Nuclear Power Plant in a Box

Asherah

R. Altschaffel[1]
T. Holczer[2]
R. A. Busqium e Silva[3]
J. Li[4]
P. Gyorgy[2]
M. Hildebrandt[1]
M. Hewes[5]

[1]Otto-von-Guericke University, Magdeburg, Germany
[2] BME Crysys, Budapest, Hungary
[3] Brazilian Government, Sao Paulo, Brazil
[4] Tsinghua University, Beijing, China
[5] IAEA

Outline

- Introduction
- Why to simulate an NPP in the first place?
- Structure of NPPs from a Computer Scientists Point of View
- Simulating …
  - The Physical Process
  - The Operational Technology
  - The Main Control Room HMI
  - The Information Technology
- Binding everything together
- Use in …
  - Training
  - Research

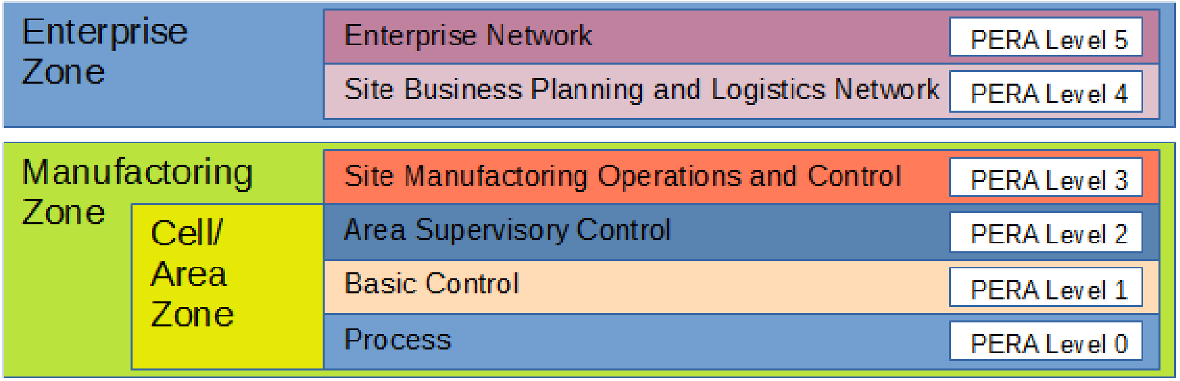
Why to simulate an NPP in the first place?

- A NPP is highly complex
  - Operators require training to increase safety
  - Research into better safety measures might also increase safety
- NPP have also become targets of cyber-attackers (=attacks performed by using the computing technology inside NPPs)
  - Cyber-Security training is also required
  - Research into better protection against cyber-attacks might also increase security, and therefore safety

- Training is performed using Mockups or simulators
  - Mockups are expensive
  - Simulators are geared towards showing the physical process, not the computing units (and are hence bad to train against cyber-attacks)
- Need for a simulator which includes realistic behavior of the computing technology

Structure of NPPs from a Computer Scientists View Point

- A NPP is …
  - A physical process
  - Controlled by computing units (operational technology, OT)
  - Operated by operators using Human-machine-interfaces (HMI)
  - Attached to a business system (information technology, IT)
- This is known as an Industrial Control System



Enterprise Zone		Enterprise Network	PERA Level 5
		Site Business Planning and Logistics Network	PERA Level 4
Manufactoring Zone		Site Manufactoring Operations and Control	PERA Level 3
	Cell/ Area Zone	Area Supervisory Control	PERA Level 2
		Basic Control	PERA Level 1
		Process	PERA Level 0

Control Hierarchy of ICS according to WILLIAMS, T. J., " The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation", Research Triangle Park, NC: Instrument Society of America, 1992 – taken from Altschaffel et al, “Nuclear Power Plant in a Box”, ICONS 2020

Simulating the Physical Process 1/2

- The physical process in the NPP is the foundation for all other components
  - controlled by the OT, operated via HMI, informs IT
- Requirements:
  - Needs to provide information about the physical process to other components
  - React on control inputs
  - Must be modular to swap out parts
- Forms the core of Asherah => Asherah Nuclear Simulator (ANS)

Simulating the Physical Process 2/2

- We use a Matlab model for the simulation of the physical process
  - 2,772 MWt pressurized water reactor
  - includes main plant subsystems & some equipment important for safety or security of the primary, secondary and tertiary cycle
    - Reactor Core with Control Rods
    - Pressurizer with proportional and Backup Heaters and Sprays
    - Reactor Coolant Pumps
    - Auxiliary Fluid Tank
    - U-tube Steam Generator (Primary and Secondary sides)
    - Turbines
    - Electric Generator Condenser
    - Condensate Extraction System
    - Condenser Cooling Pumps
    - Feedwater System
    - Reheaters

Simulating the Operational Technology 1/3

- Operational Technology controls the physical process by performing Instrumentation and Control (I&C) and consists of:

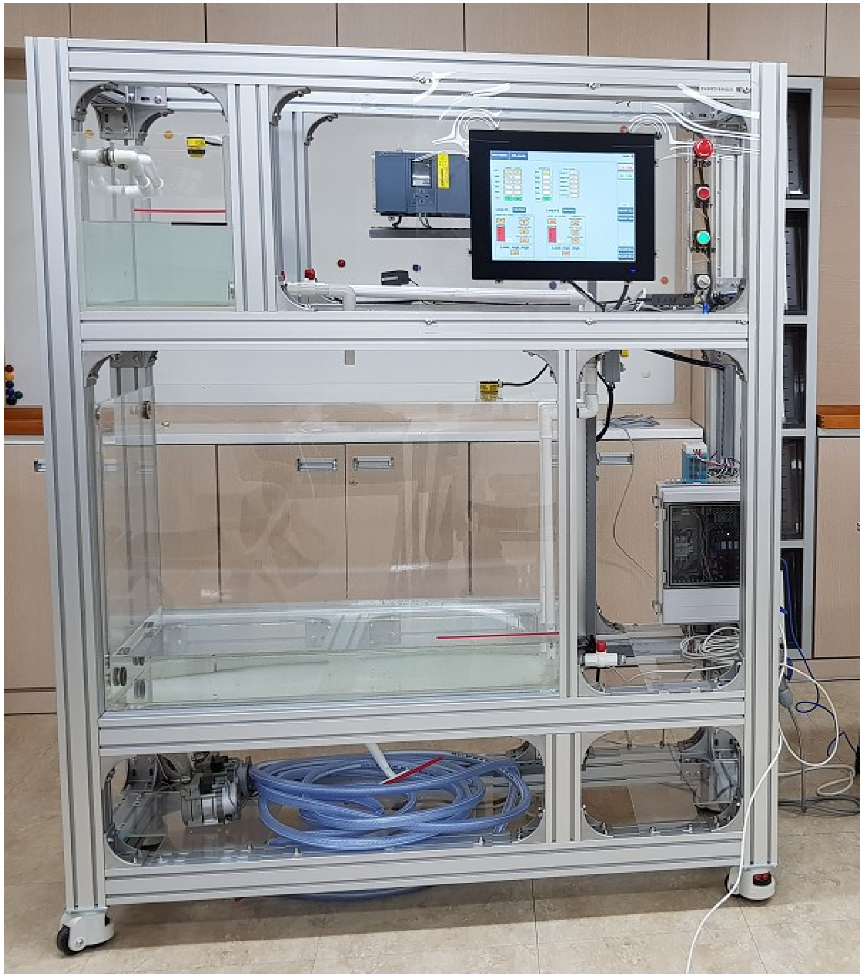
– Sensors	collecting information about the physical process
– Computing units	computing the sensor input (and control signals)
– Actors	influencing the physical process
– Communication	to tie everything together

- All these components could be the target of cyber-attacks and need to be included in a simulator aimed at researching and training for cyber-attacks

- Our approach is to swap out parts of the ANS model for real hardware

Simulating the Operational Technology 2/3

- To include physical subsystems like …

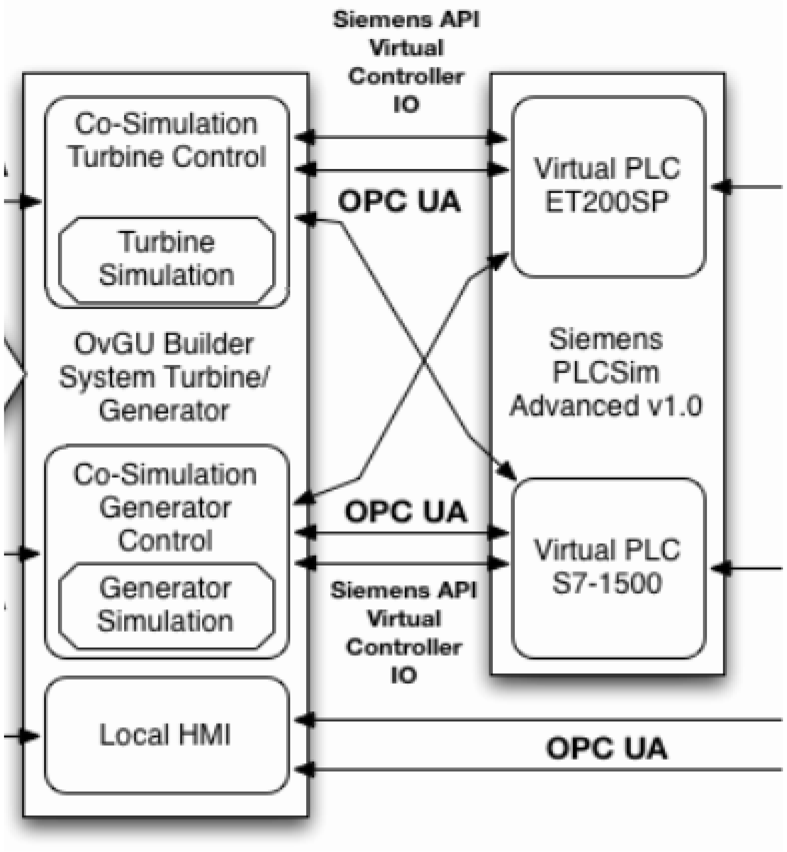


Physical Demonstrator

- Real physical process
- Real Sensors
- Real Computing Units
- Real Actors
- Local HMI
- Communicates with ANS and Main Control Room HMI

Simulating the Operational Technology 3/3

- Or completely virtualized subsystems like …

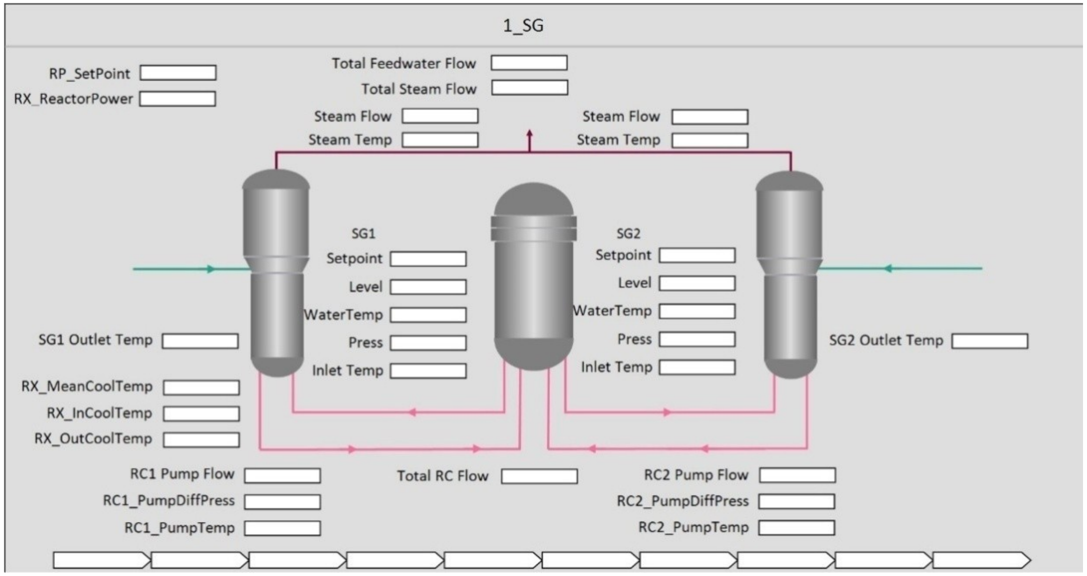

Siemens API Virtual Controller IO
Co-Simulation Turbine Control
Turbine Simulation
OPC UA
Virtual PLC ET200SP
OvGU Builder System Turbine/ Generator
Siemens PLCSim Advanced v1.0
Co-Simulation Generator Control
Generator Simulation
OPC UA
Virtual PLC S7-1500
Siemens API Virtual Controller IO
Local HMI
OPC UA

- (Co-)Simulation of physical process
- Virtual Sensors
- Real Computing Unit Firmware running in Virtual PLCs
- Virtual Actors
- Local HMI
- Communicates with ANS and Main Control Room HMI

Virtualized Subsystem, taken from Altschaffel, R., Hildebrandt, M., Dittmann, J., "A Simulated Steam Turbine Geneator Subsystem for Research and Training“, ICONS 2020

Simulating the Main Control Room HMI

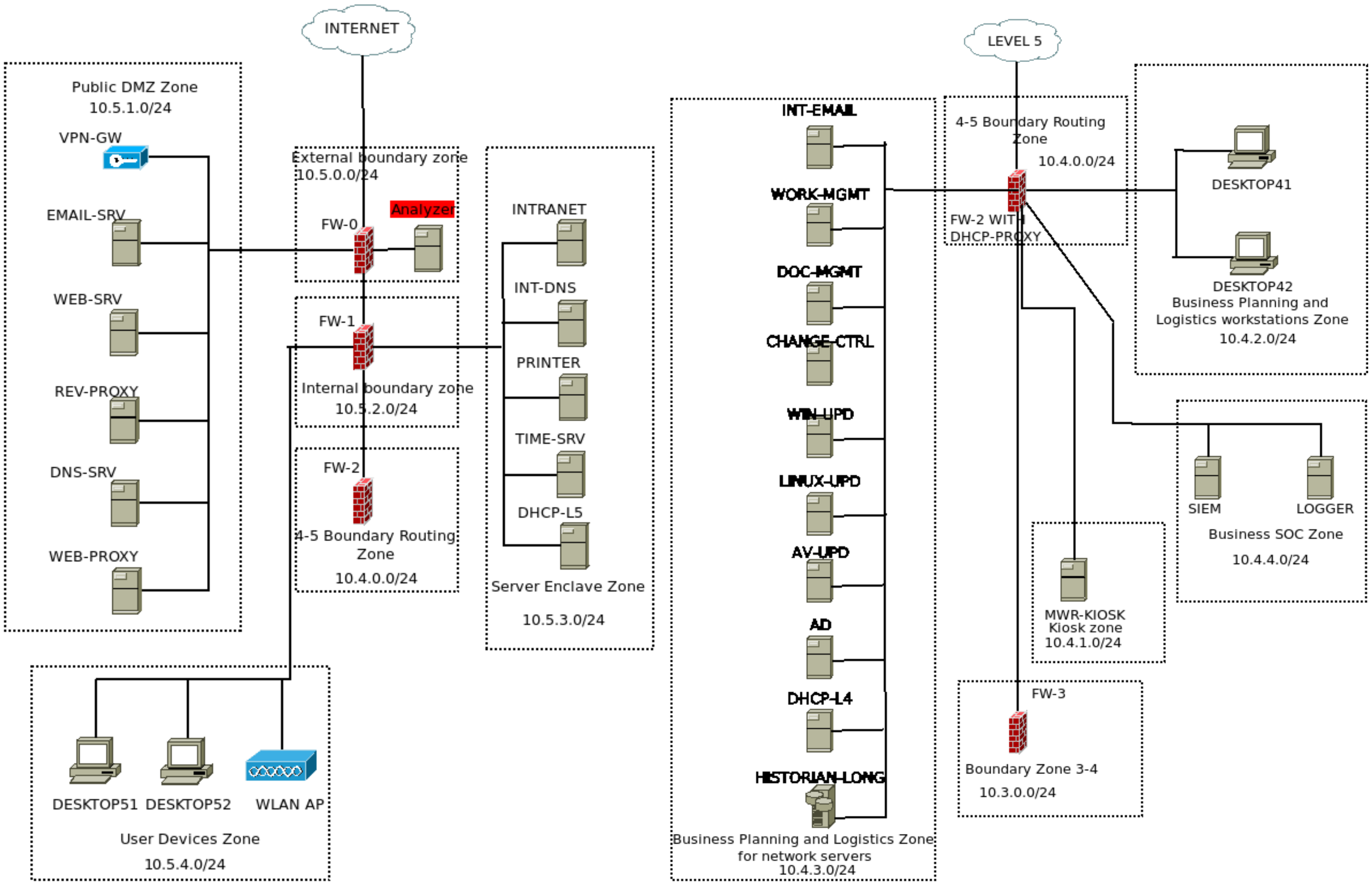
- In the Main Control Room operators supervise the physical process
- Requirements:
  - Show information about the physical process
  - Give commands to control the physical process



HMI View taken from Altschaffel et al, “Nuclear Power Plant in a Box”, ICONS 2020

- Done with SCADA BR
- Includes detail views for various subsystems

Simulating the Information Technology 2/2



IT Network taken from Altschaffel et al, “Nuclear Power Plant in a Box”, ICONS 2020

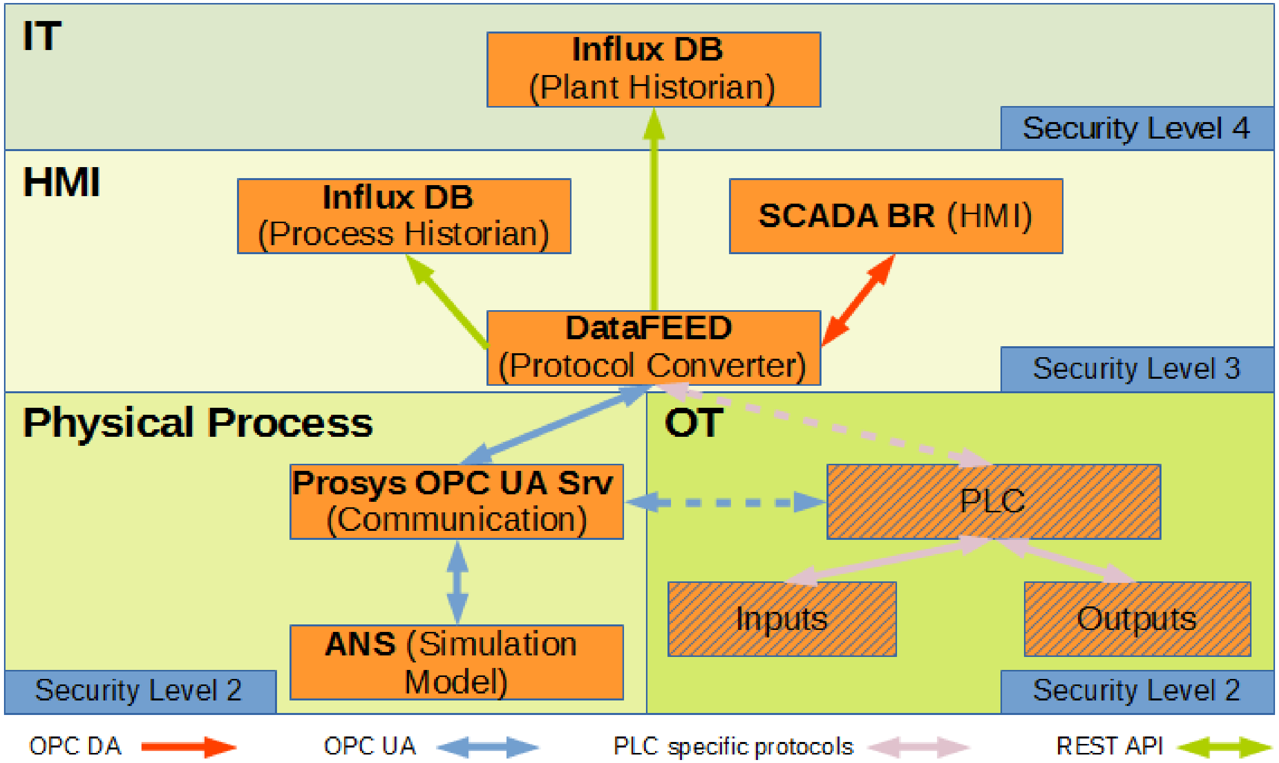
Simulating the Information Technology 1/2

- An NPP also contains a business and management network
- This network might be used as an attack venue (or as an attack target) during cyber-attacks

- Simulation using ANSIBLE and virtualized machines
  - Script for various IT components (Servers, Clients, Infrastructure)
  - Easy to deploy a complete network with functioning components
  - Historians, Work Management systems, Email, etc …

Binding Everything Together

- Communication between these components is done using realistic communication protocols and architectures based on NST047



Overall Communication Architecture taken from Altschaffel et al, “Nuclear Power Plant in a Box”, ICONS 2020

NST047
IAEA, Nuclear Security Series No. 17 Computer Security at Nuclear Facilities, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

Use in Training

- Asherah have been used for training in the ITC in Korea
- We used Asherah for a complex attack scenario
  - Involving attacks on IT and OT
- Trainees were able to …
  - see the impact of the attack
  - Investigate the attack based on realistic captures from IT and OT
  - React on the attack by giving guidance to the operators and decision makers

Use in Research

- Asherah is used in Research

- New approaches for anomaly detection
  - Requires realistic data to learn “normal behavior”
  - Requires the possibility to test the models
- Research into ICS forensics
  - Asherah helps to create realistic data from attacks/errors
  - Allows for the an understanding of additional required measures

Summary and Outlook

- Asherah is an easy to deploy simulator which focuses on a realistic behavior of plant computing components, including
  - Physical process
  - Operational Technology
  - Control Room HMI
  - Information Technology
- Can be used for Research and Training concerning cyber attacks

- Open points:
  - Increase performance
  - Increase variety of subsystems, computing units, protocols
  - Reduce dependency to commercial software