Sandia National Laboratories

Exceptional service in the national interest

Use of Modeling and Simulation technologies for Secure By Design (SeBD) Analysis of Advanced Reactors

Presented by Michael T. Rowland

Authors: Shadya Maldonado, Jacob James, Andrew Hahn

SAND2022-14084 C

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

U.S. DEPARTMENT OF ENERGY

NNSA

Our Team

Michael T. Rowland

R&D S&E, Cybersecurity

Electrical Engineer, Cyber Security Engineer, Policy Design Expert

Andrew S. Hahn

R&D S&E, Cybersecurity

Nuclear Engineer, Cyber Security Engineer, Modeling and Simulation Expert, Lead Developer

Shadya B. Maldonado Rosado

R&D S&E, Cybersecurity

Cyber Engineer, Policy Expert, Analytic Methodologist, Cyber Defensive Architecture Expert

Jacob James

R&D S&E, Cybersecurity

Mechanical Engineer, Cyber Security Engineer, Regulatory Expert, STPA Expert

Why to use Models for Cyber Security?

- Models and experimentation allow the evaluation of cyber consequences to systems.
  - Determine Digital Harm from Cyber-Attacks (Data Harm) to Physical Hazards and Losses (Physical Harm)
- Integrate systems hazards analysis techniques (e.g., STPA) with cybersecurity
  - Inherent value (significance) of systems associated with unacceptable or severe consequences
- Rapidly test diverse cyber mitigation strategies
  - Shortens development and testing pipeline for control system and network architecture designs
- Parallel and automated system testing
  - Increased efficiency to iterate cyber experiments
- Cyber sensitivity analysis and discover robustness factors of design alternatives
  - Determine the design features and control system elements that need the most protection without using sensitive cyber threat tools
- Training, exercises, and education of operators
  - Models allow realistic cyber scenarios to be run without risk of equipment

Current Efforts Existing PWRs

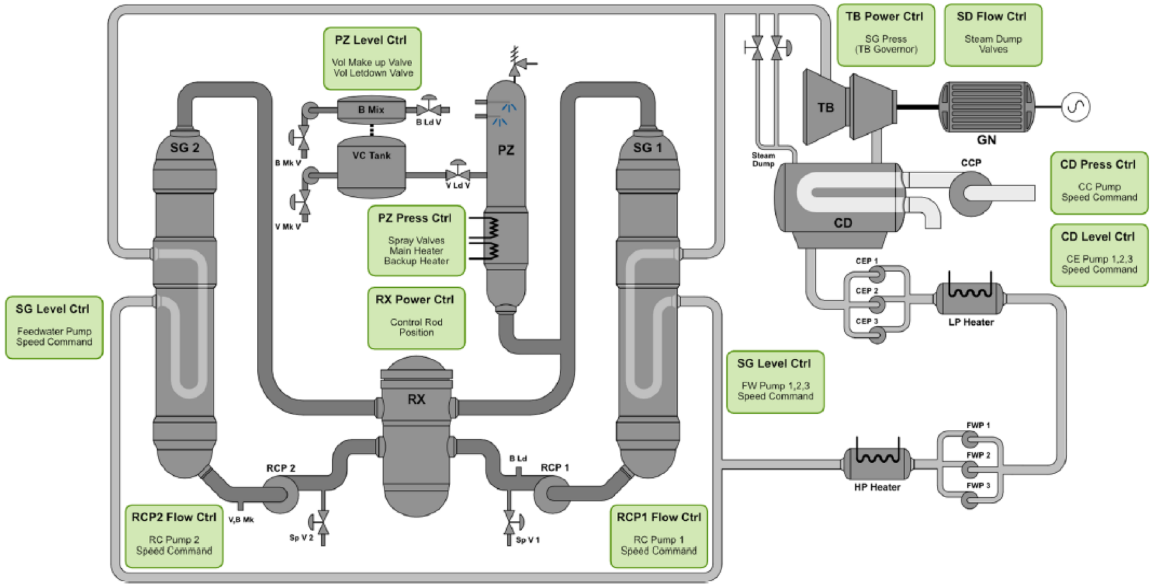
Asherah NPP Simulator

What Asherah is:

- Asherah is developed & maintained by the University of Sao Paulo
- Simulink model of a 2,772 MWt two-loop PWR, loosely based on the TMI Unit 1 B&W design.
- Can be run with or without internal Simulink controllers
- External controllers and human machine interfaces can be interfaced with using ModbusTCP or OPC UA
- Tuned using PARCS/RELAP

What Asherah is **not**:

- Qualified plant simulator
- Based exactly on an existing plant
- Network emulator
- Complete simulation of all controllers, alarms, and annunciators found in an actual plant
- Control room emulator/simulator



Citation: Silva RB, Shirvan K, Piqueira JR, Marques RP. Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment. International Conference on Nuclear Security (ICONS), 10-14 Feb 2020 in Vienna Austria 2020.

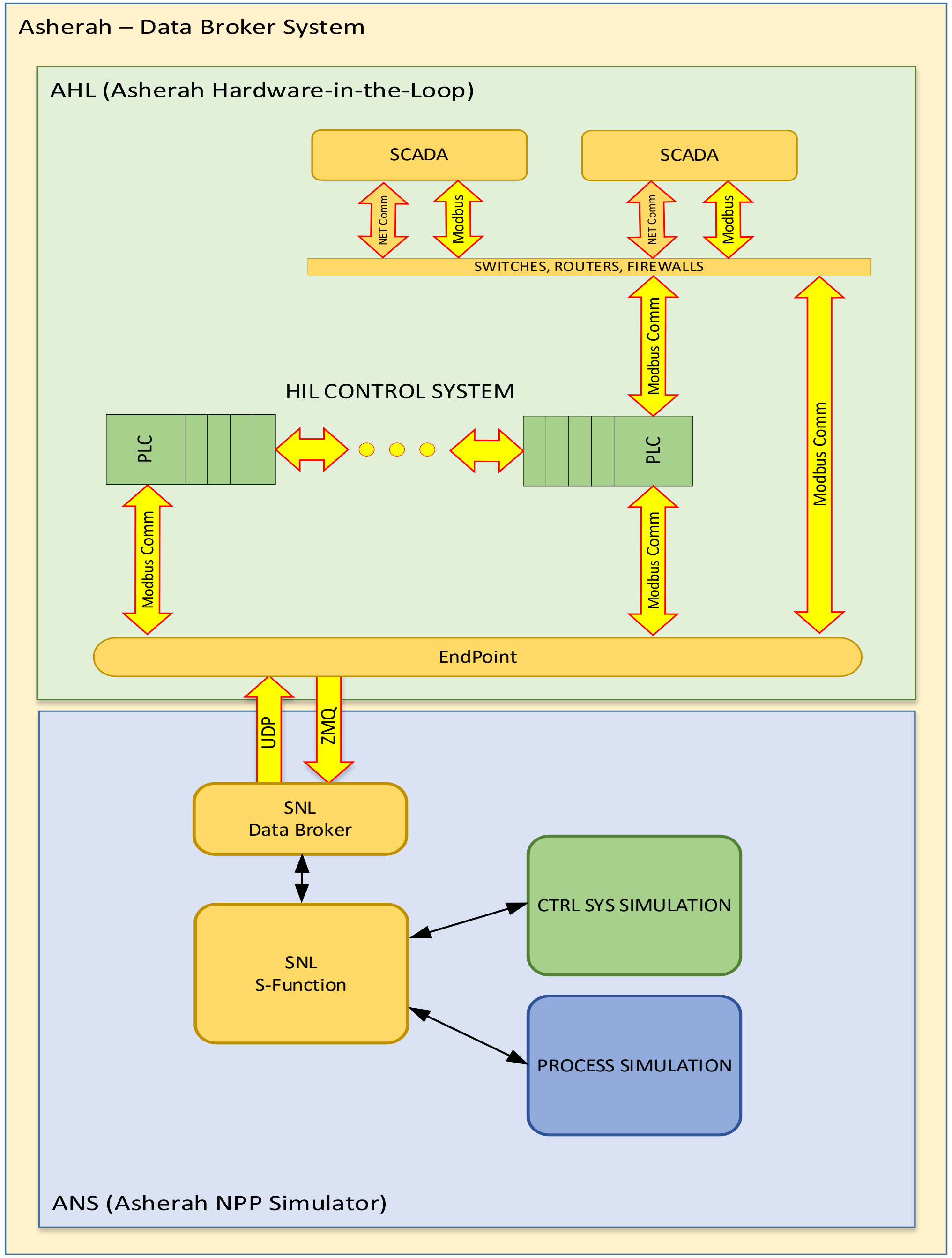
Sandia Current Efforts – Data Broker Integration

- ➢ Centralizes system control and setup

- ➢ Reduces the complexity of OT network and simulator interface

- ➢ On-the-fly switching between internal and external controllers

- ➢ Highly flexible, allows the control system to be broken out from the model in a selectable and automatic manner

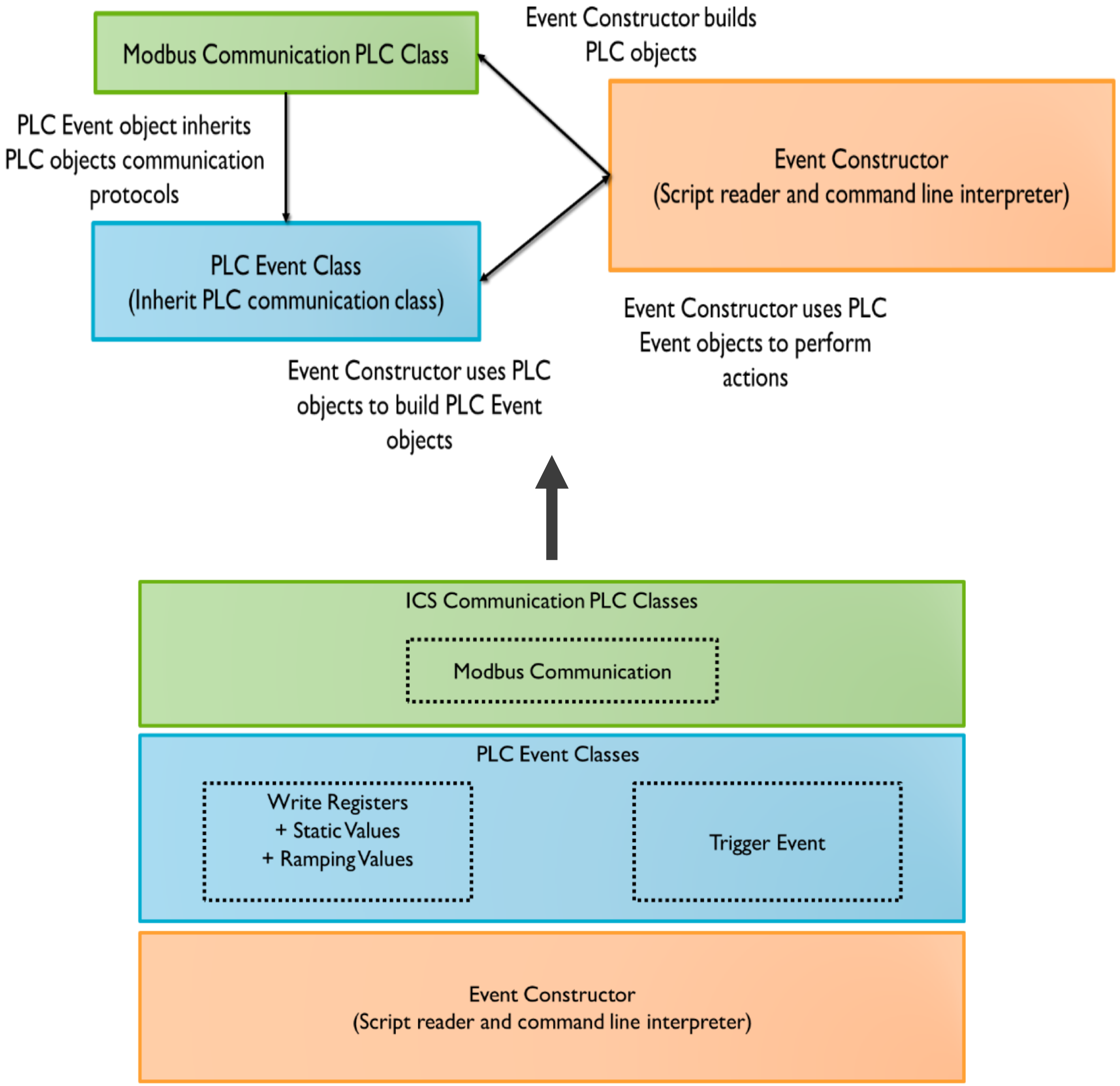


https://github.com/sandialabs/SMARTT/tree/main/OT_Emulation_Data_Broker

Sandia Current Efforts – ManiPIO

Manipulate Process I/O (ManiPIO) is an ICS evaluation tool that:

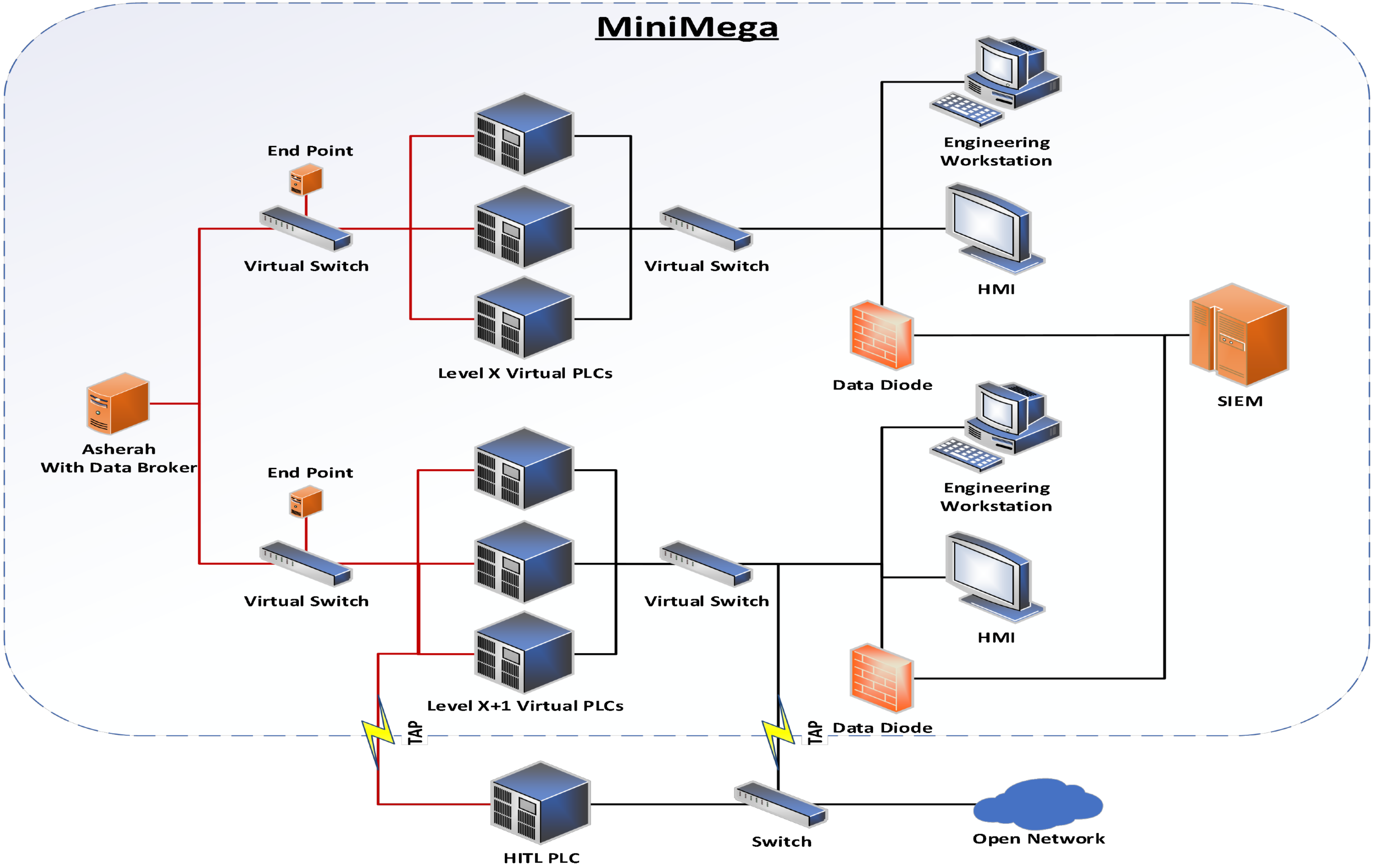
- Aids in the evaluation of the cyber security risks and resilience in ICS networks
- Provides a highly reproducible method to simulate cyber manipulations on ICS networks for training, education, and research
- Allows university partners and national laboratory researchers access to a shared utility in order to facilitate collaborative research
- Allows execution of user generated scripts and automatically generated scripts
- Is modular, allowing flexibility to add new features and ICS network protocols



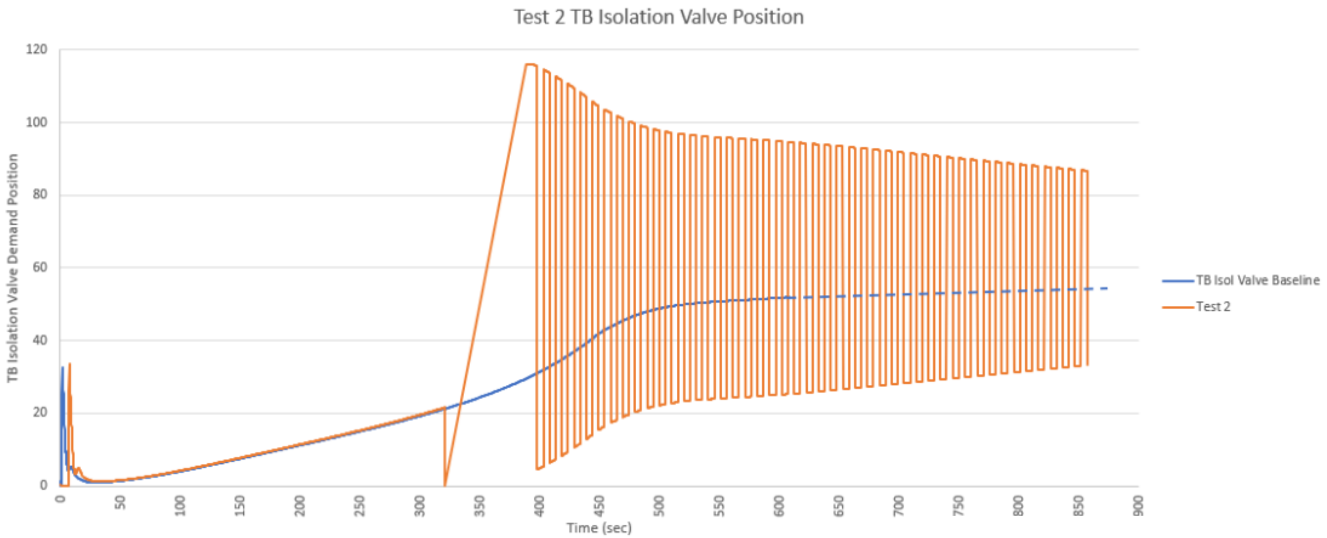
Modbus Communication PLC Class
Event Constructor builds PLC objects
PLC Event object inherits PLC objects communication protocols
Event Constructor (Script reader and command line interpreter)
PLC Event Class (Inherit PLC communication class)
Event Constructor uses PLC Event objects to perform actions
Event Constructor uses PLC objects to build PLC Event objects
ICS Communication PLC Classes
Modbus Communication
PLC Event Classes
Write Registers + Static Values + Ramping Values
Trigger Event
Event Constructor (Script reader and command line interpreter)

https://github.com/sandialabs/SMARTT/tree/main/ManiPIO

Sandia Current Efforts – Network Emulation

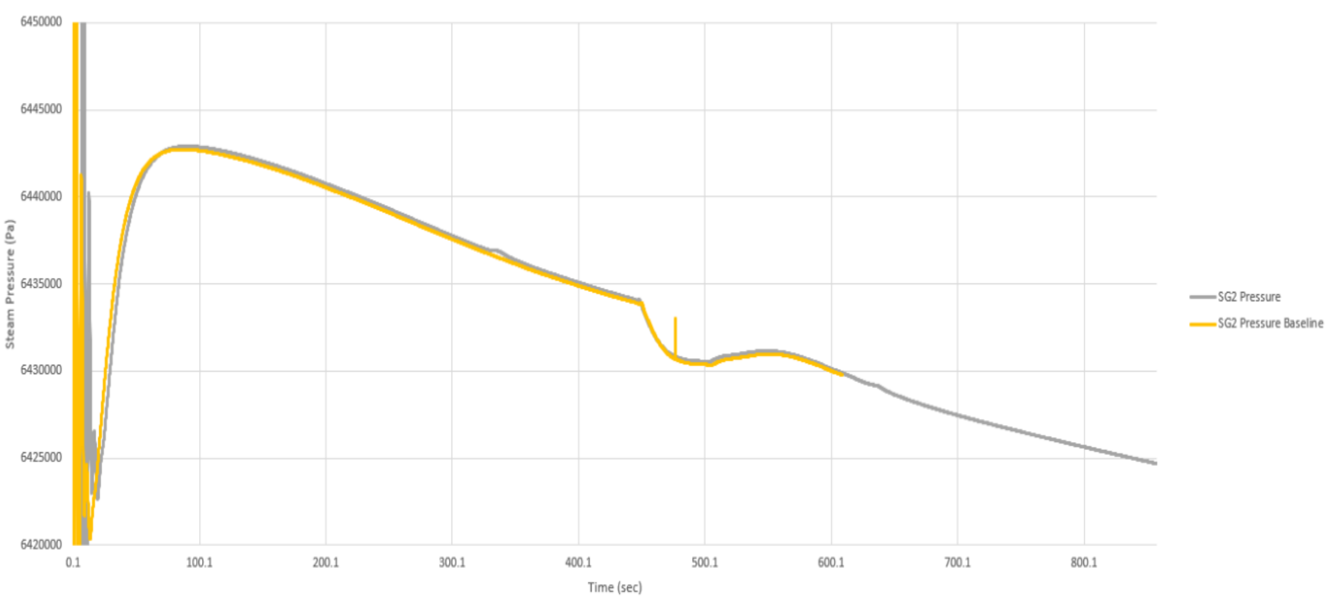


Sandia Current Efforts – Research Analysis – Design Elements



Test 2 Effects – Valve Position - DH

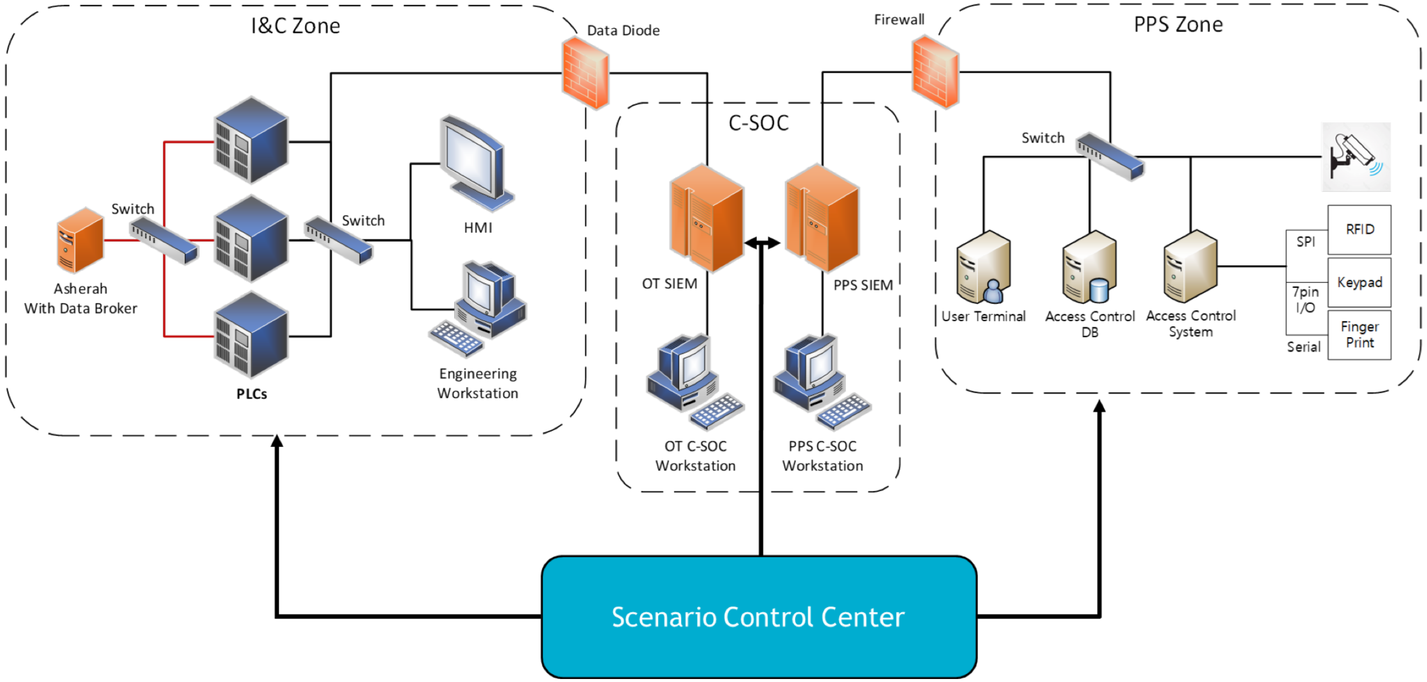
SG Pressures – PIH



Citation: Rowland, MT. Investigation of Data Harm and its Relevance to Unsafe Control Actions of Control Systems through Application of the Information Harm Triangle (2022)

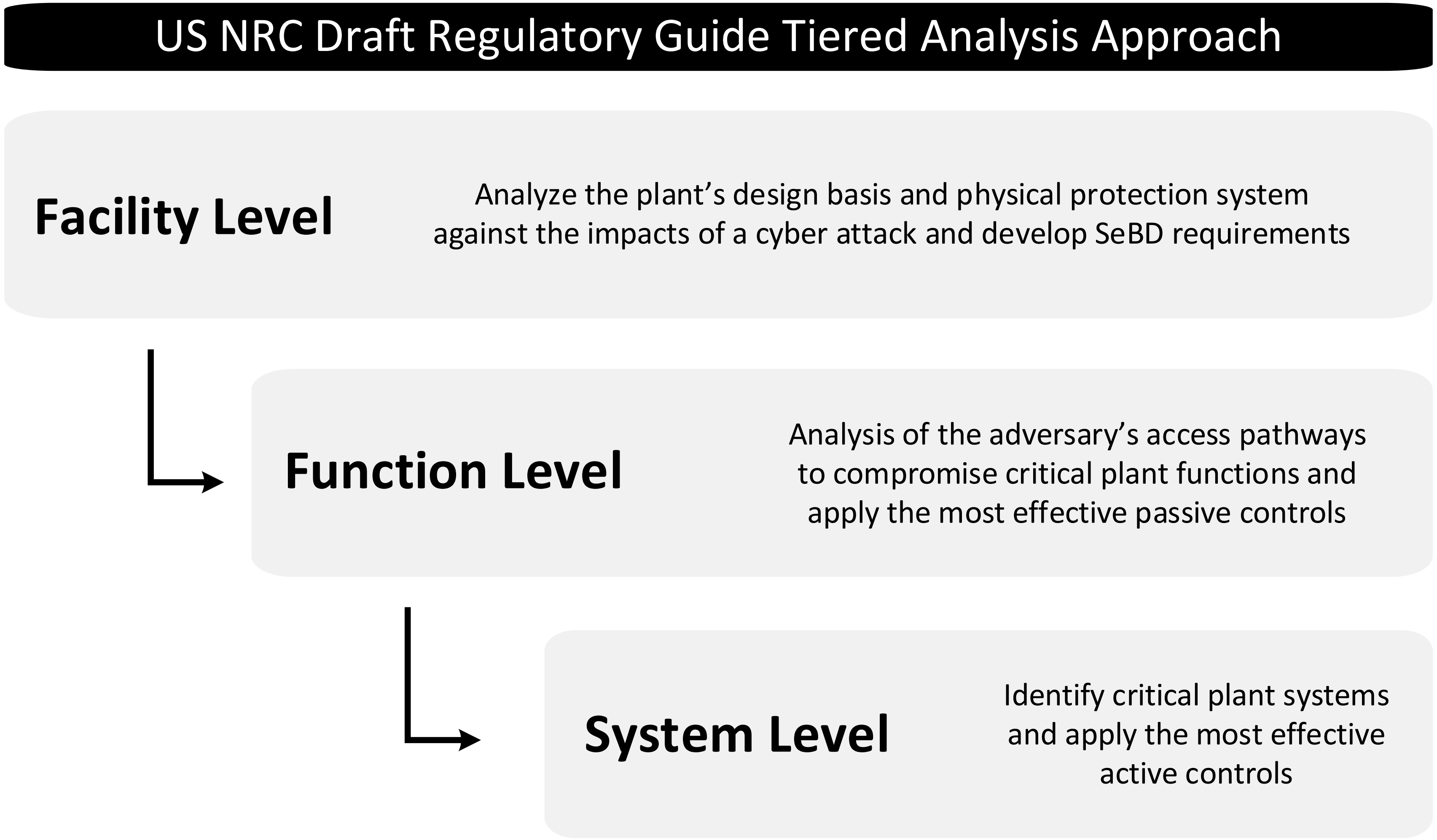
Sandia Current Efforts - Conclusions

- Models allow the study of the highly coupled systems of physics, control systems, and networks.
- Without models of plants, cyber security research is unbounded with respect to consequence based solutions.
- Models allow us to investigate through extensive iteration what systems need protection and how effective defensive architecture hypothesis are.
- Reduce cyber security costs by prioritizing efficient solutions.
- Train current operators on effective cyber responses.
- Educate future professionals on design robustness factors and SeBD approaches.



Advanced Reactors Regulatory Approach

Cybersecurity analysis for advanced reactors



US NRC Draft Regulatory Guide Tiered Analysis Approach

Facility Level

Analyze the plant's design basis and physical protection system against the impacts of a cyber attack and develop SeBD requirements

Function Level

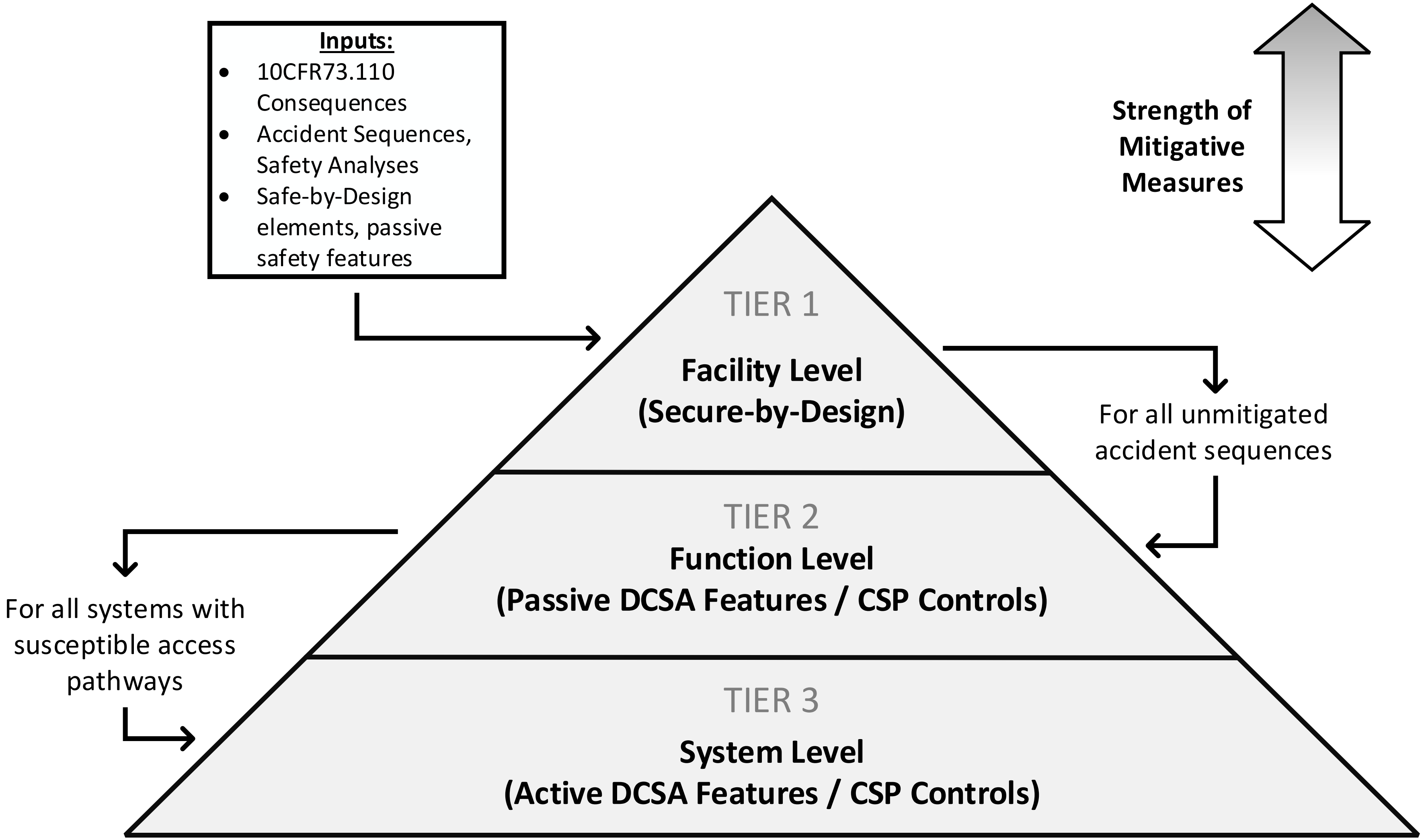
Analysis of the adversary's access pathways to compromise critical plant functions and apply the most effective passive controls

System Level

Identify critical plant systems and apply the most effective active controls

Citation: Jauntirans J, Garcia I, Rowland M T. U.S.A Regulatory Efforts for Cybersecurity of Small Modular Reactors/Advanced Reactors. IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors. 21-25 Feb in Vienna Austria 2022.

Cybersecurity analysis for advanced reactors

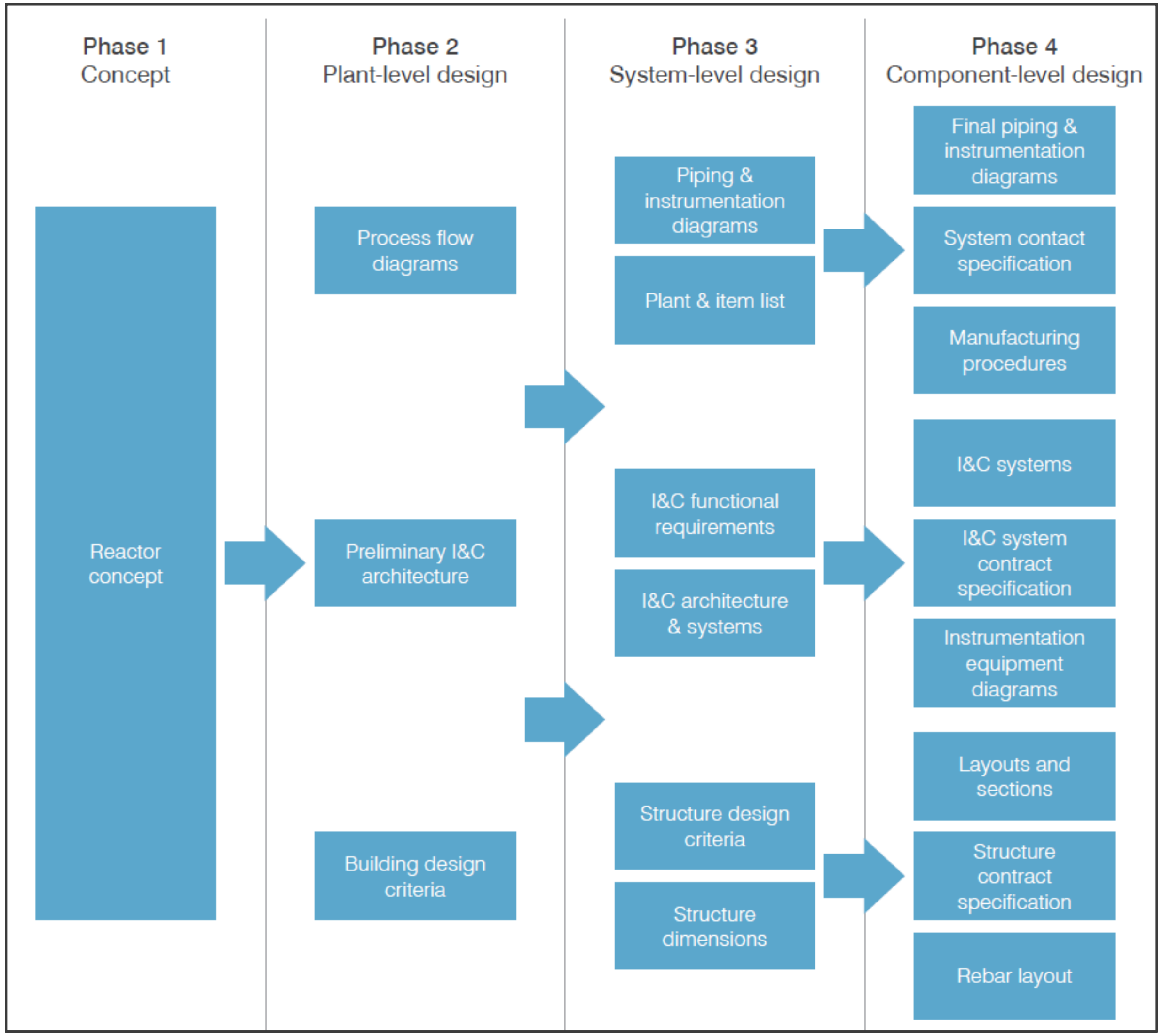


Inputs:
- 10CFR73.110 Consequences
- Accident Sequences, Safety Analyses
- Safe-by-Design elements, passive safety features

Strength of Mitigative Measures
TIER 1
Facility Level (Secure-by-Design)
For all unmitigated accident sequences
TIER 2
Function Level (Passive DCSA Features / CSP Controls)
For all systems with susceptible access pathways
TIER 3
System Level (Active DCSA Features / CSP Controls)

Citation: Jauntirans J, Garcia I, Rowland M T. U.S.A Regulatory Efforts for Cybersecurity of Small Modular Reactors/Advanced Reactors. IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors. 21-25 Feb in Vienna Austria 2022.

SeBD and Design Maturity



Phase 1
Concept

- Reactor concept

Phase 2
Plant-level design

- Process flow diagrams
- Preliminary I&C architecture
- Building design criteria

Phase 3
System-level design

- Piping & instrumentation diagrams
- Plant & item list
- I&C functional requirements
- I&C architecture & systems
- Structure design criteria
- Structure dimensions

Phase 4
Component-level design

- Final piping & instrumentation diagrams
- System contact specification
- Manufacturing procedures
- I&C systems
- I&C system contract specification
- Instrumentation equipment diagrams
- Layouts and sections
- Structure contract specification
- Rebar layout

Design Maturity Phase	Cybersecurity Analysis Tier
1-2	Tier 1 Facility Level: Analysis is based on theoretical reactor concept and can inform elements of Plant-Level Design.
3	Tier 2 Function Level: Analysis occurs during the development of I&C functional requirements and architecture where passive features (segmentation, physical separation) are credited.
4	Tier 3 System Level: Most mature level of analysis is required in order to implement effective network and device-specific controls.

Citation: World Nuclear Association (WNA). Design Maturity and Regulatory Expectations for Small Modular Reactors. Report No. 2021/001. June 202

Modeling challenges for cybersecurity analysis

- Verification of mitigative SeBD measures
  - How long do design features delay an attacker?
  - Can long do automated plant systems and operators have to respond to an attack?
- Control proficiency and efficiency
  - Tuning technical control measures with simulation
- Faster scenario development and modeling
  - Machine learning to compile TTPs into attacks
  - Attack and response modeling with SDN and SOC

Research Future

What is needed to leverage models for new regulatory approach?

- Matlab Simulink Models of Power Plants
  - Matlab Simulink in plug and play with our system
  - POSIX (Portable Operating System Interface) based core functions allow our system to integrate with nearly any codebase
- Diverse Sets of Real-Time Models of Power Plants
  - Advanced Nuclear
  - SMR
  - Micro-Reactors
  - Research Reactors
- Control System Logic for Plant Models
- Network Topologies of Plants

FY23 Sandia Activities

- Integrate into our environment
  - Improve integration schemes
  - Progress to full emulation/simulation of physics, control system, cybersecurity toolkits, and network package
- Improve analysis toolset
  - Retool and improve current set of tools (open-source software)
  - Develop new analysis tools and techniques
  - Generate a full set of tools for each tier of analysis (US NRC approach)
- Advance and Mature Best Practices and Approaches and Cyber Security
  - Develop regulatory guidance and technical basis documentation in support of international nuclear security (INS) capacity building
  - Continue to support the development of best practices (IAEA, IEC, IEEE)
- Support Domestic and International Capacity Building
  - Collaborate with Universities and AR Vendors Research Activities
  - Develop publicly available publications and technical reports

Thank you for your time and attention

Contact Information

Michael T. Rowland mtrowla@sandia.gov

Lon Dawson ladawso@sandia.gov

Sandia Current Efforts

Connecting the physical, cyber, and nuclear industry operations with modeling simulation technology and resources

Approach

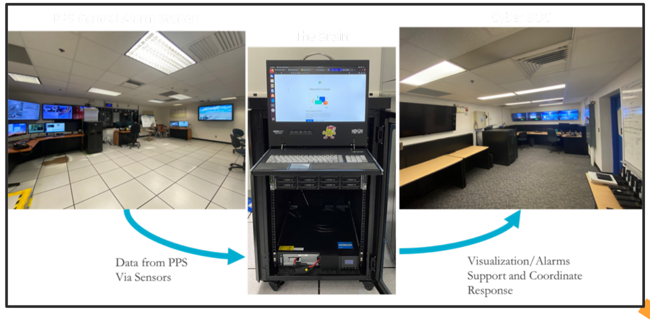
1) Cyber Field Training Exercises (e.g., cyber campaign emulation)

2) Developed SIMULATOR in-person or online training with partner countries (e.g, Brazil)

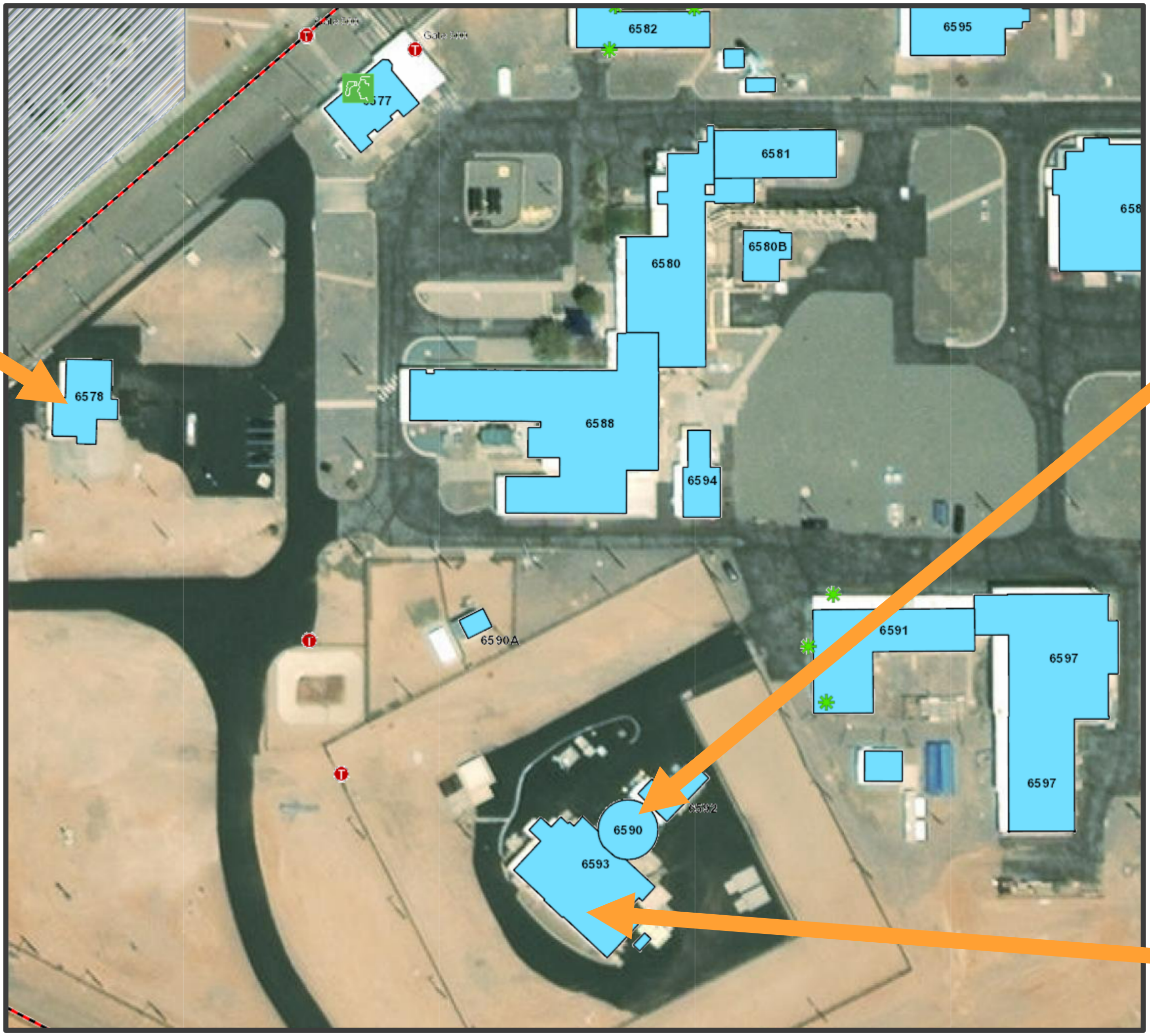
3) Simulated the performance of systems under a cyber attack

4) Mod/sim experimentation to evaluate analysis techniques

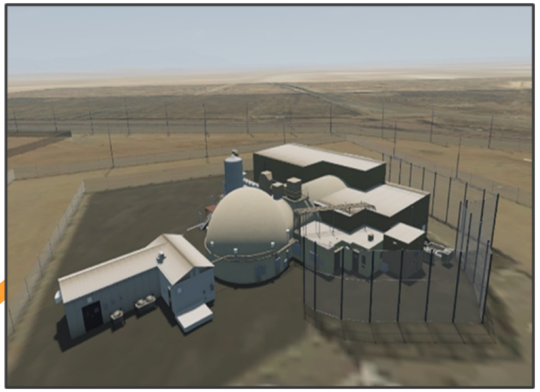
1. Modeling & Simulation for Training Exercises



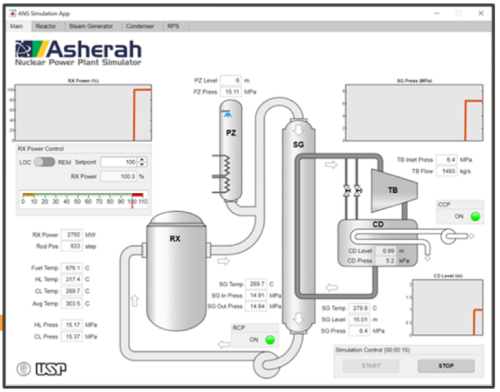
CSOC (Basement)



Physical Mock Reactor



Canada Exercise: Asherah



PZ Level 6 m

PZ Press 15.11 MPa

RX Power Control

LOC REM Setpoint 100

RX Power 100.3 %

TB Inlet Press 6.4 MPa

TB Flow 1493 kg/s

CCP ON

RX Power 2782 MW

Rod Pos 833 step

Fuel Temp 676.1 C

HL Temp 317.4 C

CL Temp 289.7 C

Avg Temp 303.5 C

HL Press 15.17 MPa

CL Press 15.37 MPa

CD Level 0.99 m

CD Press 5.2 kPa

SG Temp 289.7 C

SG In Press 14.91 MPa

SG Out Press 14.84 MPa

RCP ON

SG Temp 279.8 C

SG Level 15.01 m

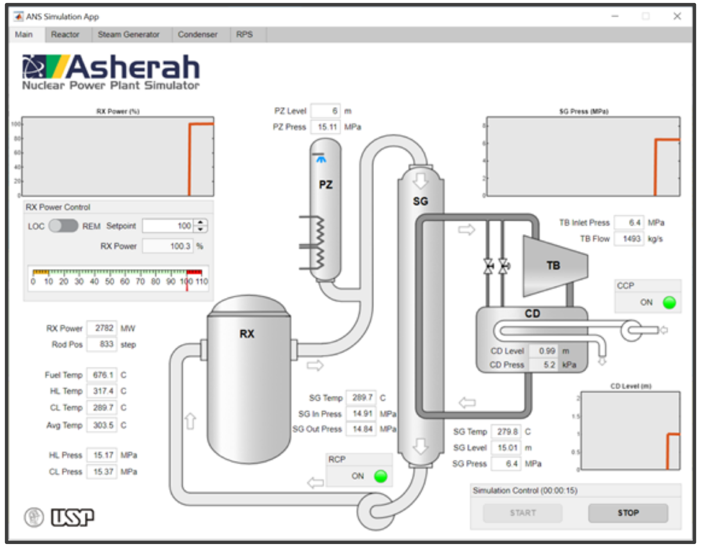
SG Press 6.4 MPa

Simulation Control (00:00:15)

Digital Representation Asherah

2. Simulating Reactor Operations for online and in-person training

Infrastructure



PZ Level 6 m
PZ Press 15.11 MPa

RX Power Control
Setpoint 100
RX Power 100.3 %

TB Inlet Press 6.4 MPa
TB Flow 1493 kg/s

CCP ON

RX Power 2782 MW
Rod Pos 833 step

Fuel Temp 676.1 C
HL Temp 317.4 C
CL Temp 289.7 C
Avg Temp 303.5 C

HL Press 15.17 MPa
CL Press 15.37 MPa

SG Temp 289.7 C
SG In Press 14.91 MPa
SG Out Press 14.84 MPa

CD Level 0.99 m
CD Press 5.2 kPa

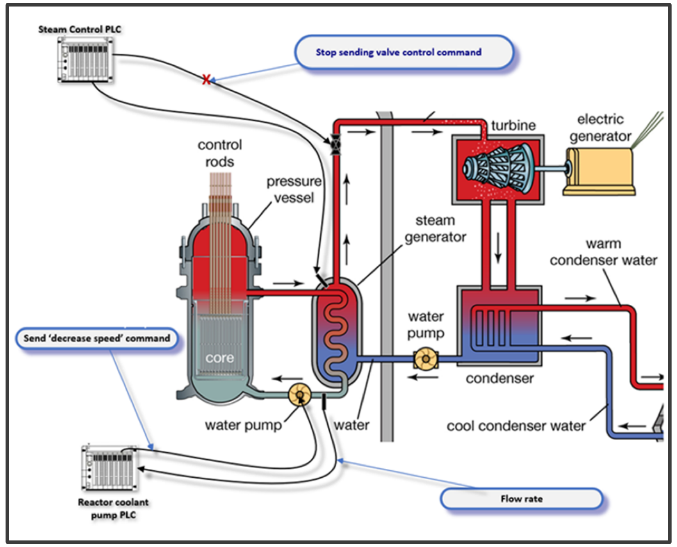
SG Temp 279.8 C
SG Level 15.01 m
SG Press 6.4 MPa

RCP ON

Simulation Control (00:00:15)

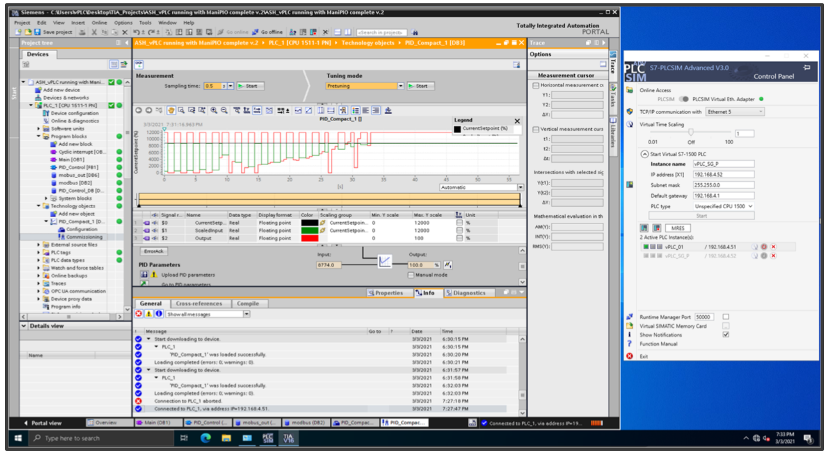
Asherah NPP Simulator

Blended Scenario Design



Steam generator pressure & reactor coolant pump controllers

Useable and Fieldable Tools



Input: 8774.0
Output: 100.0 %
□ Manual mode

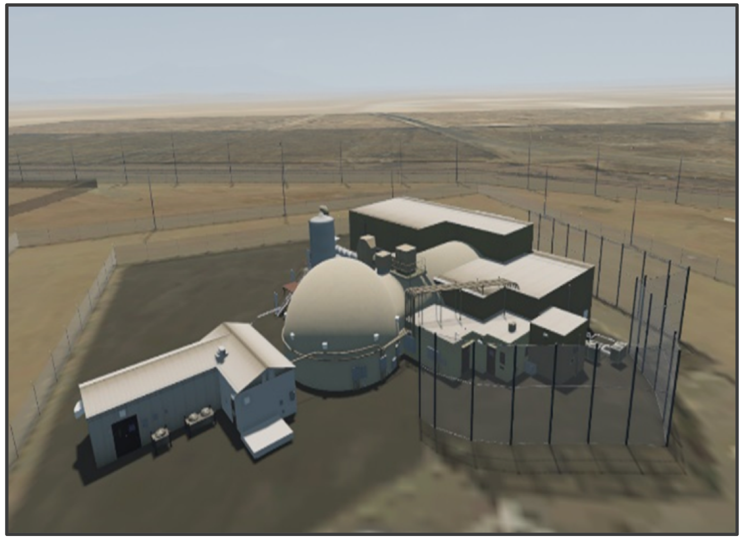
```
Message                                              Date       Time
Start downloading to device.                         3/3/2021   6:30:15 PM
  PLC_1                                              3/3/2021   6:30:15 PM
    'PID_Compact_1' was loaded successfully.         3/3/2021   6:30:20 PM
  Loading completed (errors: 0; warnings: 0).        3/3/2021   6:30:21 PM
Start downloading to device.                         3/3/2021   6:31:57 PM
  PLC_1                                              3/3/2021   6:31:58 PM
    'PID_Compact_1' was loaded successfully.         3/3/2021   6:32:03 PM
  Loading completed (errors: 0; warnings: 0).        3/3/2021   6:32:03 PM
  Connection to PLC_1 aborted.                       3/3/2021   7:27:18 PM
  Connected to PLC_1, via address IP=192.168.4.51.   3/3/2021   7:27:47 PM
```

Online Access
PLCSIM PLCSIM Virtual Eth. Adapter
TCP/IP communication with Ethernet 5
Virtual Time Scaling 1 (0.01 Off 100)
Start Virtual S7-1500 PLC
Instance name vPLC_SG_P
IP address [X1] 192.168.4.52
Subnet mask 255.255.0.0
Default gateway 192.168.4.1
PLC type Unspecified CPU 1500
2 Active PLC Instance(s):
vPLC_01 / 192.168.4.51
vPLC_SG_P / 192.168.4.52
Runtime Manager Port 50000 □
Virtual SIMATIC Memory Card
Show Notifications ☑

Siemens PLCSIM Advanced

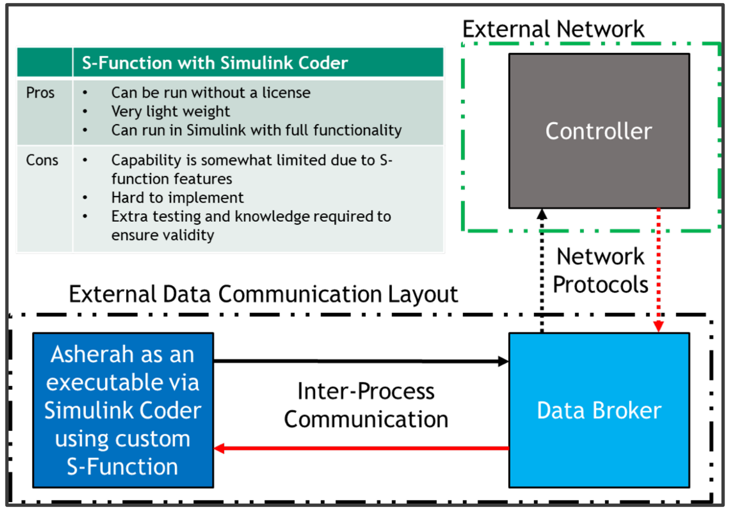
3. Simulated the performance of systems under a cyber attack

Asherah Simulator



Located within the Mock Reactor

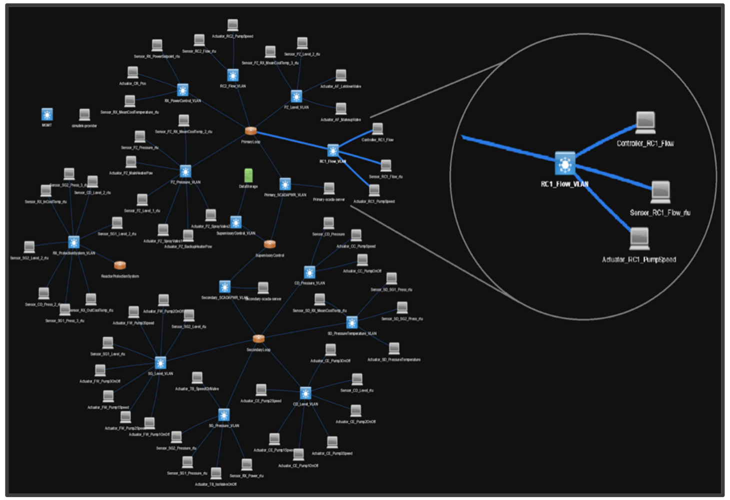
Physics Simulator + Asherah simulator integration



	S-Function with Simulink Coder
Pros	• Can be run without a license • Very light weight • Can run in Simulink with full functionality
Cons	• Capability is somewhat limited due to S-function features • Hard to implement • Extra testing and knowledge required to ensure validity

External Network
Controller
Network Protocols
External Data Communication Layout
Asherah as an executable via Simulink Coder using custom S-Function
Inter-Process Communication
Data Broker

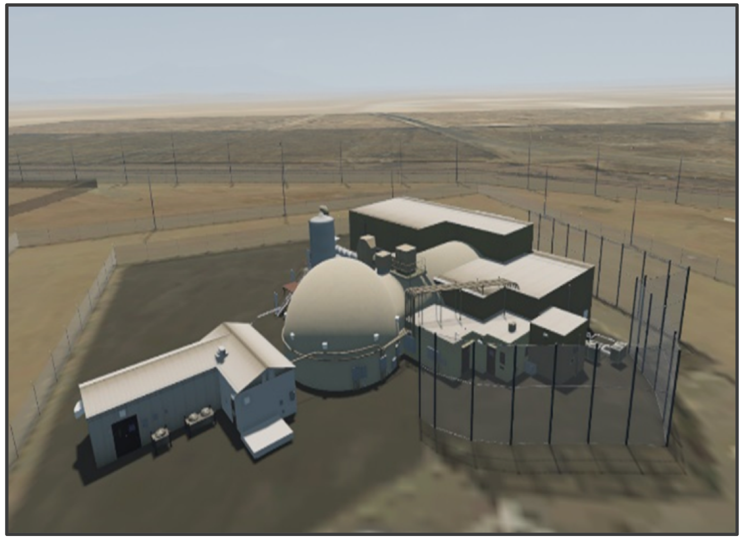
Network Emulation (MiniMega)



MiniMega virtual networking environment developed at Sandia and allows for high fidelity network traffic analysis

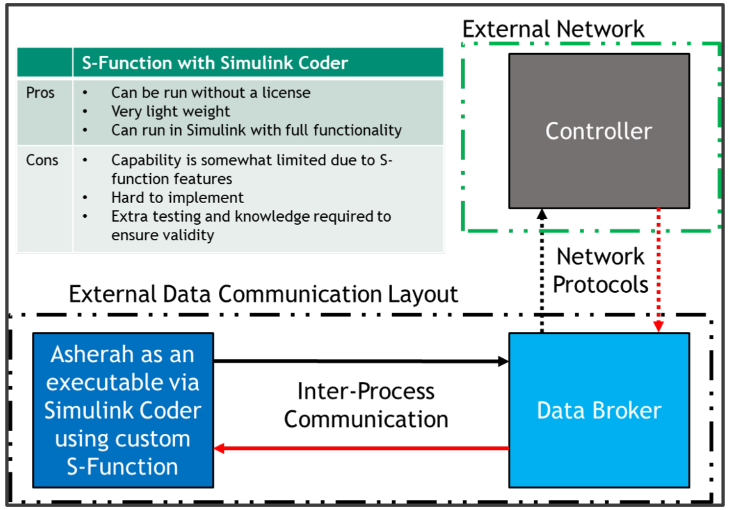
4. Mod/sim experimentation to evaluate analysis techniques

Asherah Simulator



Located within the Mock Reactor

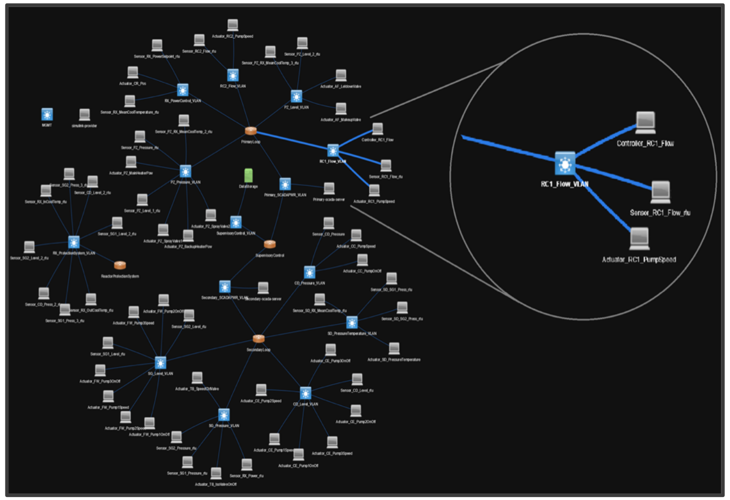
Physics Simulator + Asherah simulator integration



	S-Function with Simulink Coder
Pros	• Can be run without a license • Very light weight • Can run in Simulink with full functionality
Cons	• Capability is somewhat limited due to S-function features • Hard to implement • Extra testing and knowledge required to ensure validity

External Network
Controller
Network Protocols
External Data Communication Layout
Asherah as an executable via Simulink Coder using custom S-Function
Inter-Process Communication
Data Broker

Network Emulation (MiniMega)



MiniMega virtual networking environment developed at Sandia and allows for high fidelity network traffic analysis