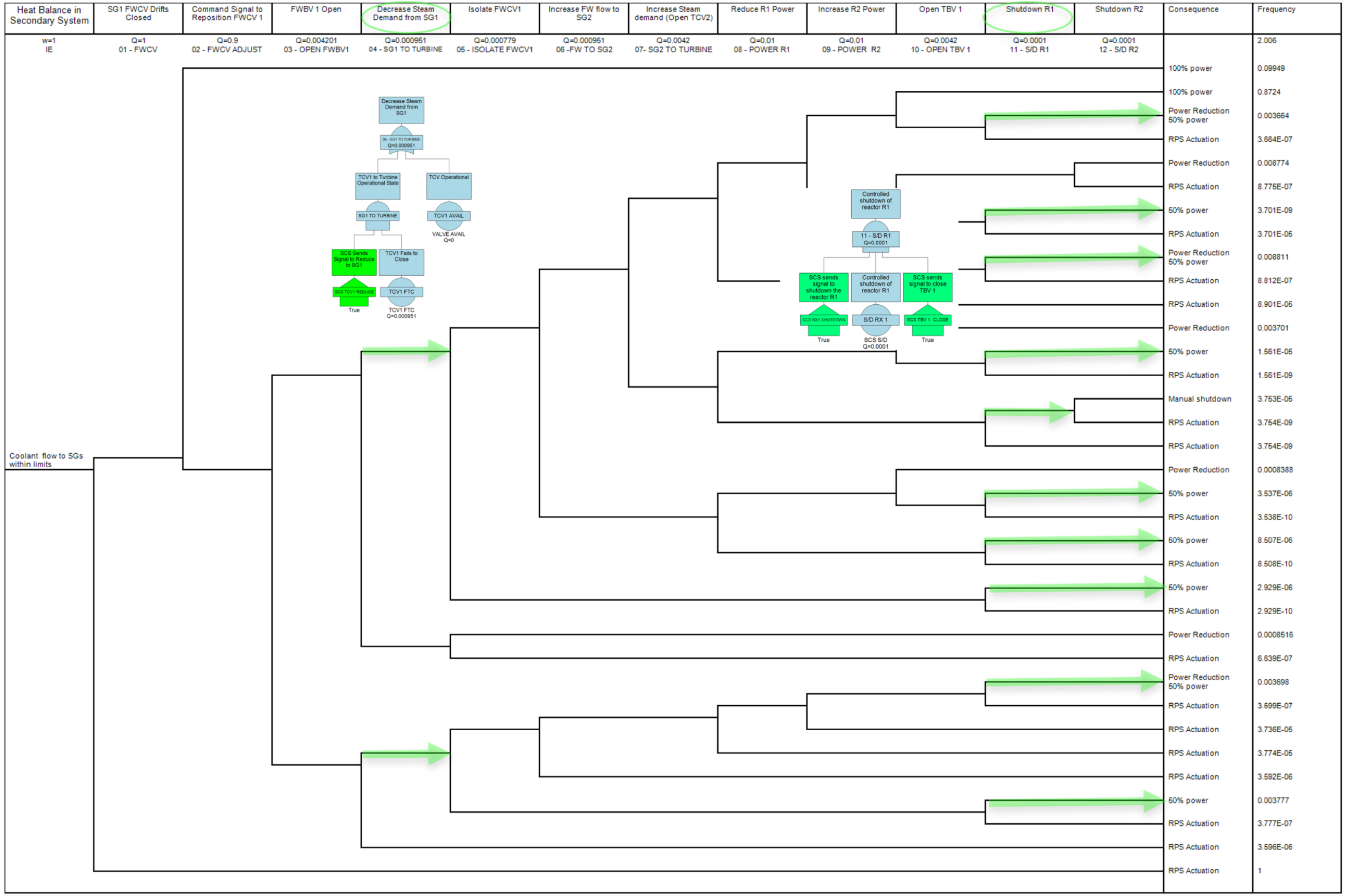
Deconstruction of the Event Tree





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

Event Tree Deconstruction of the FW FCV Drifts in Closed



Control Options Identified

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

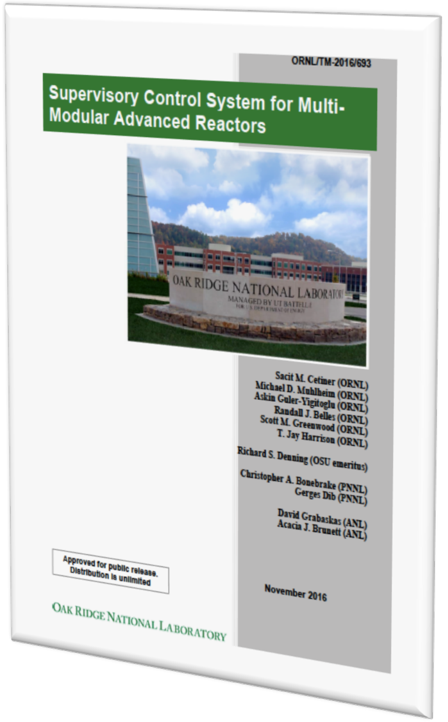
Conclusions

- 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.
- 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 multi-modular systems and potentially reduce operator workload, reduce plant staffing levels, reduce maintenance costs, and avoid unplanned outages.

Acknowledgement

Additional laboratory and university participation:

- Randall J. Belles, Scott M. Greenwood, T. Jay Harrison (ORNL)
- Christopher A. Bonebrake, Gerges Dib (PNNL)
- David Grabaskas, Acacia J. Brunett (ANL)
- Richard S. Denning (OSU emeritus)


ORNL/TM-2016/693

Supervisory Control System for Multi-Modular Advanced Reactors

Sacit M. Cetiner (ORNL)
Michael D. Muhlheim (ORNL)
Askin Guler-Yigitoglu (ORNL)
Randall J. Belles (ORNL)
Scott M. Greenwood (ORNL)
T. Jay Harrison (ORNL)

Richard S. Denning (OSU emeritus)

Christopher A. Bonebrake (PNNL)
Gerges Dib (PNNL)

David Grabaskas (ANL)
Acacia J. Brunett (ANL)

Approved for public release.
Distribution is unlimited

November 2016

OAK RIDGE NATIONAL LABORATORY

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

Questions?

Contact me at yigitoglua@ornl.gov