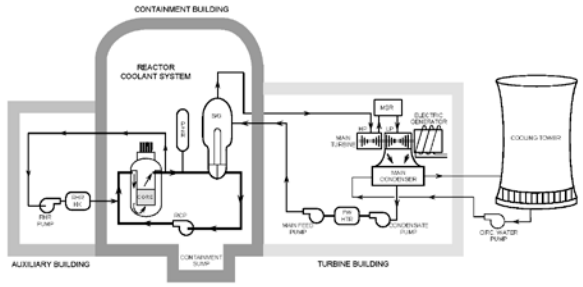
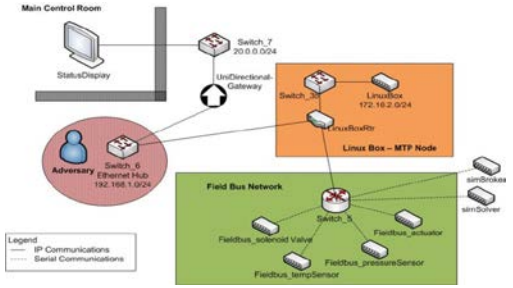
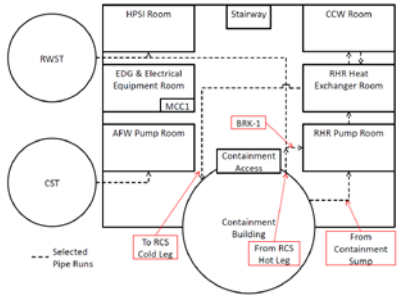
SAND2016-11476C

Exceptional service in the national interest

Sandia National Laboratories







Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model

Presented by Matthew Denman

P.L. Turner, R. A. Williams, J. N. Cardoni T. A. Wheeler

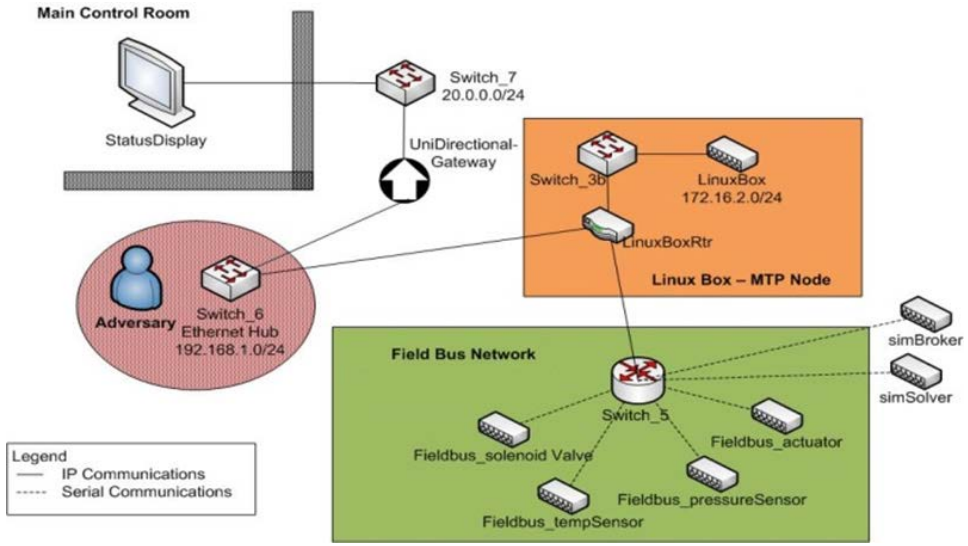
U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

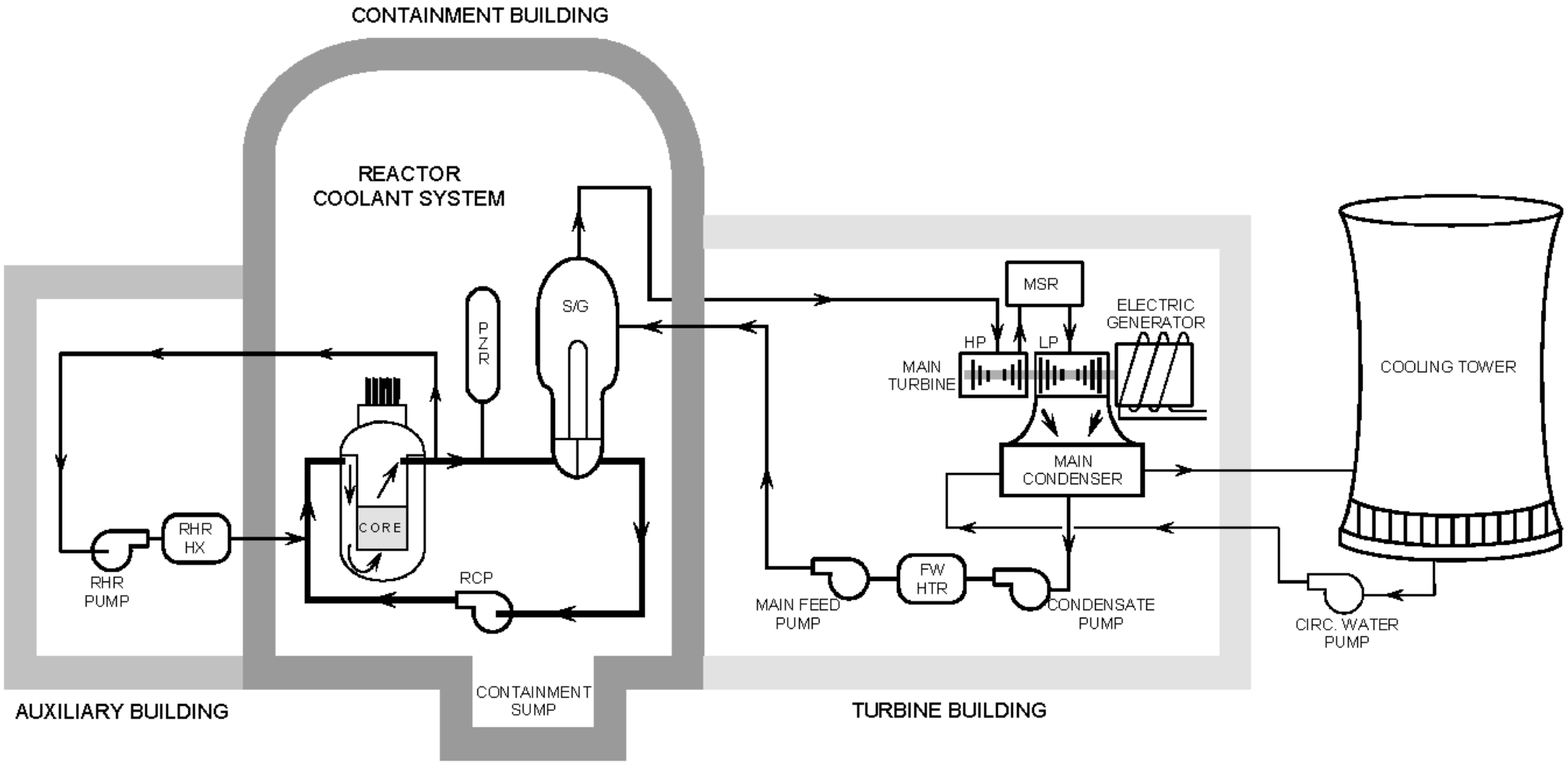
Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview of the Cyber Informed Dynamic Analysis

- Project Overview
  - Motivation – Safety Impact of Digital I&C
    - Defense in Depth –> Prevention may not be enough
    - Dynamic impacts may require simulations to assess impacts
  - Related papers in this conference
- Description of the case study
  - Plant layout
  - Accident sequence
  - Accident Mitigations
  - Path Forward



PWR Layout – Interfacing System LOCA



Project Motivation

- By identifying potential weaknesses in retrofitted DI&C systems before the retrofits occur, future designers can protect against cyber incidents easier, quicker, and cheaper than if the retrofits were found to require further modifications.
- A compromised DI&C system can have common attack vectors and impose common mode failures of active systems that may have been screened out of traditional safety analyses.
  - Mitigation of DI&C failures need to be analyzed at the systems level to ensure that the system is robust to new accident conditions.
  - Studying such potential time-sequenced cyber-attacks and their risks as they pertain to accident management can provide a risk-informed basis for developing effective cyber security controls for nuclear power.

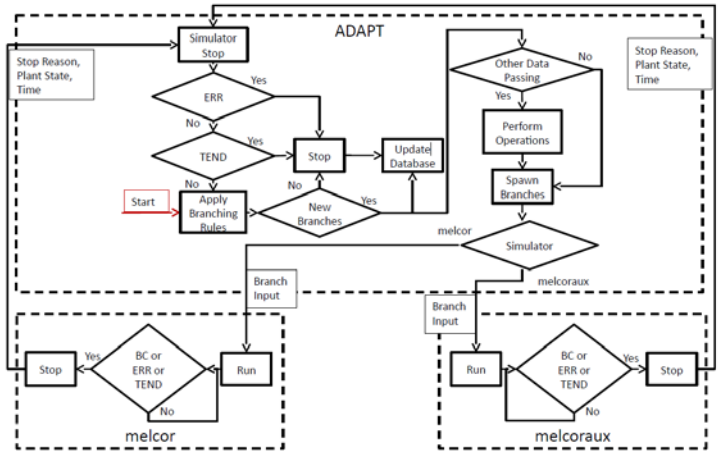
Overlapping roles of safety and security

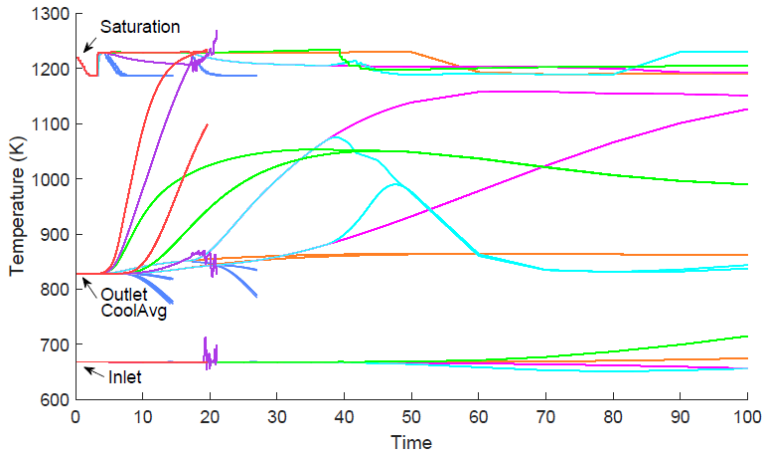
Sandia National Laboratories

- Operator Response is key but DI&C systems can also delay diagnosis and remediation of a resulting transient by providing the operator with misleading data.
- This project is focused on accident sequences that would:
  - Lead relatively quickly to core damage.
  - Have redundancy of components which would cause the accident to be screened through traditional techniques, but
  - The redundancy is completely comprised of active digital components that could possibly be defeated by a cyber-faults.
- Codes and Models used to the support this work:
  - Physical Simulator – MELCOR
  - Cyber Environmental Simulators – OPNET and SCEPTRE (System for Circuit Evaluation and Prediction of Transient Radiation Effects)
  - Exploration of uncertainties – ADAPT (Analysis of Dynamic Accident Progression Trees)
  - Operator Habitability - RADTRAD

Related Publications at this Conference

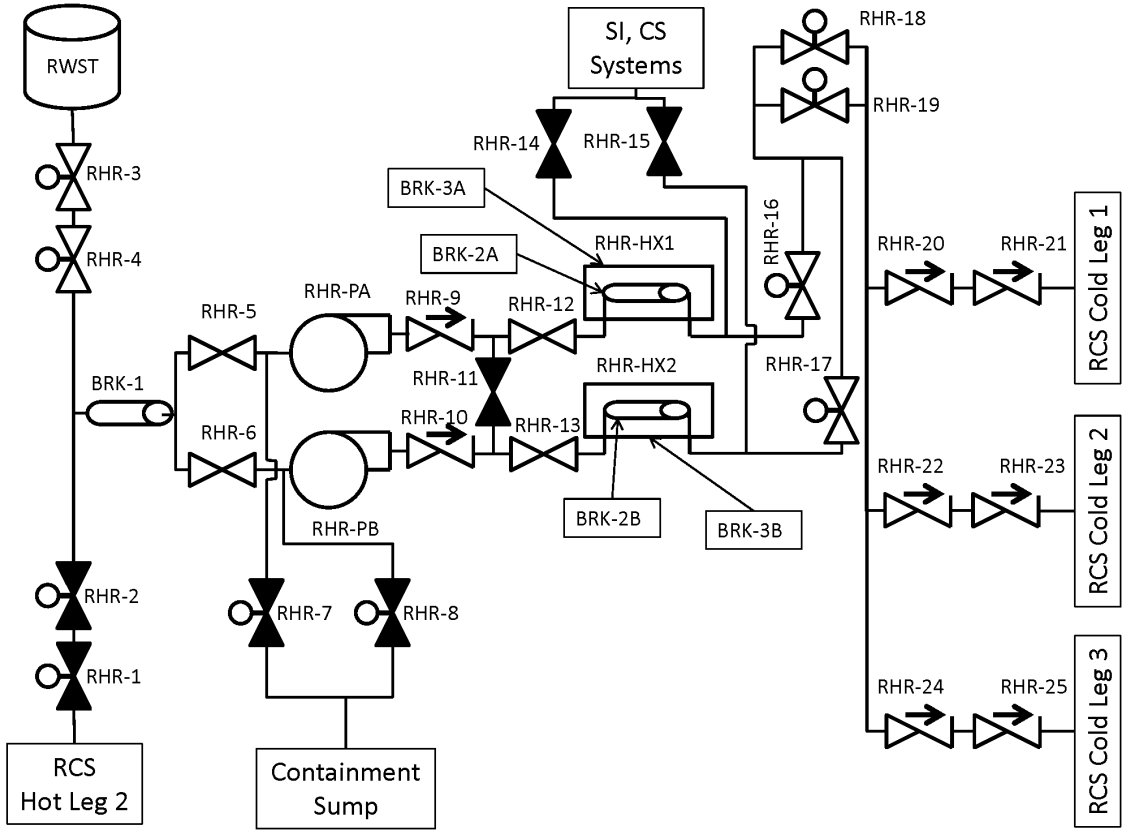
- N. Martin “Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping”
  - Tuesday 1PM: Current Topics in Probabilistic Risk Analysis —I
- M. Denman “Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model”
  - Tuesday 1:25PM: Current Topics in Probabilistic Risk Analysis —I
- Z. Jankovsky “Dynamic Importance Measures in the ADAPT Framework”
  - Tuesday 2:40PM: Current Topics in Probabilistic Risk Analysis —I
- Z. Jankovsky “Conditional Tree Reduction in the ADAPT Framework”
  - Wednesday 10:05AM: Computational Methods
- Z. Jankovsky “Extension of the ADAPT Framework for Multiple Simulators”
  - Wednesday 10:30AM: Computational Methods
- J. Cardoni “Severe Accident Modeling for Cyber Scenarios”
  - Wednesday 1:00PM: Nuclear Installations Safety: General —I





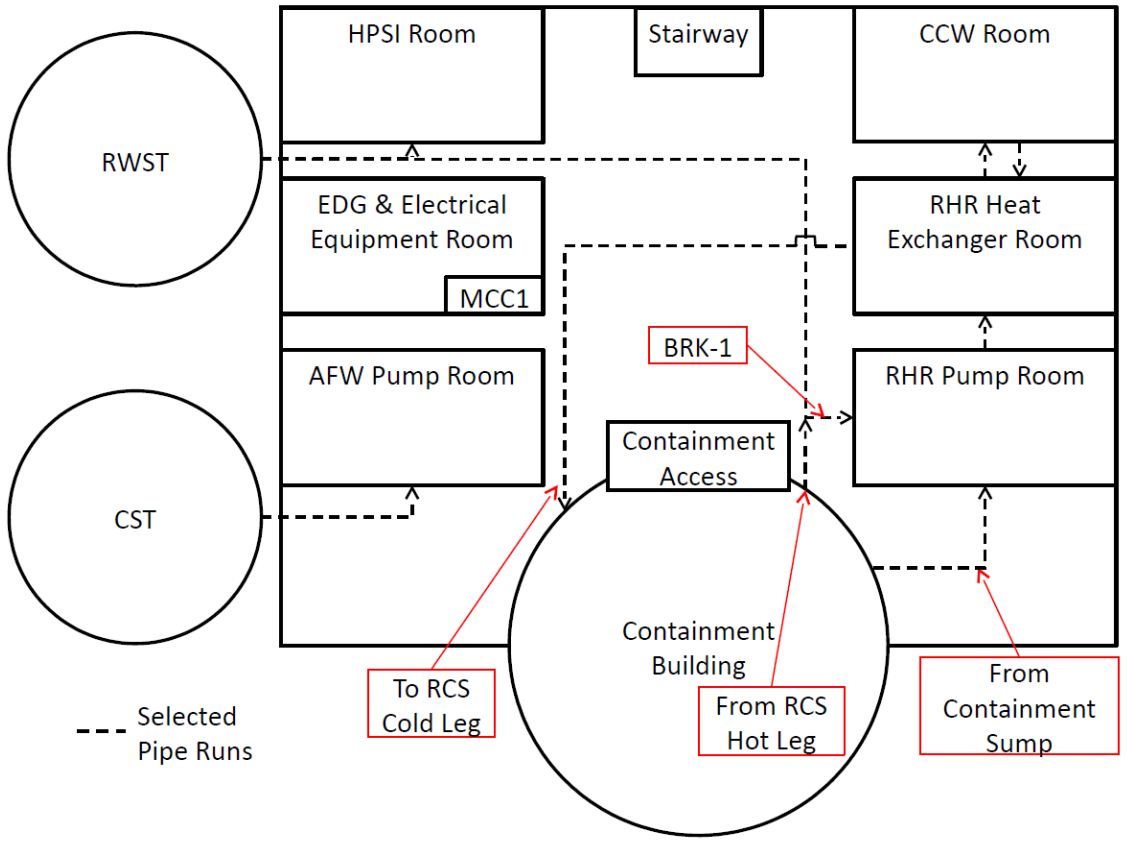
IS-LOCA in the Residual Heat Removal System

- Residual Heat Removal System (RHR) Interfacing System Loss of Coolant Accident (ISLOCA)
  - Both isolation motor-operated valves (MOVs) held open in cyber-induced controller failure
    - Administrative controls may lock the circuit breakers for these MOVs out in some plants
  - May lead to large pipe break outside containment
    - Uncertain timing of initiation and resolution
  - May lead to RHR heat exchanger tube rupture, introducing reactor coolant system (RCS) water into component cooling water (CCW)
    - Possibility of failing CCW, upon which many engineered safety features depend
    - May lose safety injection (SI) pumps



Operator Response and Remediation

- Cyber incidents may require operators to respond to the IS-LOCA from outside the Auxiliary Building
  - Manual signal to isolating the RHR isolation MOV
  - Closing the manual valves in the RHR Pump Room
    - Isolates RWST and prevents further drainage
- Some actions from the control room may help if available:
  - Opening of the Pilot Operated Relief Valves of the Pressurizer



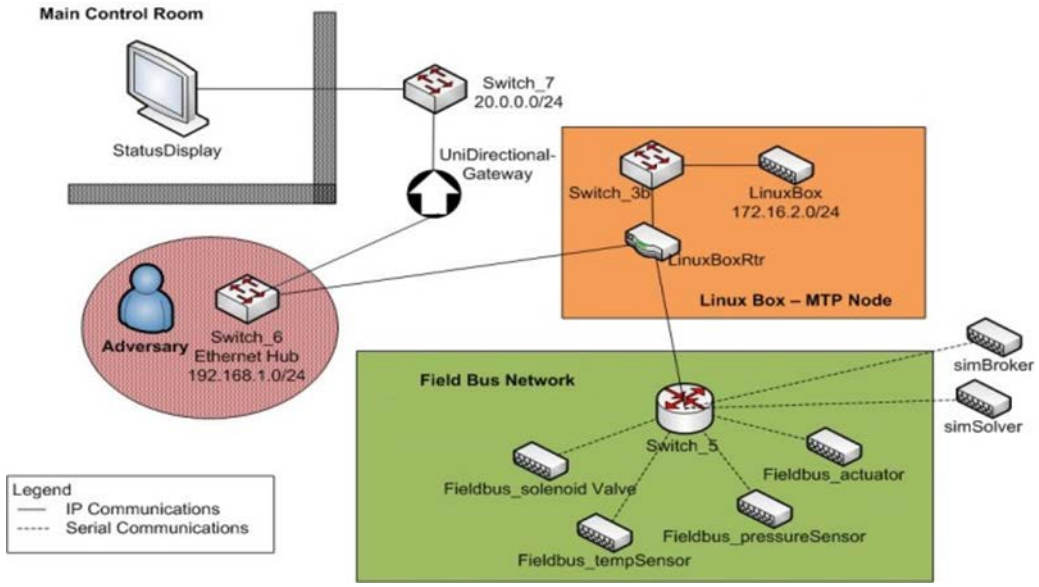
Operators may be hindered in their responce

- Operator Hazards
  - Flooding
  - Steam
  - High Temperatures
  - High Radiation Levels
  - Hydrogen and other combustible materials
- These hazards impact the operators ability to navigate the plant and respond to the accident
  - RADTRAD

Used by permission from TEPCO
Kenji Tetawa

Path Forward

- Conduct integrated cyber-physical-operator assessment of the cyber incident
  - ADAPT controlled and schedule on the SNL Tree Cluster
    - MELCOR - Plant
    - SEPTRE/OPNET – Network
    - RADTRAD – Habitability
  - Evaluate the effectiveness of various mitigation strategies in optimizing the end state of the reactor.
- Study to be finished by September of 2017



Thank you for your time

- This work was supported by the Laboratory Directed Research and Development program at Sandia National Laboratories.
- The Ohio State University (Prof. Tunc Aldimer) was contracted with to made interacting improvements to ADAPT in support of this effort.