DEVELOPMENT OF THE ASHERAH NUCLEAR POWER PLANT SIMULATOR FOR CYBER SECURITY ASSESSMENT

R. A. BUSQUIM E SILVA
Polytechnic School of University of Sao Paulo - Sao Paulo, SP, Brazil
Massachusetts Institute of Technology – Cambridge, MA, USA
Navy Technological Center in Sao Paulo - Sao Paulo, SP, Brazil
Email: busquim@alum.mit.edu

K. SHIRVAN
Massachusetts Institute of Technology – Cambridge, MA, USA

J. R. C. PIQUEIRA
Polytechnic School of University of Sao Paulo - Sao Paulo, SP, Brazil

R. P. MARQUES
Polytechnic School of University of Sao Paulo - Sao Paulo, SP, Brazil

Abstract

This work presents a nuclear power plant simulator developed specifically for performing cyber security assessment. The Asherah Nuclear Power Plant Simulator reproduces the dynamic behavior of a two-loop 2,772 MWt pressurized water reactor including primary, secondary and tertiary loops as well as the control system. It is implemented in the MATLAB/SIMULINK platform with the use of relatively simple dynamic models for all systems and equipment. The main ANS feature is its capability for hardware-in-the-loop integration with test beds including advanced instrumentation and control, operational technology and conventional information technology device integration. ANS uses include computer security research and assessment, security measures development, information sharing and training.

1. INTRODUCTION

This work presents the development of a Nuclear Power Plant (NPP) Simulator developed specifically for performing cyber security assessments, The Asherah NPP Simulator (ANS) is based on a Pressurized Water Reactor (PWR) that borrows several subsystems from the well-known 2,772 MWt Babcock & Wilcox (B&W) design, subject of several studies published after the Three Mile Island (TMI) Unit 1 accident [1,2].

The simulator is implemented in the Matlab/Simulink environment and is capable of simulating all main plant subsystems in the primary, secondary and tertiary cycles as well as selected parts of the network infrastructure, including communication protocols and the control system.

It is also designed for hardware-in-the-loop integration with test beds including advanced Operational Technology (OT) and Information Technology (IT) devices integration.

Section 2 presents the background for the simulator main concept, including the basic guidelines and requirements for its development. Section 3 presents the reference plant and Section 4 discusses different aspects of the simulator. Section 5 presents examples of simulator integration in different testbeds. Section 6 concludes the work with comments and future development.

2. BACKGROUND AND REQUIREMENTS

In 2016 the International Atomic Energy Agency (IAEA) commenced a new Coordinated Research Project (CRP) entitled *Enhancing Computer Security Incident Response Analysis at Nuclear Facilities*. This was the first coordinated project proposed by the agency on the subject of computer security [3]. The project eventually counted with the official participation of seventeen research institutes from thirteen countries, among them the University of São Paulo in Brazil (USP). One of the project goals was the creation of a hypothetical facility with a PWR NPP named *Asherah*, from a goddess of the Canaanite pantheon (previously another hypothetical research facility developed by the IAEA and other institutions was named after Shapash, another Canaanite goddess). The Asherah NPP would function as a reference plant for the security studies.

During the project development, USP identified the need for an Asherah NPP simulator (ANS), especially with respect to the following aspects.

- Assessment of the first physical consequences to the plant provoked by functional discrepancies in the control system, that might be explicitly caused by a computational attack or be the direct consequence of one.
  For example, a compromised level controller in a steam generator would immediately affect its level. The assessment of how fast and how intense this disturbance would be is a very difficult task without the aid of a simulation tool.
- Assessment of the progression of such disturbances.
  For example, a disturbance in the steam generator level would affect its internal pressure and the heat exchange with the primary loop.
- Coupling effects of a compromised control subsystem on other controllers.
  For example, the above-mentioned steam generator level controller fault would also affect the steam generator pressure and subsequently provoke an automatic response from the steam generator pressure controller.
- Further consequences.
  For example, an unintended plant shutdown due to deficient heat extraction from the reactor.

Even with a very accurate reproduction of a compromised control system, these coupling dynamic effects would be very difficult to infer without resorting to a plant and control system simulation.

Due to the international cooperative context of the CRP and its teams, the research itself and the institutional role of the IAEA, the simulator should respect the following guidelines and requirements.

- Accuracy. The simulator should be accurate enough to attend the teams needs listed above without being excessively complex.
- Real-Time. The simulator should be capable of real-time, and preferably much faster than real-time, simulation on conventional computing platforms.
- Simplicity. The simulator code should be simple enough to be tweaked by the teams whenever needed, preferably without a steep learning curve. Also, the physics principles employed should be simple enough as to be understandable by personnel not specialized in Nuclear Engineering or Physics.
- Flexibility and modularity. The simulator should be flexible enough to be deployed in different contexts and integrated in diverse testbeds, accordingly to each team needs. Functional and physical units in a typical plant also should be associated with simulation modules as to facilitate its integration.
- Network & equipment integration. The simulator should be readily capable of integration with physical and realistically simulated controllers and other network equipment and communication protocols, so as to be able to support security studies and simulated attacks.
- Non-proprietary. No proprietary, restricted or confidential information or data should be used in the simulator design, so as to allow the code to be freely distributable among teams in different countries.
- Technological neutrality. The simulator should not reproduce any real facility, so as to prevent its use by malicious agents for development or training.

3. ASHERAH NUCLEAR POWER PLANT

Asherah NPP is a hypothetical facility with a 2,772 MWt two-loop PWR, loosely based on the TMI Unit 1 B&W design. The choice for this design was made basically due to the large availability of public information and studies produced after the TMI Accident. Additionally, a two-loop plant was deemed to be more convenient for its simplicity with relation to plants with more loops, while still retaining most technical characteristics that enable the proposed security analysis (i.e. similar control systems, etc.).

There is also available a very accurate PARCS/RELAP-based simulator for this plant [4,5] that was used as reference for the development and fine tuning of the new simulation model.

Main systems and equipment include for the primary cycle: control rods (CR), reactor core (RX), pressurizer (PZ), reactor coolant pumps (RCP1, RCP2), auxiliary fluid tank (AF) and u-tube steam generator (SG1, SG2 - primary side). For the secondary cycle: u-tube steam generator (SG1, SG2 - secondary side), turbine (TB), generator (GN), condenser (CD), condensate extraction system (CE), feedwater system (FW) , and reheaters. For the tertiary cycle: condenser cooling pumps (CC). Control systems include for the primary cycle: reactor power control, pressurizer pressure control, pressurizer level control, reactor cooling flow control. For the secondary cycle: steam generator pressure control, steam generator pressure control, condenser pressure control, condenser level control and steam dump control. There is also a rector protection system. Figure 1 presents a basic diagram for the NPP.

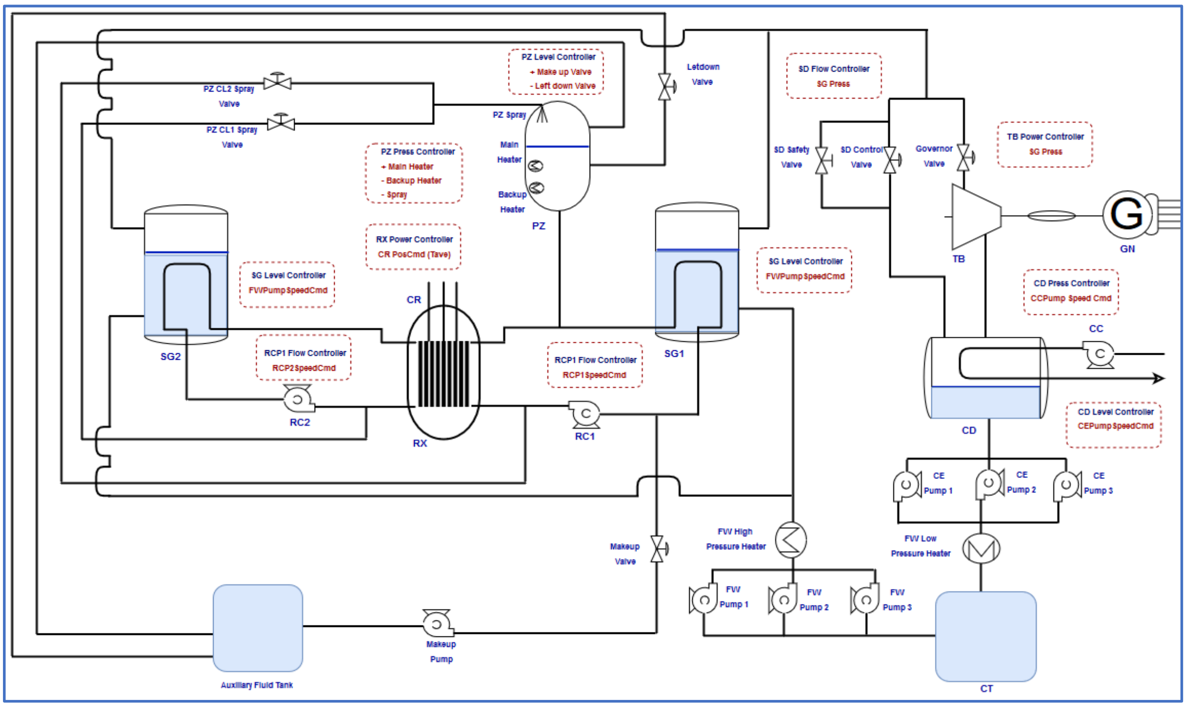


Figure 1. Basic Diagram for Asherah NPP

4. ASHERAH NUCLEAR POWER PLANT SIMULATOR

4.1 Plant Modelling

Following the guidelines listed above, basic principle models were developed for the plant systems and equipment. A point-kinetic model was employed for the reactor core, with formulations for neutronics and reactivity based on those of [6] and [7]. These models were adjusted and calibrated with respect to correspondent simulations of the reference model [5]. The pressurizer employs a three-element model similar to that of [8]. The reactor cooling pump model is based on the normalized curves of the reference model, as presented in [2] with added dynamics, while simple heat exchange equations and water/steam relations were employed for the development of the steam generator model.

The turbine and generator models were based on generic non-proprietary curves for equipment of similar dimensions with added dynamics. All pumps in the secondary cycle are also modelled from the normalized curves used in the reactor cooling pump models. All valves are modelled based on typical and standard curves for industrial valves with simple actuator dynamics. Water and steam thermodynamic properties are calculated following the 1997 formulation for industrial use of the International Association for the Properties of Water and Steam (IAPWS-IF97) (see www.iapws.org).

The models were originally intended to be capable of simulating normal transients, but to be adaptable and extendable to include some selected abnormal ones, such as turbine trips and equipment faults, according to eventual needs. Events such as loss of coolant accidents (LOCA) require complex modelling and great computer effort, so are outside the scope of the ANS current design, as well as post-accident and post-shutdown simulations.

4.2 Control Modelling

Control systems for NPPs present relatively complex structures [9], but considering the limited scope of this work, they will be functionally separated in: Supervisory Control System; Process Control Systems; Limitation Systems; Reactor Protection Systems and Engineered Safety Systems.

Limitation Systems were not considered, at least for the moment. Also, since the simulator scope is mostly limited to normal operation, engineered safety systems were not yet included.

It is expected that some of the studied computer attacks might cause automatic shutdown of the plant, so a simplified and preliminary reactor protection system was specified and included in the simulator. It is basically a list of conditions that activate a control signal intended to trip the reactor. Although post-accident and post-shutdown conditions are still outside the simulator scope, this signal simulation is important for marking the point in which a more prioritary control system would take over the (potentially compromised) process control system. This is also important to prevent deviation of the operational parameters to unrealistic regions (e.g. unlimited pressure surges or excessively high temperatures).

In view of that, greater emphasis was given to process control systems and supervisory control. All control loops were implemented with mostly industry-proven, very simple strategies, basically relying on Proportional + Integral + Derivative (PID) controllers whenever possible, following NPP Control standards even at the cost of plant performance. It should be stressed that controller performance was considered a non-fundamental requirement for the security analysis, so simple control algorithms are preferred.

Control for normal operation is essentially power lead, with the control system adjusting the plant operation point to produce the desired power output.

Apart from very simple embedded interfaces, a supervisory control system is not implemented in the simulator. The general idea being that realistic supervisory systems will be integrated to the simulator using communication interfaces, as has been the case of the early applications reported in the sequel.

Figure 2 presents a diagram of the simulator with respect to plant and control systems, assuming full simulation, i.e. all systems included in the simulation.

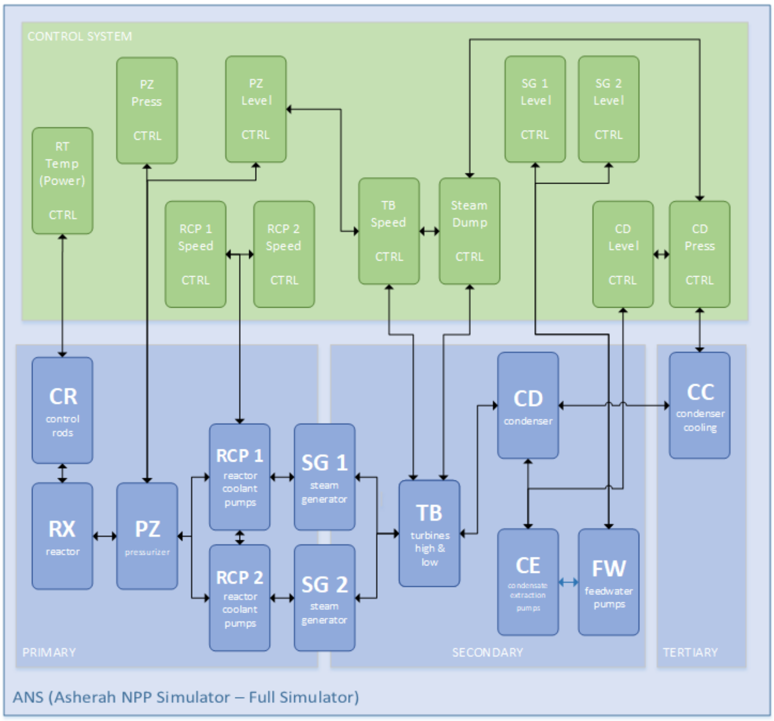


Figure 2. ANS Diagram

4.3 Communication

An important characteristic of the simulator is the capability of integrating with physical or virtual controllers and other IT equipment by means of network connection. The teams involved in the CRP defined Open Platform Communications – Universal Architecture (OPC-UA) as the preferred protocol for all types of communication.

The simulator also supports Modbus communication as an alternative if communication with equipment or systems that do not support OPC-UA is necessary.

There are two channels for network communication, named PROC I/O INTERFACE and CTRL DATA INTERFACE. The first should be used for all plant inputs and outputs, simulating selected sensor and actuator physical signals, that normally would not be transmitted in conventional networks, but rather through 4mA-20mA electrical loops, etc. These are segregated from other network communication so as not to pollute the network traffic and interfere with its analysis. The second channel should be used to simulate network communication between controllers or the supervisory system, representing the network traffic in a real system.

All communication is made using tags, and all relevant signals in the simulator have their own tags. These tags are compatible with the referencing of the OPC-UA protocol.

The general idea is that it is possible to replace any of the simulated blocks in the Figure 2 with physical counterparts in a specific test bed, therefore allowing ANS integration in Hardware-in-the-Loop (HIL) schemes.

For example, Figure 3 shows a configuration in which the simulated condenser (CD) is replaced with a physical system.

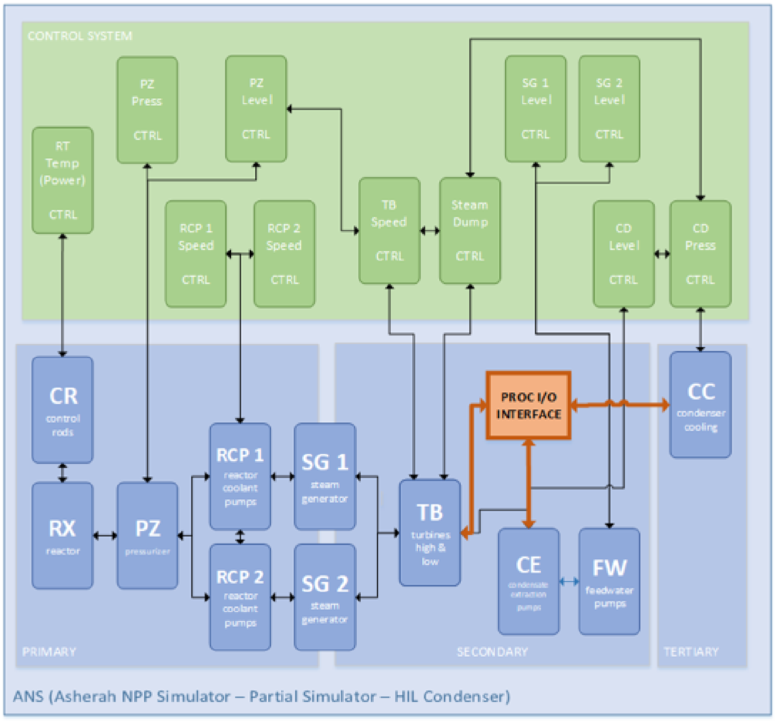


Figure 3. ANS Diagram (CD replaced with physical equipment)

Figure 4 shows a configuration in which the simulated pressurizer level controller is replaced with a physical controller. For this case both communication channels are used. The process I/O channel transmits signals related with sensors and actuators of that specific control loop while the control data channel performs communication, if needed, between the physical controller and related simulated controllers that exchange information with it.

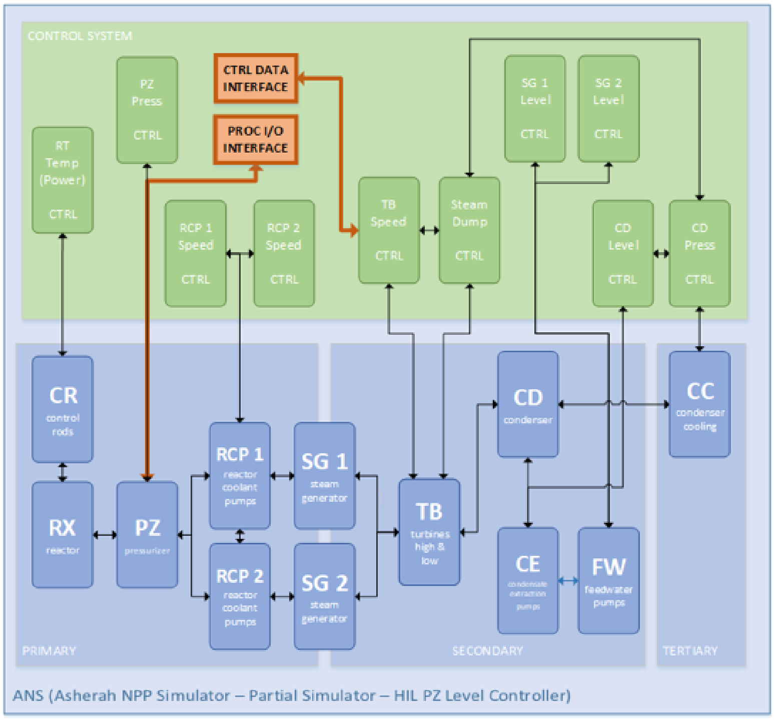


Figure 4. ANS Diagram (PZ Level CTRL replaced with physical equipment)

4.4 Configuration and Attack Terminal

A Configuration and Attack Terminal (CAT) was developed to perform tasks outside those of the regular equipment in the simulation setup or test bed. Such tasks include simulator configuration and control, e.g. start/stop, pause, etc.; attack initiation; data collection, storage and analysis (the simulator historian); network sniffing and analysis; attack initiation; general interface and supervision system for training.

Terminal functionality is a based on a diverse set of tools and it can be connected to the test bed in any of the test bed networks, as needed.

4.5 Implementation

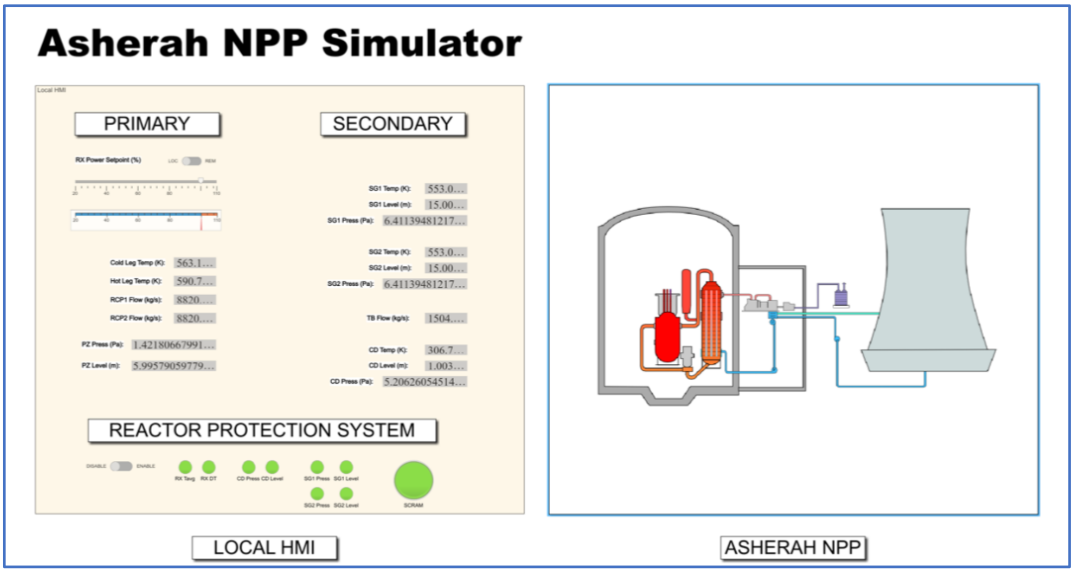
The simulator was mainly developed in the MATLAB/SIMULINK platform (see www.mathworks.com). This platform was adopted due to its graphical interface that simplifies coding tasks as well as its scientific capability.

The implementation is divided in two parts:

i. Configuration scripts, written in M, the MATLAB language, which serve two main purposes:
   - Parameter calculation and loading. There are different scripts for each plant or control system in order to facilitate modifications. All model parameters are easily located and loaded from the scripts. Any calculation needed to obtain these parameters can also be easily modified and performed in these scripts.
   - Initial condition calculation and loading. For every simulation, a set of coherent initial conditions must be loaded. The scripts allow the initial state to be chosen, e.g. Hot Full Power (100% Power) and loads all initial conditions. Like above, there are different scripts for each plant or control system.

ii. Simulation diagrams, created with function block diagrams from SIMULINK, containing all the formulation for the dynamical model of the plant and the control system. These can also be easily modified with mostly no coding required.

A very simple supervision interface is also implemented in the simulation diagram, as can be seen in Figure 5.



Cold Leg Temp (K): 563.1...
Hot Leg Temp (K): 590.7...
RCP1 Flow (kg/s): 8820....
RCP2 Flow (kg/s): 8820....
PZ Press (Pa): 1.42180667991...
PZ Level (m): 5.99579059779...

SG1 Temp (K): 553.0...
SG1 Level (m): 15.00...
SG1 Press (Pa): 6.41139481217...
SG2 Temp (K): 553.0...
SG2 Level (m): 15.00...
SG2 Press (Pa): 6.41139481217...
TB Flow (kg/s): 1504....
CD Temp (K): 306.7...
CD Level (m): 1.003...
CD Press (Pa): 5.20626054514...

Figure 5. Basic local interface for ANS, implemented in SIMULINK

Figures 6 and 7 present the simulation diagram for the primary and secondary cycles. The simulator currently contains more than 3,200 blocks in several similar diagrams, hierarquically arranged.

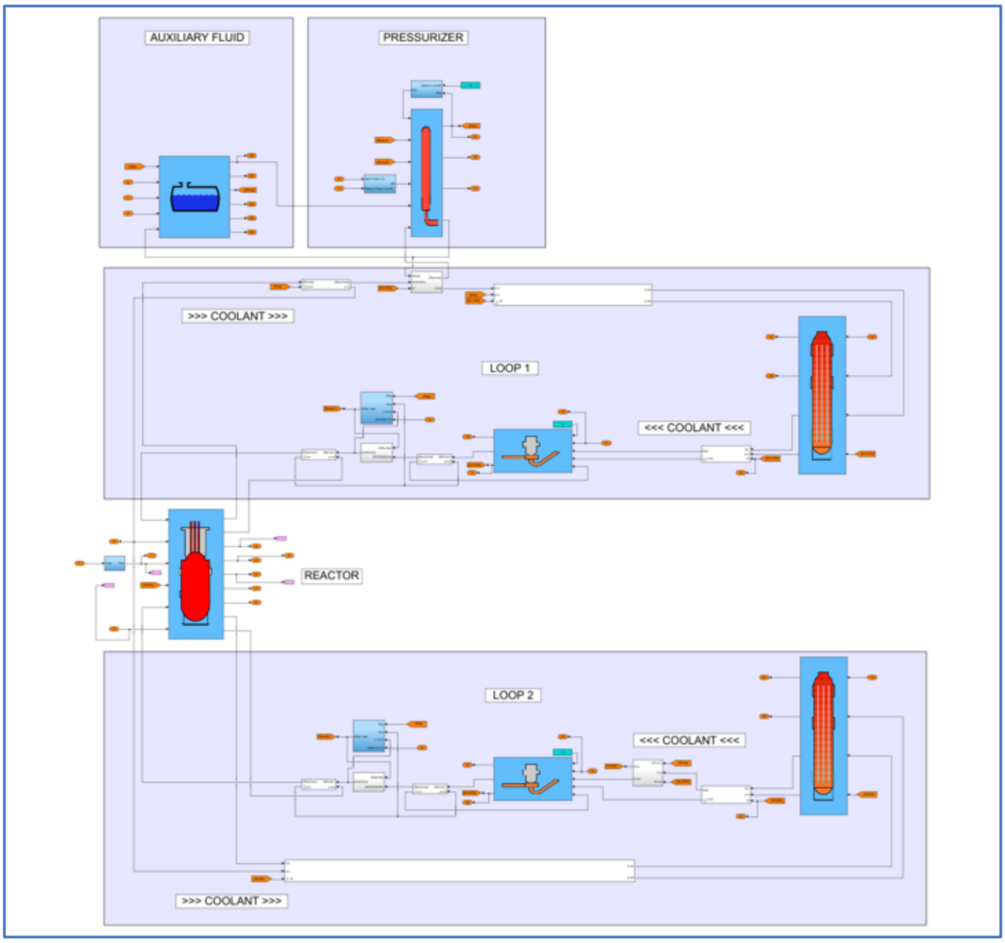


Figure 6. Simulation diagram for the primary cycle

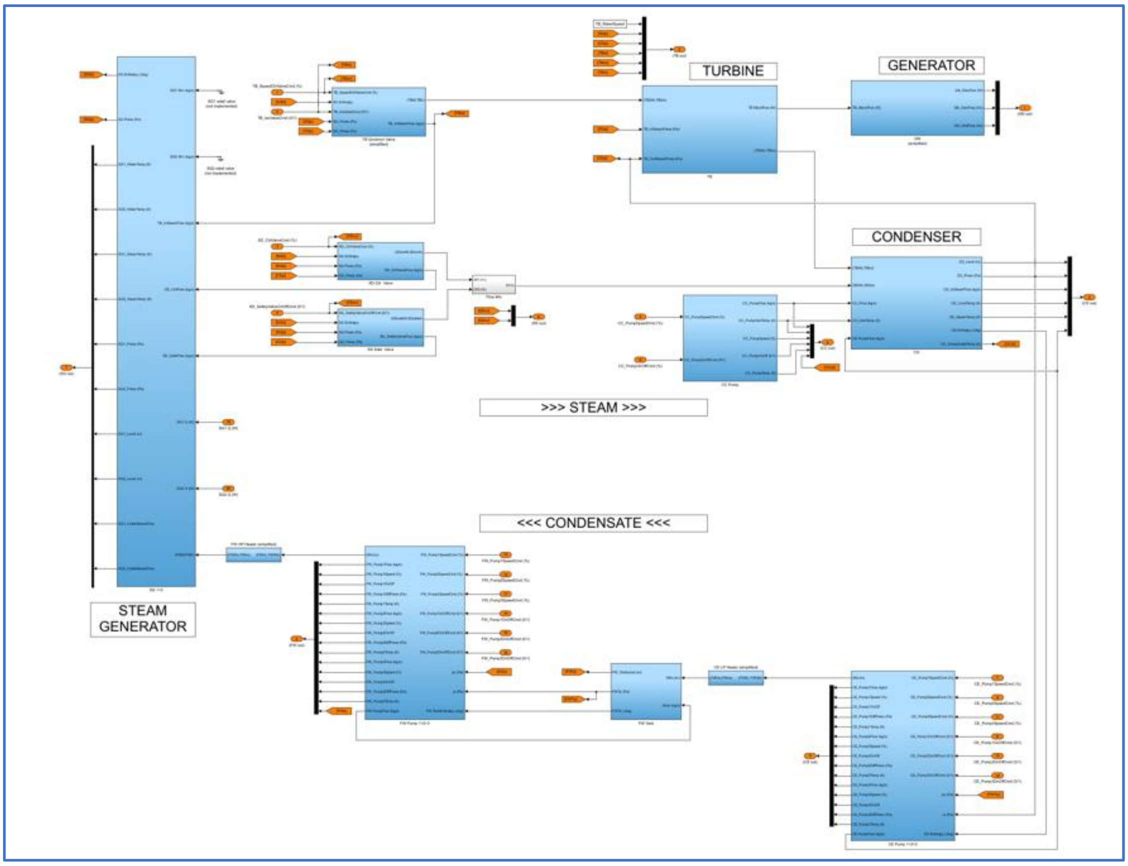


Figure 7. Simulation diagram for the secondary cycle

5. TEST BED INTEGRATION

5.1 Architecture

The simulator was developed specifically with test bed integration in mind and several different architectures can be implemented. A typical implementation is sketched in Figure 8. Part of the control system is simulated in ANS while part is implemented with physical Programable Logic Controllers (PLCs). In the figure implementation, actual analog signals are generated with a specific PLC acting as the process I/O. Although this setup reproduces in more detail a real application, it can be simplified using direct OPC-UA communication between ANS and the physical control system.

The test bed is here referred as Asherah Test Bed (ATB), while the part of the test bed containing physical equipment is referred as Asherah Hardware in the Loop (AHL), so the actual test bed ATB is comprised of ANS, AHL and CAT.

Several network architectures can be implemented in ATB, from Security Level 1 (SL1) up to Security Level 5 (SL5) [10].

5.2 First applications

An implementation of a configuration of ATB similar to that of Figure 8 was done in the University of São Paulo (USP), as shown in the picture of Figure 9. Similar implementations have also been done by other teams and institutions involved in the CRP.

The setup of Figure 4 has been successfully implemented for computer security training exercises during the the *2nd Brazilian Guardian Cyber Exercise (EGC 2.0)*, event held in Brasília, Brazil in July/2019. It is also reported that a somewhat similar setup to the one in Figure 3 was successfully implemented in the *International*

Training Course for Protecting Computer Based Systems in Nuclear Security in Daejeon, Republic of Korea in November/2019.

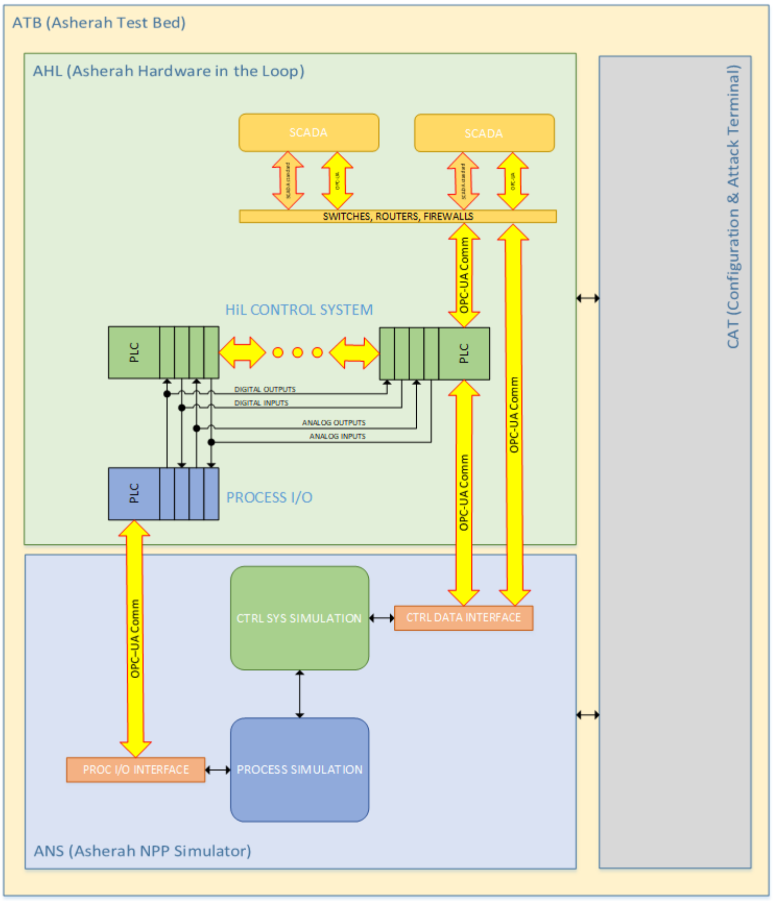


Figure 8. Asherah Test Bed (typical configuration)

6. COMMENTS AND FUTURE DEVELOPMENT

Although ANS and ATB are works in progress, the current experience indicates that they are very valuable tools for computer security research and assessment. Further uses include computer security measures development, information sharing and training.

Development of ANS is expected to proceed and further improvements such as the production of a runtime version, independent of the MATLAB/SIMULINK platform and a remote interface for deployment are being considered. New capabilities and features such as post-shutdown simulation, more comprehensive modelling, enhanced integrability, etc. are expected to be added as development progresses.

7. ACKNOWLEDGEMENTS

This work was made possible by the support of the São Paulo State Research Foundation (FAPESP) through Grant 2016/04600-0 and IAEA, through Research Contract No. 22527.

The authors also acknowledge the invaluable inputs, contributions and support from the participants of the CRP J02008.

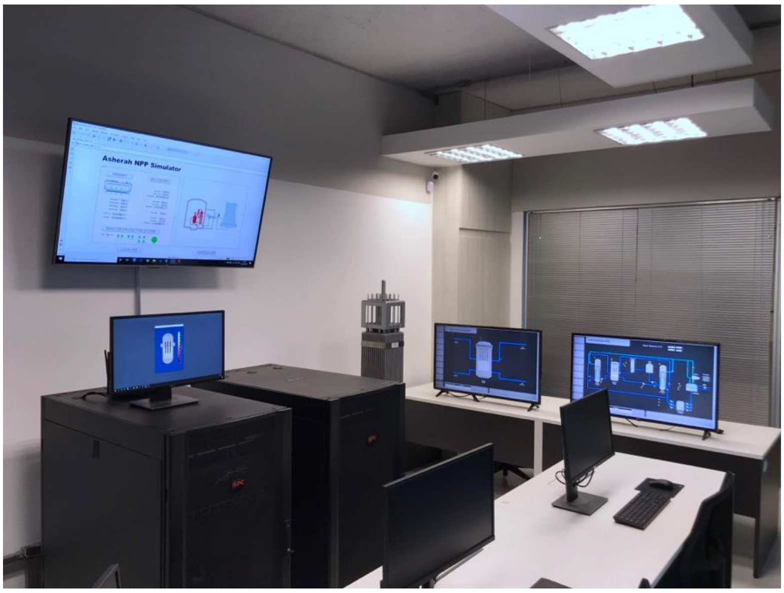


Figure 9. ATB at University of São Paulo, Brazil

REFERENCES

[1] U.S. NUCLEAR REGULATORY COMMISSION. Backgrounder on the Three Mile Island Accident. www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html. Accessed on September 16, 2017.

[2] IVANOV, K.N. et al. Pressurized Water Reactor Main Steam Line Break (MSLB) Benchmark. Volume I: Final Specifications. Organization for Economic Co-Operation and Development (OECD), Nuclear Energy Agency (NEA), 1999.

[3] ROWLAND, M.T.; BUSQUIM e SILVA, R.A. IAEA Coordinated Research Project on Enhancing Incident Response at Nuclear Facilities. *11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*. Orlando, 2019.

[4] BUSQUIM e SILVA, R.A.; SHIRVAN, K.; CRUZ, J.J.; MARQUES, R.P.; MARQUES, A.L.F.; PIQUEIRA, J.R.C. Use of State Estimation Methods for Instrumentation and Control Cyber Security Assessment in Nuclear Facilities. *International Conference on Nuclear Security: Commitments and Actions*, Vienna, 2016.

[5] BUSQUIM e SILVA, R.A.; SHIRVAN, K.; CRUZ, J.J.; MARQUES, R.P.; MARQUES, A.L.F.; PIQUEIRA, J.R.C. Advanced method for neutronics and system code coupling RELAP, PARCS and MATLAB for instrumentation and control. *Annals of Nuclear Engineering*. https://doi.org/10.1016/j.anucene.2019.107098

[6] KINARD, M.; ALLEN, E.J. Efficient numerical solution of the point kinetics equations in nuclear reactor dynamics. *Annals of Nuclear Engineering* 31 (2004) 1039-1051.

[7] PUCHALSKI, B. et al. Nodal models of Pressurized Water Reactor core for control purposes – A comparison study. *Nuclear Engineering and Design* 322 (2017) 444-463.

[8] JIN, M.A. et al. Mechanism Model and Simulation of Pressurizer in the Pressurized Water Reactor Nuclear Power Plant. *30th Chinese Control Conference*. Yantai, 2011.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY. Modern instrumentation and control for nuclear power plants: a guidebook. Technical Report Series No. 387. Vienna, 1999.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. IAEA Nuclear Security Series No. 33-T. Vienna, 2018.