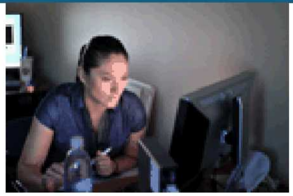
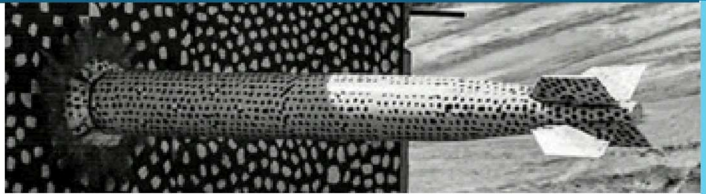
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-14276C

IAEA CRP on Enhancing Incident Response at Nuclear Facilities





Michael Rowland

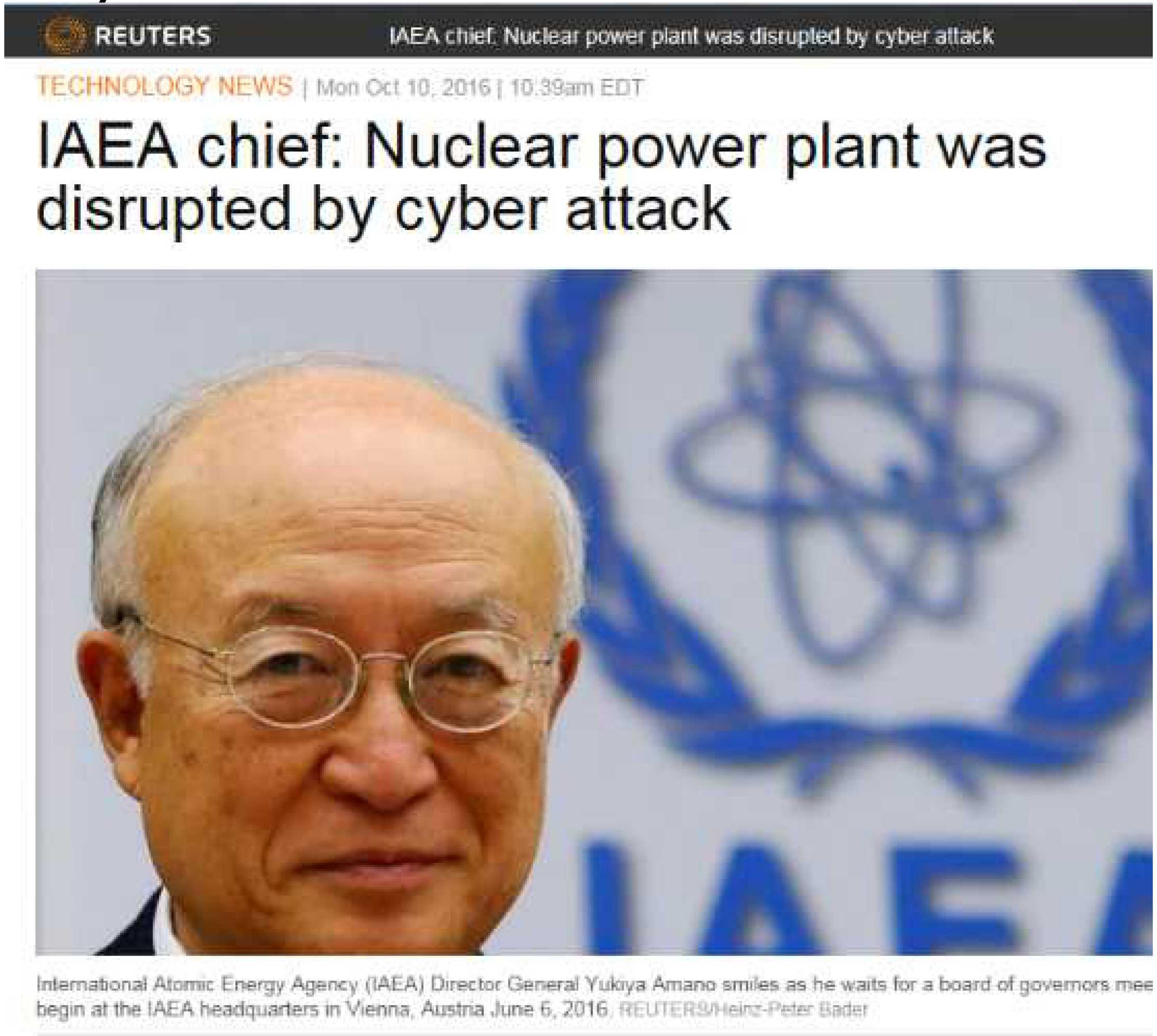
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

IAEA Role in Computer Security

- Nuclear Security Plan 2018-2021

- Directs the IAEA to assist Member States, upon request, in improving computer security capabilities at State organizations and licensees through:

  - Guidance Development
  - Training Courses
  - Information Exchange
  - *Coordinated Research Projects*



REUTERS IAEA chief: Nuclear power plant was disrupted by cyber attack

TECHNOLOGY NEWS | Mon Oct 10, 2016 | 10:39am EDT

IAEA chief: Nuclear power plant was disrupted by cyber attack

International Atomic Energy Agency (IAEA) Director General Yukiya Amano smiles as he waits for a board of governors mee begin at the IAEA headquarters in Vienna, Austria June 6, 2016. REUTERS/Heinz-Peter Bader

Enhancing Computer Security Incident Analysis at Nuclear Facilities

CRP objective is research methods and technologies to improve and support:

- prevention
- detection of, and
- response to,

computer security incidents.

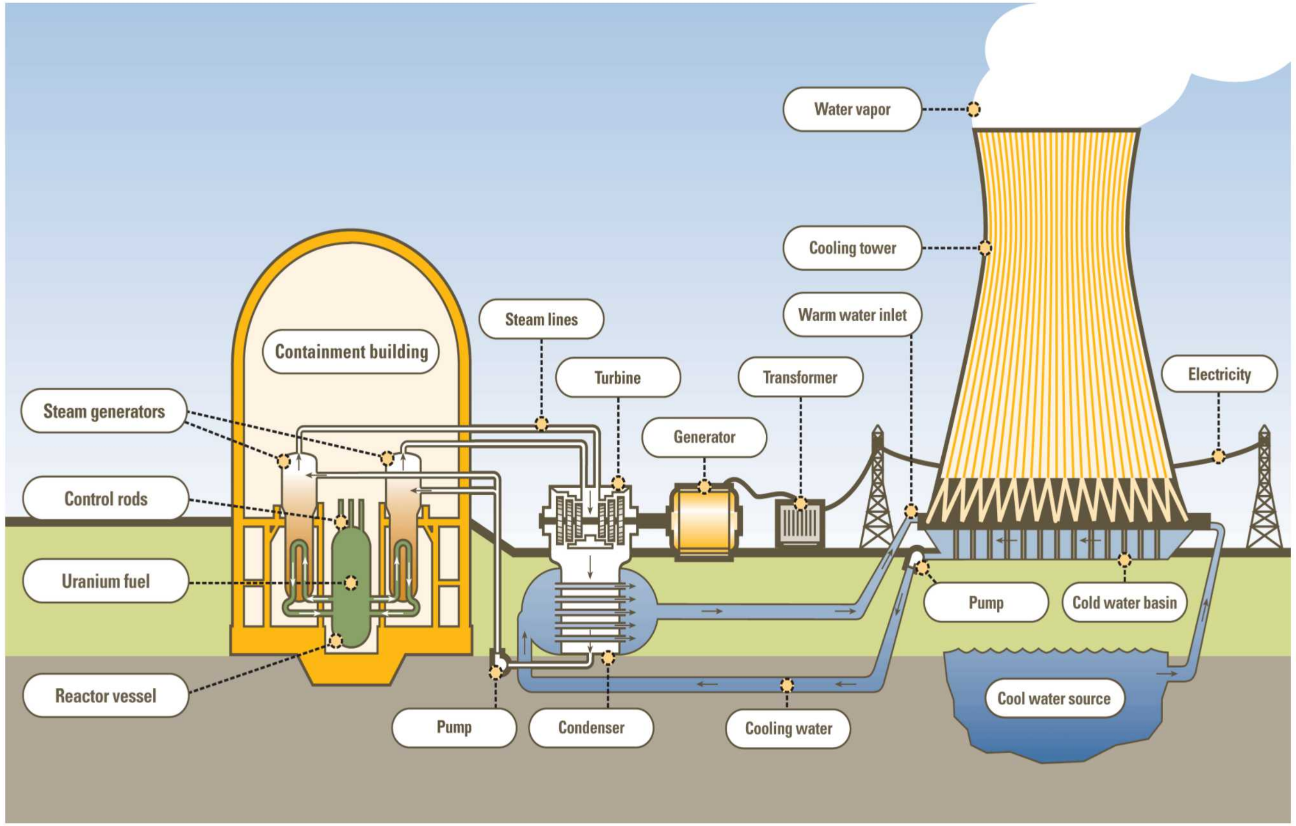


Figure Ref: https://www.nuclear-power.net/nuclear-power-plant/

CRP Overview

1. Developing a **model/simulator** of a hypothetical PWR to allow for research testing of the effects of cyber-attacks

2. **Real control equipment can be interfaced** with the model to determine the consequences of sabotage resulting from the exploitation vulnerabilities resulting in loss of Confidentiality, Integrity, and Availability (CIA).

3. **Threat Model/Scenario** approach to develop of research test cases to mimic good practices in regulatory regimes

4. Informs the development of **Computer Security Measures** to prevent and protect against cyber-attacks on its systems.

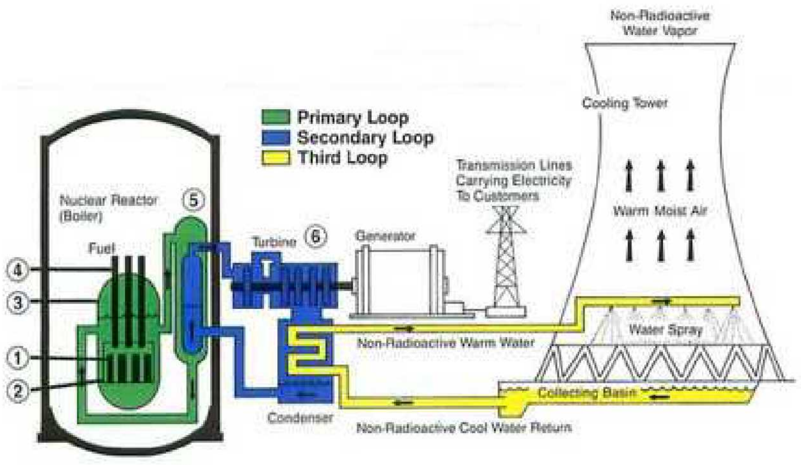


Figure Ref: http://www.co.ottawa.oh.us/ottawacoema/davisbesse.html

CRP Team Roles

- ✓ **Facility/System Builders**: organizations that are building mock-ups/simulators of nuclear systems (7/17).

- ✓ **Capability Providing**: organizations that can provide specific capabilities to others in the CRP that stem from their background expertise (8/17).

- ✓ **Threat Modellers**: organizations that are developing Design Basis Threat, Scenarios, and Threat Tactics, Techniques and Procedures (2/17).

13 Countries / 17 Institutes

Argentina

CNEA
Comisión Nacional de Energía Atómica

Austria

AIT

AREVA

Brazil

Universidade de São Paulo
Scientia Vinces

Canada

Canadian Nuclear Laboratories
Laboratoires Nucléaires Canadiens

Bruce Power

China

Tsinghua University
1911

Germany

Otto von Guericke
Universität
Magdeburg

Ghana

Nuclear Regulatory Authority
Ghana

Hungary

Mexico

ININ

Republic of Korea

KAERI

KINAC
한국원자력통제기술원

Pakistan

Pakistan Atomic Energy Commission

Poland

ncbj

United States

INL

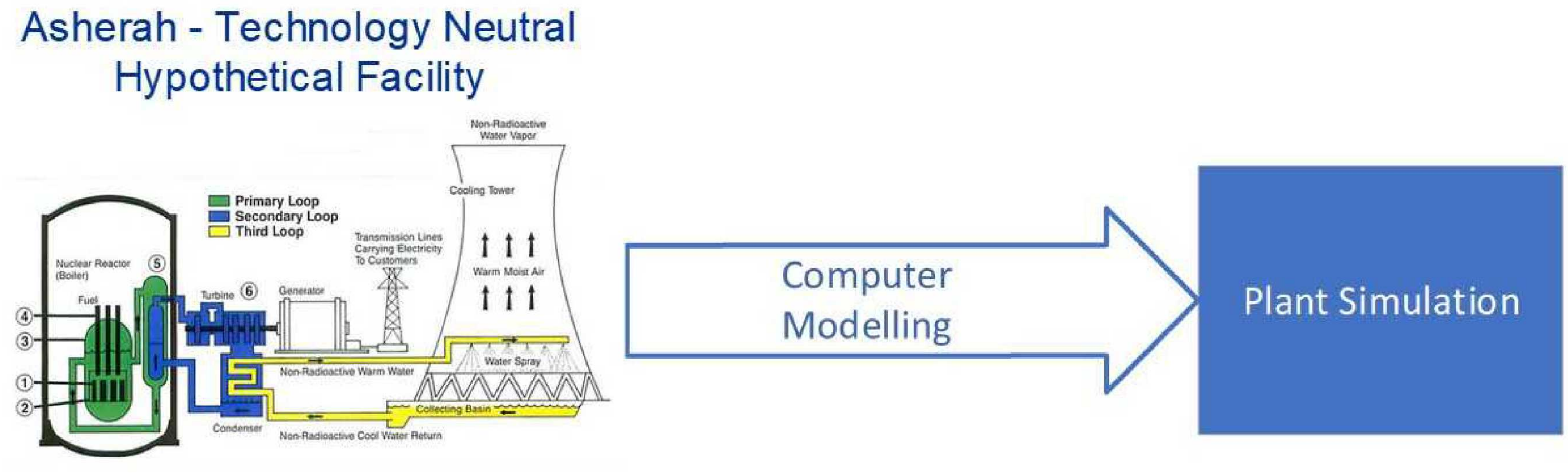
MITRE

UMASS
LOWELL

UL

The University of
Tennessee
Knoxville

Model/Simulator: Asherah NPP Simulator



Asherah - Technology Neutral Hypothetical Facility
Non-Radioactive Water Vapor
Cooling Tower
Primary Loop
Secondary Loop
Third Loop
Transmission Lines Carrying Electricity To Customers
Warm Moist Air
Nuclear Reactor (Boiler)
5
Turbine
6
Generator
Fuel
4
3
1
2
Water Spray
Non-Radioactive Warm Water
Collecting Basin
Condenser
Non-Radioactive Cool Water Return

Computer Modelling

Plant Simulation

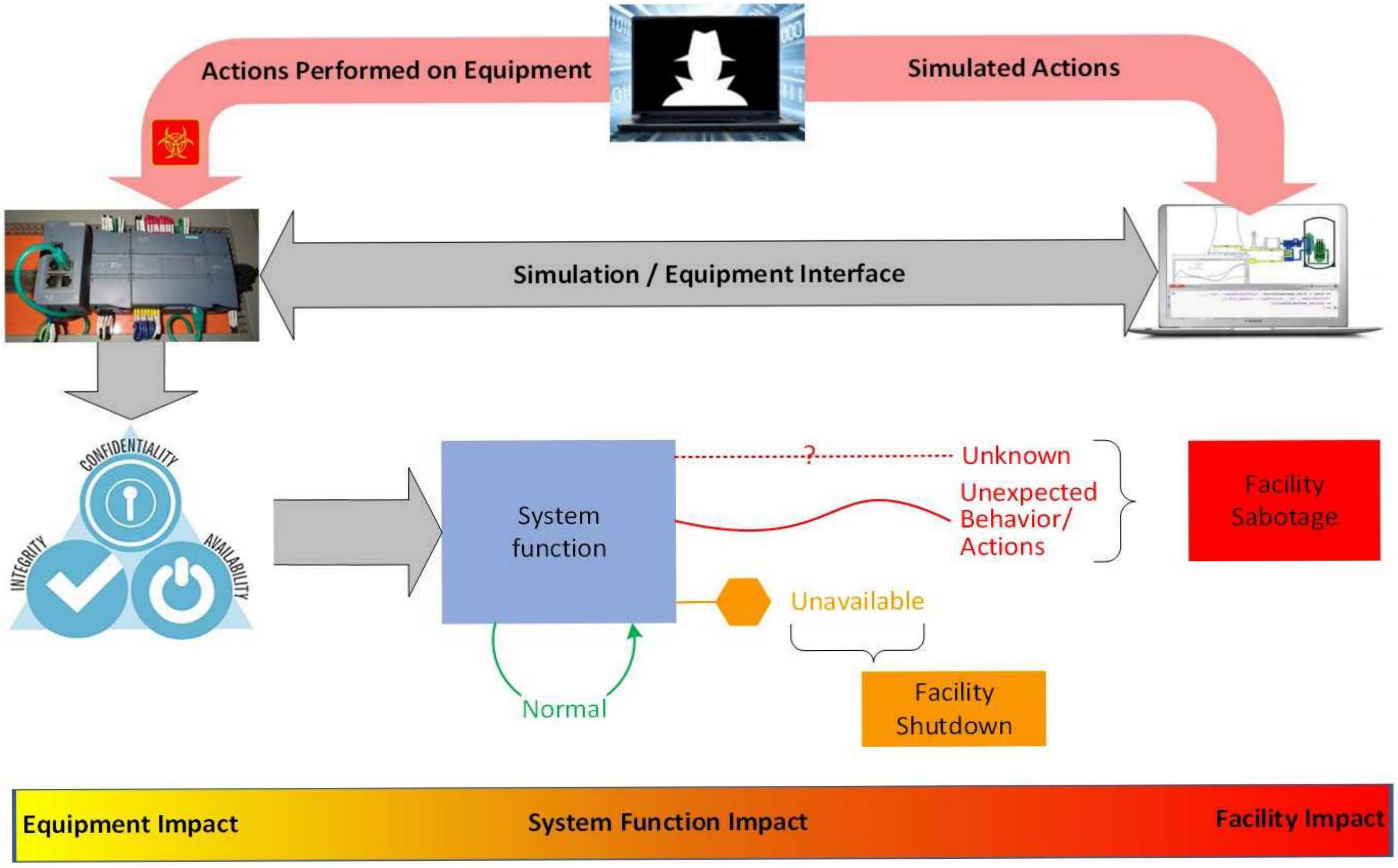
- A hypothetical Pressurized Water Reactor (PWR) named “Asherah” was defined based upon several existing PWR designs.

- Sensitive design elements were removed, and other elements were fabricated.

- The results were combined to produce a technological neutral facility.

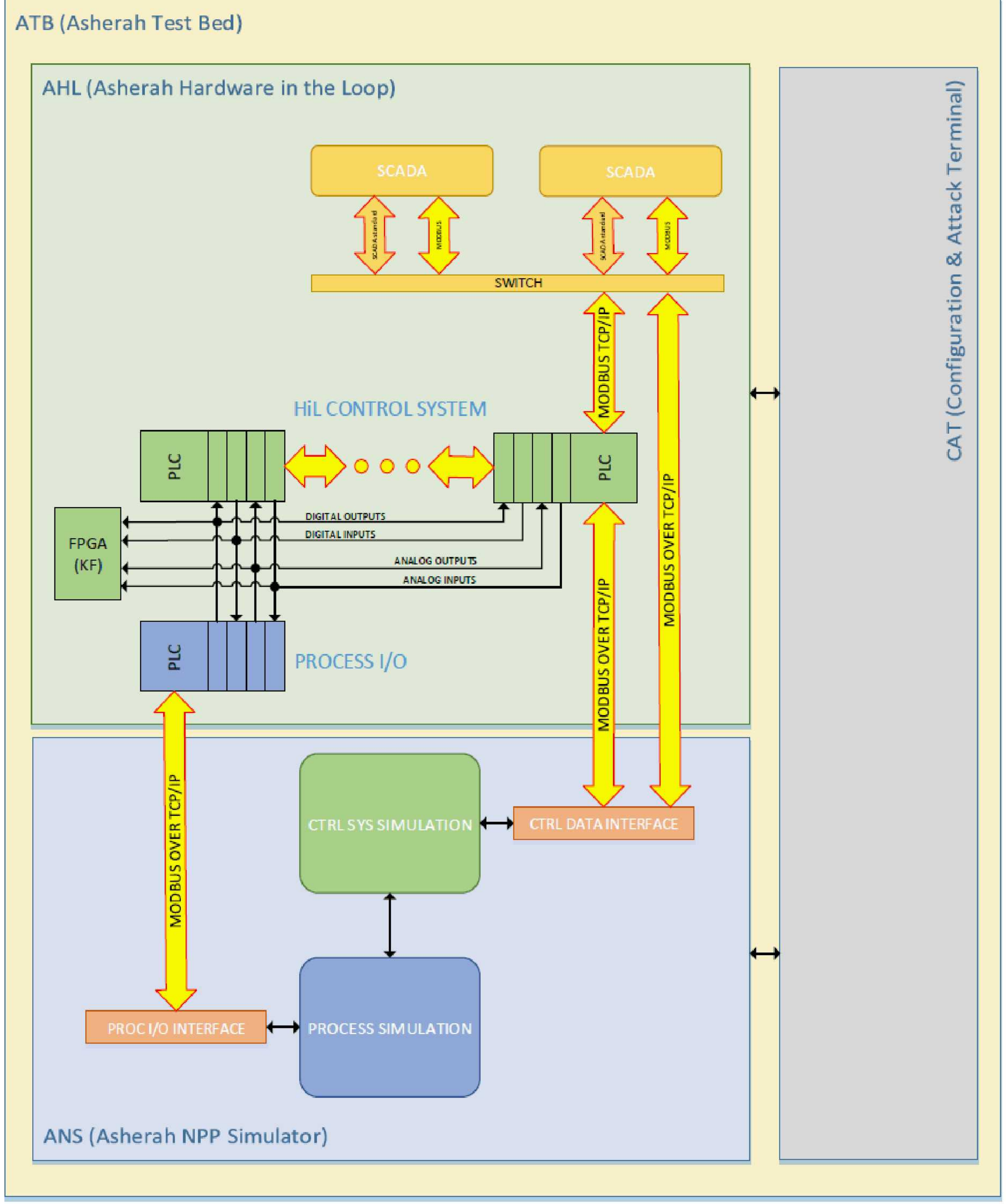
- The model is the heart of a Hardware in the loop (HIL) architecture

Facility, Functional, System Impacts



Asherah Test Bed

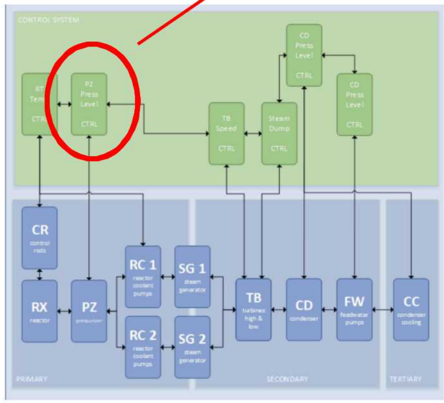
- Matlab/Simulink Model
- Primary, Secondary & Tertiary Cooling Loops
- Steady State & Transient under normal operation
- Controllers & network equipment
- Cyber attack scenarios & system configuration

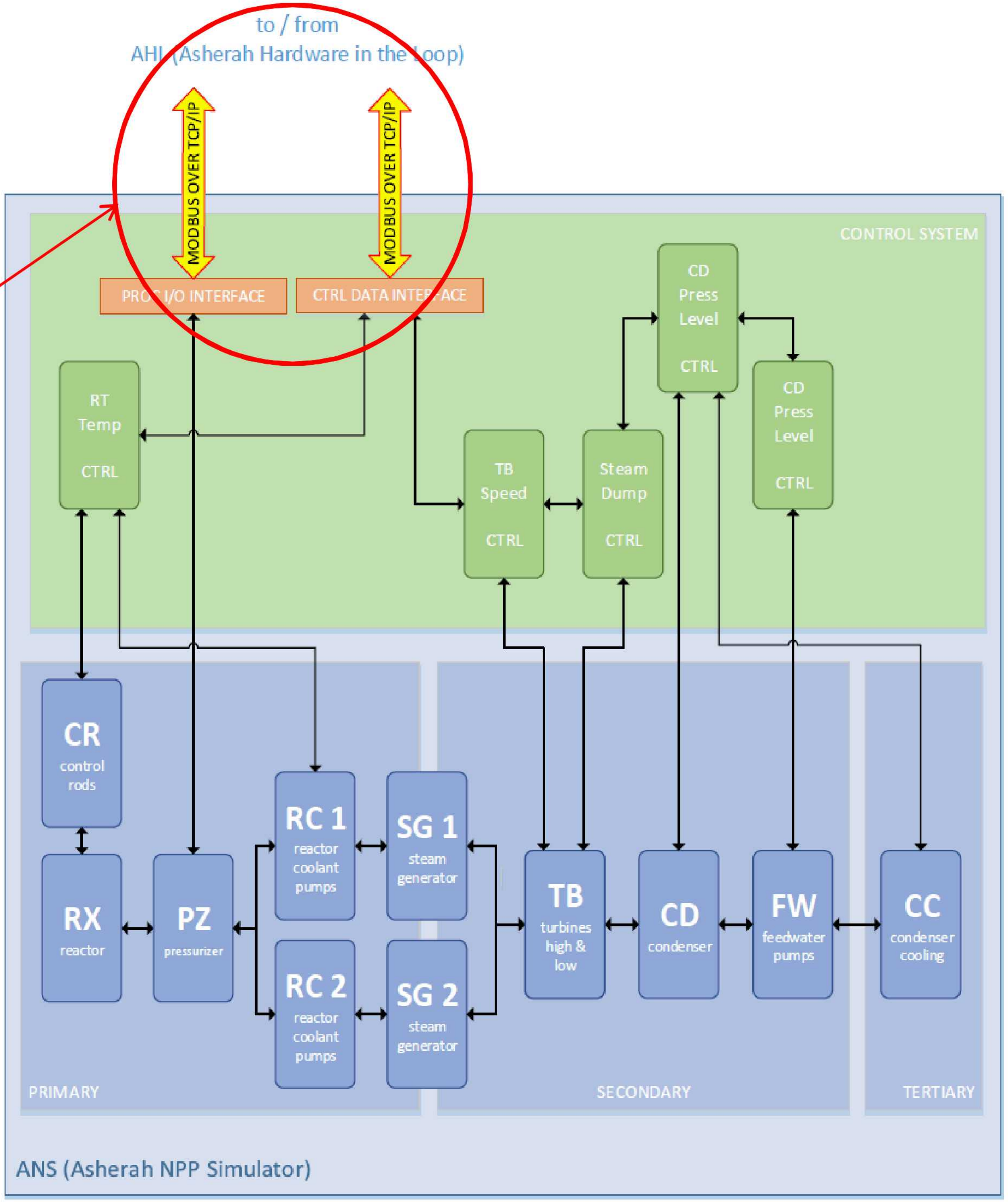


✓ Process I/O Interfaces
Plant Environment and Physical Process Simulation

✓ Control I/O Interfaces
Allows for Hardware in the Loop

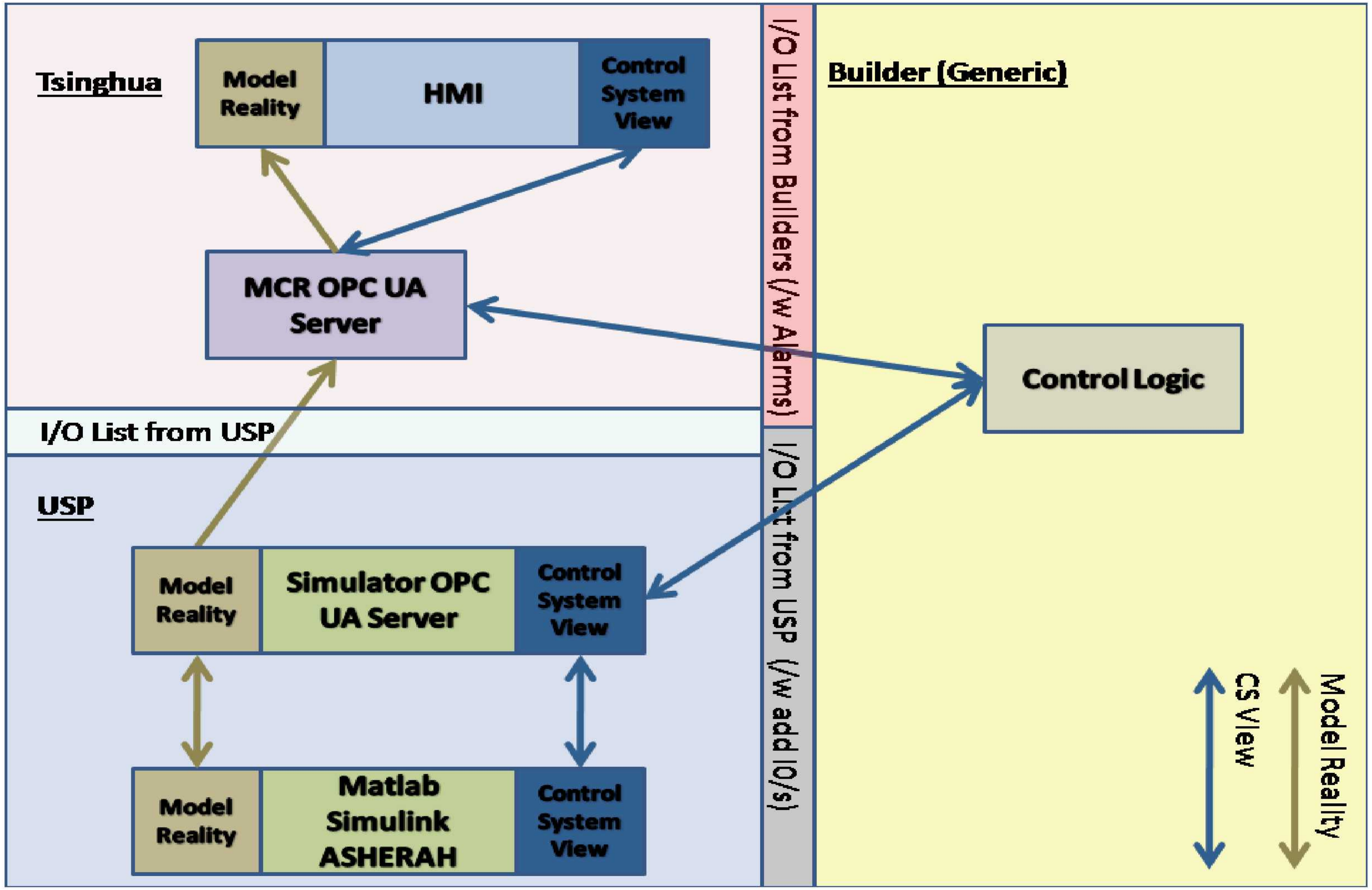
Asherah Test Bed



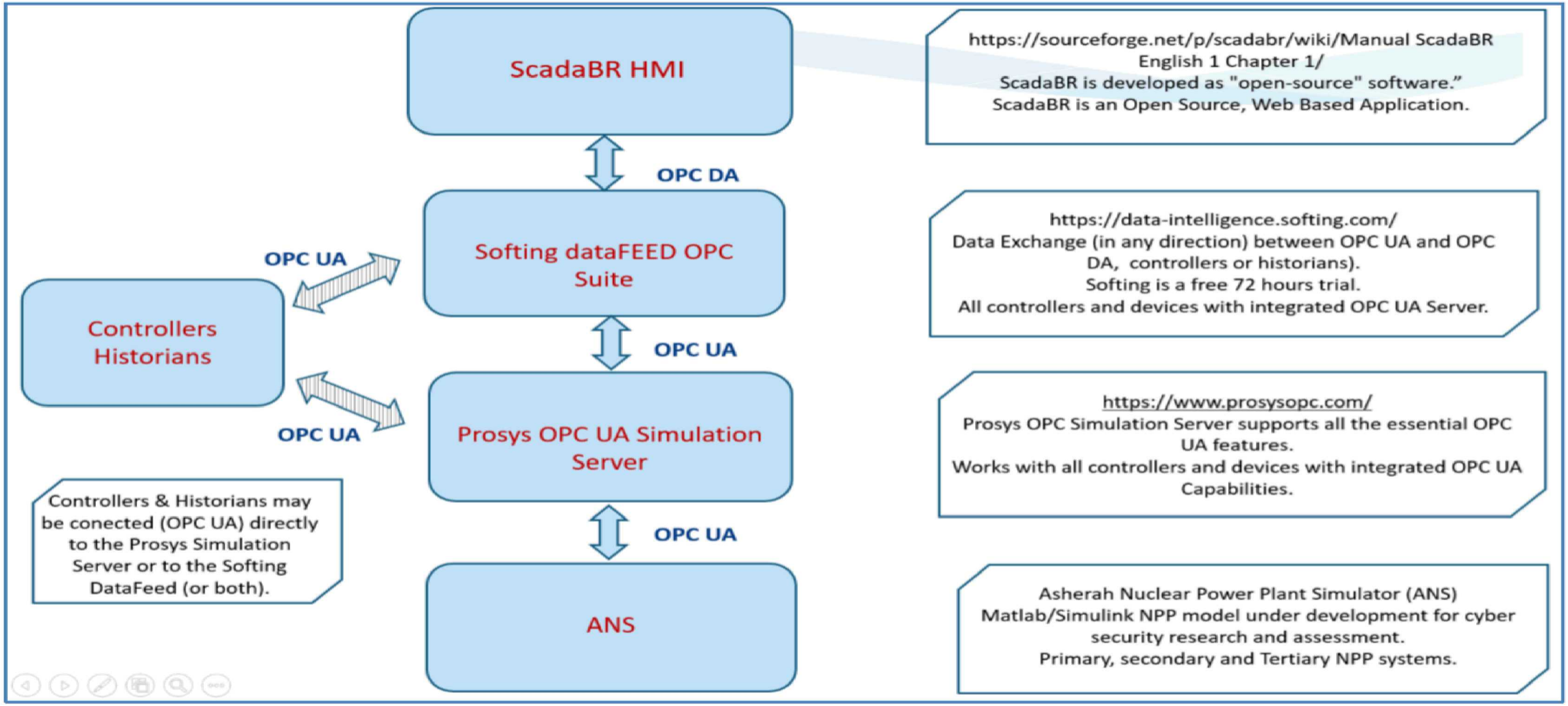


Coordination of Builders

- Expandable Architecture
- Function approach



Test Bed Tools and Connections Scheme



ScadaBR HMI

OPC DA

Softing dataFEED OPC Suite

OPC UA

Controllers Historians

OPC UA

OPC UA

Prosys OPC UA Simulation Server

OPC UA

ANS

https://sourceforge.net/p/scadabr/wiki/Manual ScadaBR English 1 Chapter 1/
ScadaBR is developed as "open-source" software."
ScadaBR is an Open Source, Web Based Application.

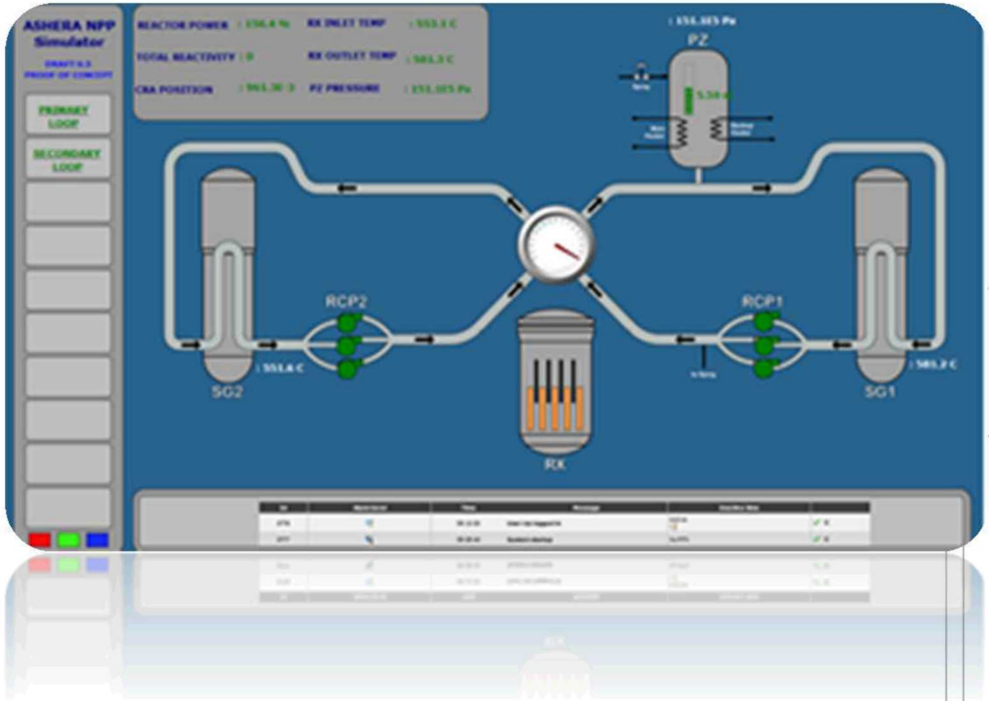
https://data-intelligence.softing.com/
Data Exchange (in any direction) between OPC UA and OPC DA, controllers or historians).
Softing is a free 72 hours trial.
All controllers and devices with integrated OPC UA Server.

https://www.prosysopc.com/
Prosys OPC Simulation Server supports all the essential OPC UA features.
Works with all controllers and devices with integrated OPC UA Capabilities.

Asherah Nuclear Power Plant Simulator (ANS)
Matlab/Simulink NPP model under development for cyber security research and assessment.
Primary, secondary and Tertiary NPP systems.

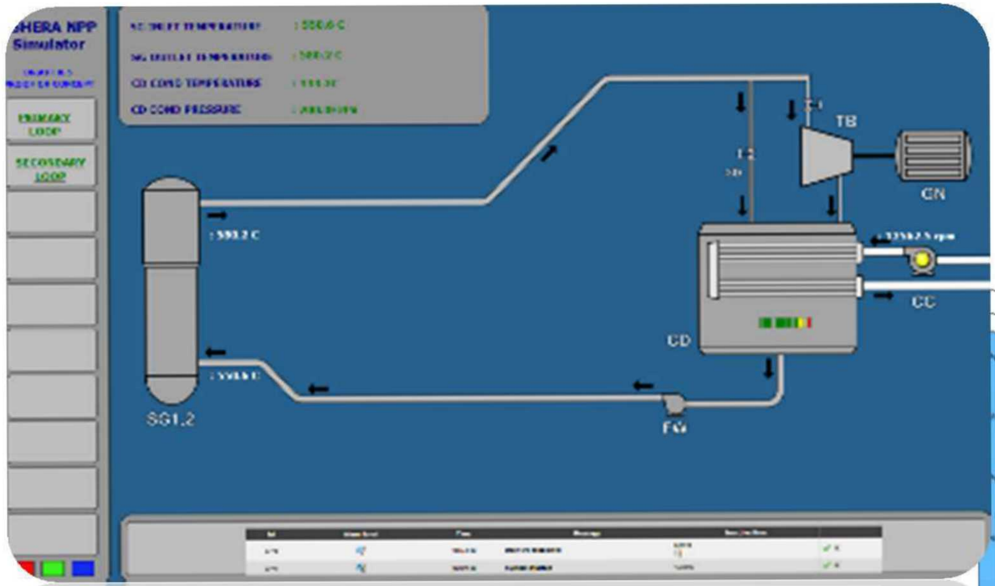
Controllers & Historians may be conected (OPC UA) directly to the Prosys Simulation Server or to the Softing DataFeed (or both).

Human Machine Interface - Primary

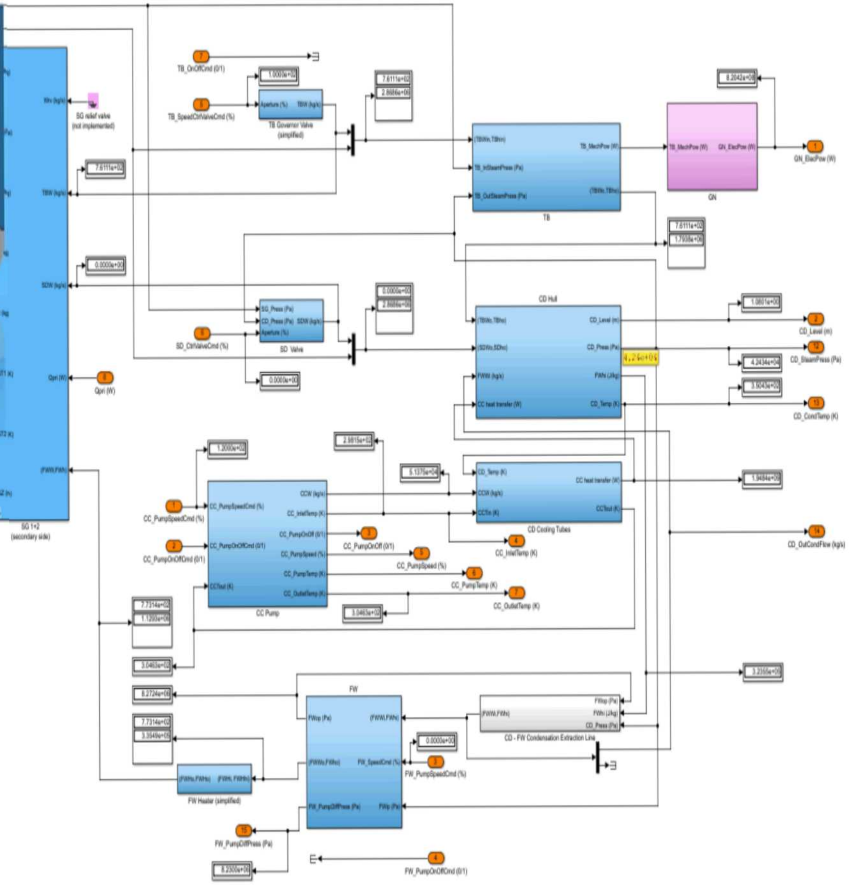


Control and Process I/O

Human Machine Interface - Secondary

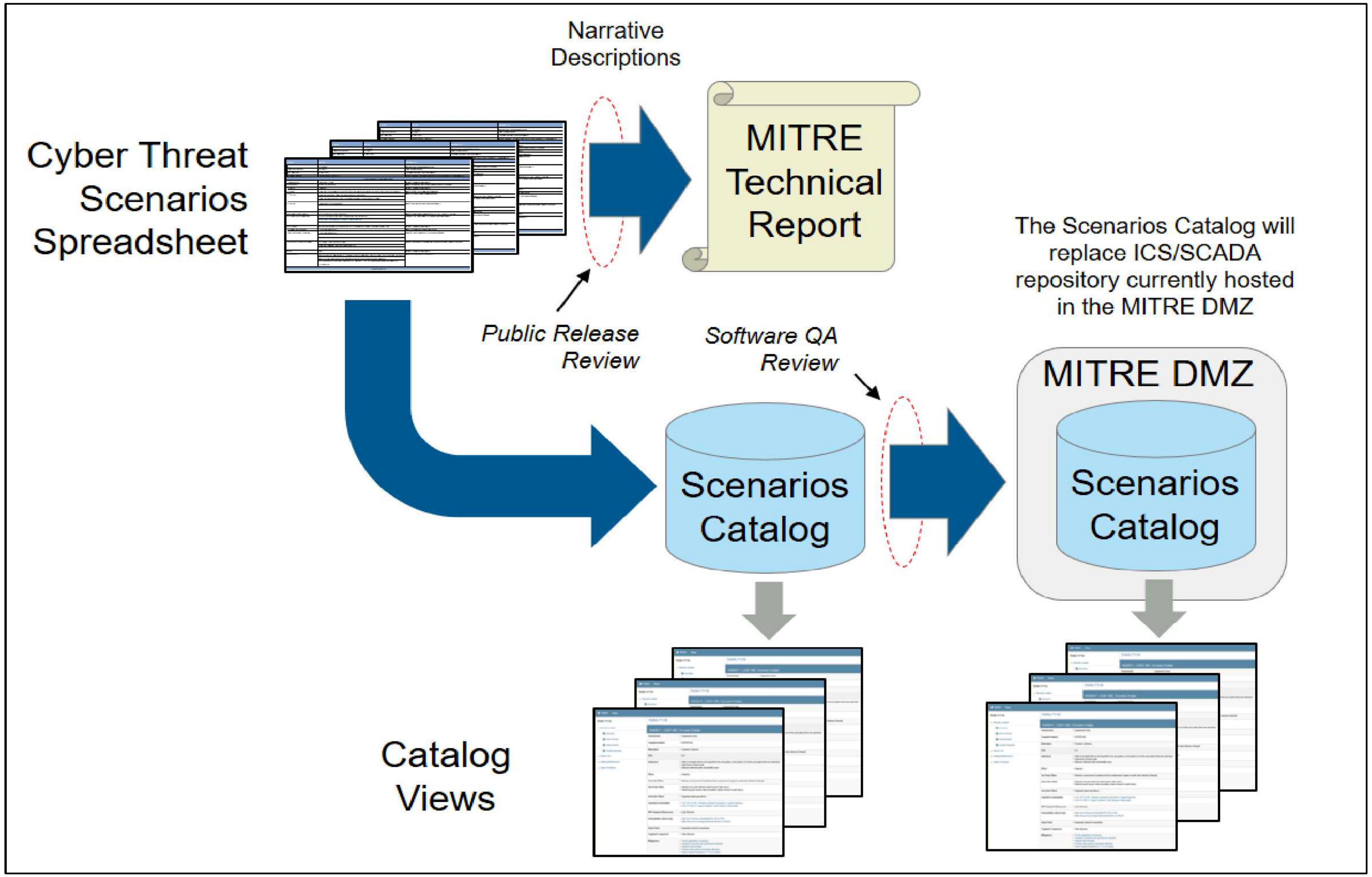


Control and Process I/O

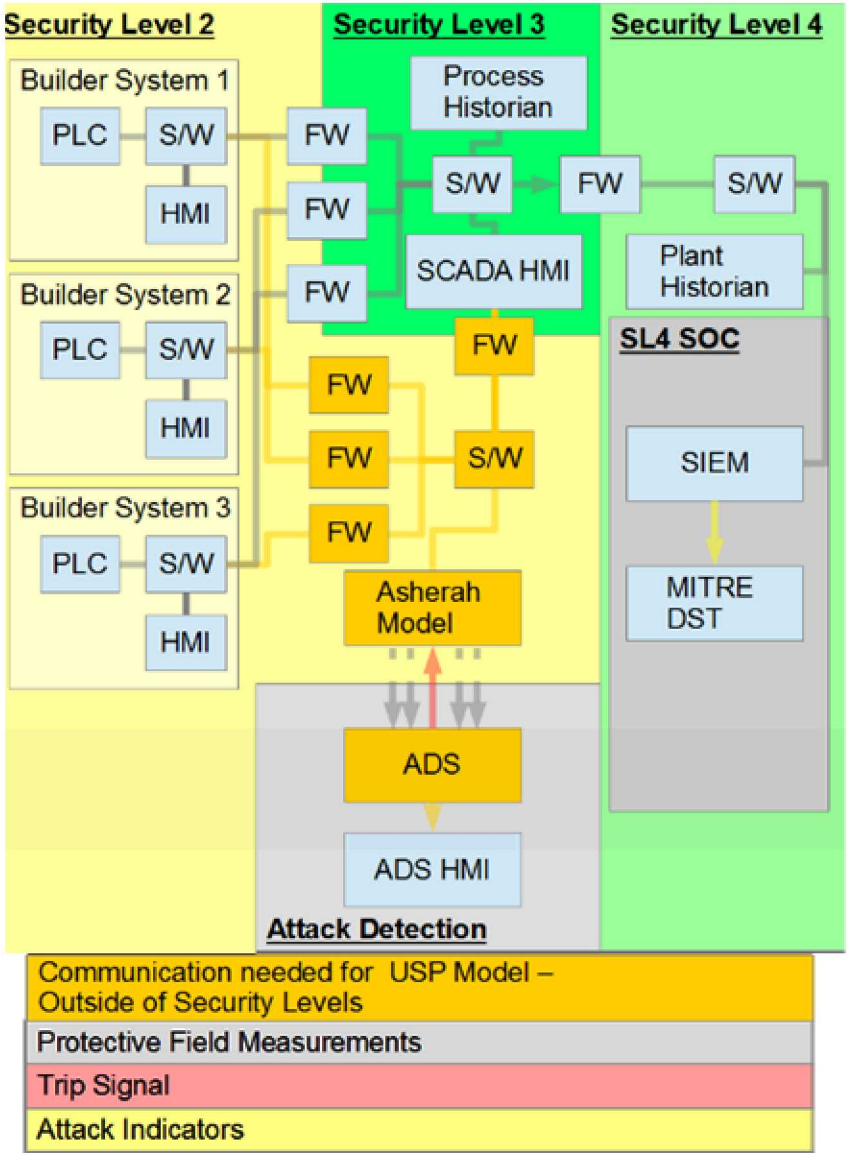


Threat Modelers Activities

- Attack scenarios
- Compromise of Functions



CPOs Activities



CPOs identify potential:

- Graded Approach
- Defense in Depth
- Policy and Procedures
- Measures and Controls

International Conference on Nuclear Security
Key Deadline and Dates

Release announcement	31 Jan 2019
Submission of synopses	31 May 2019
Submission of Forms A, B or C	14 Jun 2019
Notification of acceptance to authors	30 Sep 2019
Submission of full papers	29 Nov 2019
Submission of presentations	20 Dec 2019
ICONS 2020	**10-14 Feb 2020**

Summary

- System Builders & Capability Providers Organizations have been successful developing mock-ups of nuclear systems.
- Threat Modellers are providing cyber threat scenarios for System Builders and Capability Providers organizations.
- Cyber security techniques have been developed (fuzzing, Kalman Filter, Anomaly Detection) and applied to the test beds.
- Key IAEA role on the coordination of all activities and all institutes.
- Solid information sharing network among all participants.
- All tools developed and documents produced under the CRP J02008 will be available for Member States and may be used for training purposes.

Thank you!