NUCLEAR POWER PLANT IN A BOX

R. ALTSCHAFFEL
Otto-von-Guericke University
Magdeburg, Germany
Email: Robert.Altschaffel@iti.cs.uni-madeburg.de

T. HOLCZER
BME Crysys
Budapest, Hungary

R. A. BUSQUIM E SILVA
Brazilian Government
Sao Paulo, Brazil

J. LI
Tsinghua University
Beijing, China

P. GYORGY
BME Crysys
Budapest, Hungary

M. HILDEBRANDT
Otto-von-Guericke University
Magdeburg, Germany

M. HEWES
IAEA

Abstract

The paper presents the development of an architecture to deploy a simulated nuclear power plant in order to support training and research. In contrast to other simulators, which focus on the underlying physical processes, this approach also covers the industrial control systems (ICS) supervising and controlling these processes. Additionally, the IT components required for the associated business processes are also included, allowing for training with regard to threats to these IT components, including cyber-attack scenarios.

1. INTRODUCTION

Training and research are essential in keeping nuclear power plants (NPP) safe and secure. Training enables operators to react adequately to incidents and emergencies, while research helps to identify potential problems beforehand and allows for mitigations which prevent these incidents in the first place.

Training requires access to the equipment on which the operators are supposed to train. As this is in general hard to achieve, simulators and mock-ups are used instead. Complex hardware-based simulators including the Instrumentation and Control (I&C) of a NPP are expensive and often cover only a subsystem. Other software-based simulators are cheaper to deploy and focus on the physical processes in the NPP alone, allowing the operator training in this regard. These simulators are perfectly fine for training in normal operations and often include options to simulate various physical breakdowns in components. However, these software-based simulators do not take into account the underlying operational technology (OT, also referred to as Industrial Control System - ICS).

With the increasing relevance attacks on ICS, training to increase awareness and to support adequate incident response and contingency measures is necessary. Here, simulators that realistically implement the behaviour of the ICS are required.

Additionally, higher level business processes are a part of every nuclear power plant. These processes are supported by information technology (IT). While these processes are segregated from the ICS, they still might offer a potential attacker information about the ICS processes or even an access to the ICS itself. Hence, they cannot be left out of the picture for comprehensive cyber-security training.

This paper presents the development of an architecture to deploy a simulated nuclear power plant in order to support training and research within the scope of CRP J02008[1]. This simulated nuclear power plant ASHERAH consists of components covering the underlying physical process, the OT components supervising and controlling these processes, the control room and the IT components required to the associated business processes.

This architecture is created to be a. easily deployable, b. extendable, c. realistic in the simulation of the underlying physical process d. realistic in the behaviour of its digital assets, e. allows access to a broad range of data and f. customizable for the use in training scenarios.

This paper is structured as follows: After this introduction in the first section, the second section will describe the structure of the OT and IT within nuclear power plants and how they interact with the underlying physical process. The third section will show how the underlying physical process is implemented in this simulator, while the fourth and fifth section discuss the implementation of the OT and IT respectively. The sixth section gives a brief overview over the implementation of a control room (a HMI - Human-Machine-Interface) to supervise and control the simulated physical process. The seventh section ties these components together and discusses the communication between the various elements of this simulator. The eight section serves as a conclusion and gives an outlook on future work.

2. IT AND OT IN NPPS

The Purdue enterprise reference architecture (PERA) [1] describes the structure of Industrial Control Sysstems and the associated business systems in five different levels and three different zones according to their function. For the sake of a clarity of terms, these levels will be referred to as *Purdue levels* and *Purdue zones* for the scope of this work.

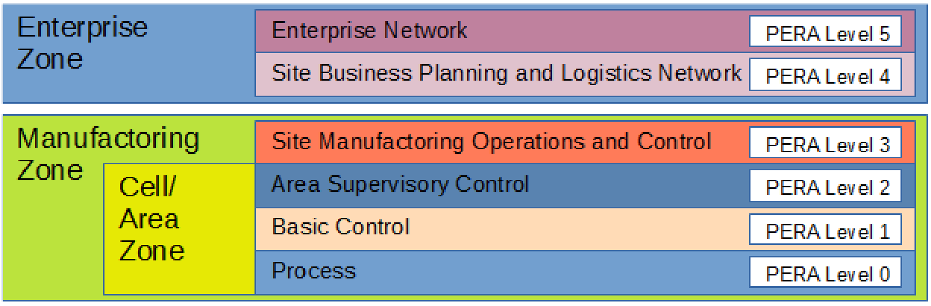

Fig. 1. Control Hierarchy of ICS according to [1]

This hierarchy (as shown in Fig. 1.) consists of:

- Purdue Level 0 - Process sensors and actuators involved in the basic manufacturing process, performing basic functions of the ICS;
- Purdue Level 1 - Basic Control controllers (typically a PLC) that direct and manipulate the manufacturing process, interfacing with the Level 0 devices;
- Purdue Level 2 - Area Supervisory Control applications and functions associated with the Cell/Area zone runtime supervision and operation (incl. operator interfaces or alarms);
- Purdue Level 3 - Site Level plant-wide ICS functions;
- Purdue Level 4 - Site Business Planning and Logistics functions and systems incl. basic business administration tasks) that need standard access to services provided by the enterprise network and
- Purdue Level 5 - Enterprise centralized IT systems and functions

[1] https://www.iaea.org/projects/crp/j02008

Within the Cell/Area-Zone ICS functions are located, while the Enterprise zone describes functions of classical IT-environments. While this dictates the basic structure of IT and OT, the nuclear field warrants additional considerations based on network segregation for the sake of security. The IAEAs exemplary implementation in the Nuclear Security Series Draft on Computer Security Techniques for Nuclear Facilities (NST047 [2]) defines communication flows between various Security Levels and Security Zones. The five security levels within are described to cover, based on a graded approach to addressing the consequences of compromise, protection systems (Security Level 1), operational control systems (Security Level 2), supervision real time systems (Security Level 3), technical data management systems (Security Level 4) and other systems (Security Level 5) [2].

These Security Levels roughly corresponds to the Purdue levels. Security Level 1-3 roughly aligns to the Cell/Area-Zone while Security Levels 4 and 5 align with the Enterprise Zone.

In order to create a realistic environment for training and research, the proposed architecture follows this hierarchy.

3. SIMULATING THE PHYSICAL PROCESS

A NPP is a very complex power system: it consists of a myriad of complex industrial processes, with a large number of technology information and automation control systems – many of these systems perform nuclear safety and security functions. Under the IAEA CRP J02008, the University of Sao Paulo (USP) developed the Asherah NPP simulator (ANS) suitable for digital research, cyber security assessment and computer security measures development. This NPP model is based on a 2,772 MWt pressurized water reactor (PWR) Babcock & Wilcox (B&W) (see [3],[4] and [5] for further information] core implemented using Matlab/Simulink[2]. This nuclear power plant was previously modelled using the nuclear codes PARCS/RELAP (see [6]) and its simulation results were benchmarked against open source literature used as reference (see [7]) for the development and fine tuning of ANS.

ANS is the heart of a hardware in the loop simulation (HIL) test bed that integrates operational technology (OT) and information and technology (IT) capabilities. Its integration capabilities include realistic process behaviour and network communication by means of the open cross-platform machine-to-machine OPC Unified Architecture[3] (OPC-UA) protocol. In addition, two CRP developed interfaces allow the replacement of simulated NPP subsystems or controllers by their real counterparts (as discussed in more detail in Section 4). The OT plant inputs and outputs, which simulate sensors and actuators physical signals, may be accessed outside ANS by means of the PROC I/O INTERFACE. The CTRL DATA INTERFACE allows the network communication between controllers or the supervisory system, representing the network traffic in a real system. Using both interfaces, process data and network data may be captured (using sniffers, for instance) and analysed. It is worth noting that the process communication uses predefined tags (I/O) compatible with the OPC-UA protocol but industrial protocols can be easily deployed.

ANS runs in soft real time (non deterministic) on Windows-based computers. Therefore, latency values are those expected of common Windows applications. Due to its design, controllers and process systems can run in different virtual machines if required by the scenario being simulated – a network time protocol may be needed. These features add significant flexibility that may be useful for the implementation of complex HIL setups.

ANS, from the physical process point of view, comprehends the main plant subsystems - and some piece of equipment important for safety or security of the primary, secondary and tertiary cycle: the reactor core with the control rods; the 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, and reheaters. Besides real IT systems, virtual programmable logic controllers (PLC), routers, firewalls and multilayer virtual switches

[2] https://www.mathworks.com/products/simulink.html

[3] https://opcfoundation.org/about/opc-technologies/opc-ua/

can be integrated under the same HIL set up. These features allow the use of as many virtual OT and IT systems as needed to adequate simulate, without large number of dedicated hardware, security levels 2 to 5.

Although ANS was designed to run using the control room human-machine-interface (HMI, as discussed in Section 6), a few simple embedded interfaces, including a supervisory control system, helps the integration of the simulator with distinct test beds.

4. SIMULATING THE OT

The operational technology handles Instrumentation and Control (I&C) of the physical process. As the physical process is split between various subsystems, such is the OT. In order to simulate IT in a realistic manner, it is necessary to include the primary components of OT. These are sensors (which gather data about the physical process), computing units (usually a PLC; which compute this data and send control signals accordingly), actors (which implement these control signals and hence influence the physical process) and the communication between these components.

In the simplest form, sensors and actors can be handled by attaching the simulated OT to the simulation of the physical process. A sensor would in this case take a physical property from the simulation of the physical process, translate it into a sensor reading and then transmit it to the computing unit. A control signal from computing unit to an actor would also be relayed to the simulation of the physical process. Here, sensors and actors are merely converters between the physical simulation and the computing unit. For the communication between sensors, actors and the computing units would employ I&C specific protocols.

However, this solution is not optimal, as it would require communication between the physical simulation and these mock sensors and actors. This communication would not occur in a realistic setting and hence might be problematic for some training scenarios or research questions.

A better solution is the employment of a co-simulation. In this case, the physical process which is handled by the subsystem in question, is simulated within the OT portion. Sensors translate signals coming from the co-simulation to I&C specific protocols before transmitting these to the computing units. Actors give feedback to the co-simulation after receiving control signals using I&C specific protocols again. The overall subsystem still communicates with the simulation of the overall physical system, where information about other subsystems, like inputs are required.

However, the necessary readings are usually gathered within the historians anyway. Thus, the specific overhead for the communication within the simulated environment depends on the implementation.

An alternative approach is the usage of multiple network interfaces, whereas the first interface is used like it would be attached to the infrastructure of a nuclear power plant. The second interface could be used to interface with the physical process simulation in order to provide inputs with the necessary readings and to adjust the behaviour of the simulation according to the outputs of the PLCs. This is also possible for hardware-in-the-loop (HIL) setups with PLCs with multiple network interfaces.

Indeed, it would also be possible to use a physical mock up of a subsystem instead of a co-simulation. The approach presented here is adaptable enough to support such an approach, but in order to fulfil the requirement of an easy deployment, a more detailed description of a completely virtualized subsystem is given.

Our proposal for a simulated portion of the OT relies on PLCSIM Advanced [4]to create virtualized PLCs The virtualized PLC communicates (physical) process variables using OPC UA with the co-simulation module This co-simulation module handles the underlying physical process and provides the virtualized PLCs with realistic input via the PLCSIM Advanced API. The simulation module is programmed in C# and allows for easy alteration or extension of the system setup. In addition, the simulation module is able to inject various cyber events, errors and jitter to the transmitted data. Additionally, a local HMI is included to give a system operators view to a potential trainee or investigator. This architecture allows the researcher access to the 'physical reality' of the simulated process (hence, rather 'model reality') as well as the 'PLC reality' (how the physical process performs from the viewpoint of the PLC) as well as the 'Operator reality' (how the physical process performs from the viewpoint of the Operator). This approach is discussed in more detail in [8].

[4] https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10316003

5. SIMULATING THE IT

As described in Section 2, a Nuclear Power Plant does not only include an OT portion, but also traditional corporate systems like email or web systems, and special-purpose systems like document management or work order management systems. In this section, we will briefly describe how they can be simulated.

Simulating the traditional IT part of a Nuclear Power Plant is a straightforward task. Our goal was to make it stable, easy to deploy, easy to modify and as compact as possible. This goal can be achieved by using some Infrastructure as Code (IaC) solution with virtualization.

An IaC solution enables us to write the topology and configuration of some virtual machines as an easy to read set of configuration files. From the configuration files, an orchestrator can deploy the whole infrastructure on will. There are many IaC solutions accessible. Our objective was to select one with the following features: (i) open-source – anyone can use and enhance it on will[5], (ii) support for different systems like Linux or Windows virtual machines or VMware and Cisco devices, (iii) agentless – it is good if we can configure the infrastructure without leaving any traces of the instrumentation after the deployment phase. These requirements can be fulfilled by Ansible[6]. Ansible also has the big advantage that we can select from thousands of predefined roles created by the community to use in our infrastructure[7].

To run tens of virtual machines and virtual networks in parallel, we need some virtualization infrastructure. This infrastructure should support the following: (i) full virtualization of hosts, (ii) virtualization of networks with switches, VLANs, routers, etc., (iii) support from Ansible, (iv) support for snapshots and reverting. These requirements can be met by VMware ESXi[8], which was our choice for the implementation.

The steps of creating the required Security Level 4 and 5 infrastructures are the following: (i) design the desired network and systems, (ii) create base images for the virtual machines, (iii) create scripts which can deploy the networks populated with base virtual machines, (iii) create scripts to configure the virtual machines.

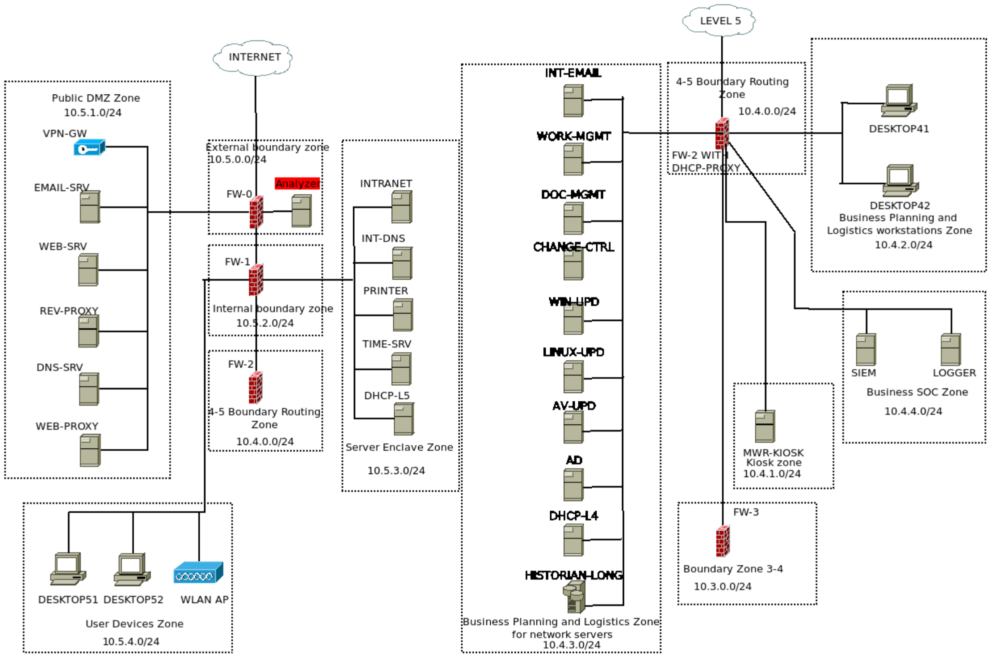

Fig. 2. Virtual Security Level 4 (right) and 5 (left) topology

[5] We made an enhancement to Ansible to create mirror ports on our virtual infrastructure to enable traffic monitoring: https://docs.ansible.com/ansible/latest/modules/vmware_vspan_session_module.html

[6] https://www.ansible.com/

[7] https://galaxy.ansible.com/

[8] https://www.vmware.com/products/esxi-and-esx.html

In our work, we created more than 30 virtual machines to populate our network. The design of Security Level 4 and 5 can be found in Fig. 2.

We had both Linux and Windows virtual machines in our network with two different versions of Windows (Server and Desktop versions) so we created three base images. After this, we could start writing the playbooks for installing the previously defined roles on our virtual machines. Most of the roles we needed to install were available on Ansible Galaxy, however, in most cases, the downloaded roles had to be customized for our needs.

Finally, we had roles for each virtual machine including the following: firewalls between the levels and zones, email and web servers, time and printer servers, desktop machines and a plant historian. The plant historian stored the data in an InfluxDB[9] with a Grafana[10]-based visualization and got its input from a Security Level 3 service in a way described in Section 7. The whole implementation of the Security Level 4 and 5 systems enables a realistic simulation of the Plant with realistic attack scenarios, where the kill-chain can include initial adversarial steps in the higher levels before attacking the operational technology parts.

6. CONTROLLING AND SUPERVISING THE SIMULATED PHYSICAL PROCESS

In an NPP, the physical processes or systems are ultimately controlled and supervised by the operations personnel via the Human-Machine Interface (HMI). The HMI links the two key components of the "central nervous system" of an NPP together - the I&C system architecture, and plant operations personnel [9]. The HMI provides the personnel a visual overview of the status of each process/systems and multiple controls of the NPP’s operation.

In the simulated NPP, the HMI controlling and supervising the simulated physical process also plays an essential role for the following reasons: First, since it can display the data from the simulated physical process, the HMI could visually demonstrate the effect of cyber-attacks on OT systems. Second, the HMI itself is a part of the attack surface of an NPP. The falsified information could be presented to operators for hiding an attack or misleading the operators. In this case, incorrect control commands based on false information could be issued from the compromised HMI. Third, the HMI is also an important part for the cyber security incident response. The alarms of detected anomalies will be shown on the HMI. Many steps of cyber emergency procedures are also to be executed through the HMI.

The design of the HMI is full of challenges since the status information of each system should be elaborately organized in the manner of human-factor engineering (HFE). Many commercial HMIs have the features satisfying the requirements of HFE. However, the costs of these commercial HMIs exceed the budget of an easy to deploy simulator project.

In ASHERAH, open source software together with an HMI design guide serve as the basis for the HMI development. The HMI guidance for the CRP is based on design experience of real NPP HMI. It specified the design requirements of HMI for better compliance with the principle of HFE, such as the colour, the character, the diagram symbol, the display layout, the display type, the human-machine interaction, etc. The local HMI as well as the HMI of the Main Control Room (MCR) could be qualified and consistent when following the HMI guidance. Four displays of the MCR HMI have been developed for the simulated NPP. They are:

— Steam Generator (as seen in Fig.3.)
— Pressurizer
— Turbine
— Condenser

An exemplary view of the Steam Generator HMI display is given in Fig. 3. Here the various points for the display of data are visible. In addition, some setpoints where an operator can control the physical process, are visible.

[9] https://www.influxdata.com/

[10] https://grafana.com/

In summary, the HMI compliant with the HFE principle based on open source software (in this case ScadaBR[11]) have been developed to control and supervise the simulated physical process.

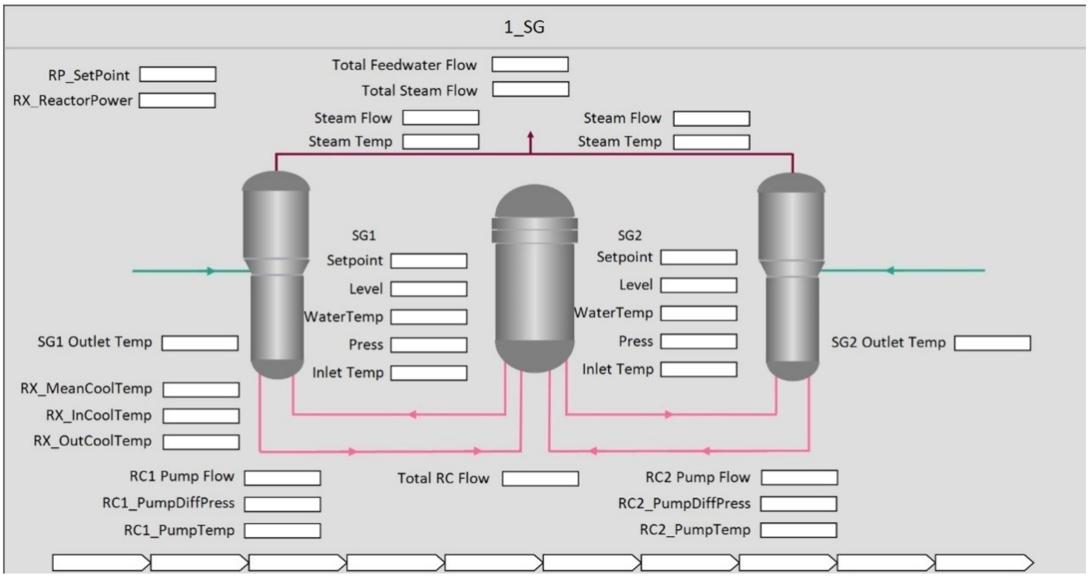

Fig. 3. Steam Generator Display

7. COMMUNICATION BETWEEN THE ELEMENTS OF THE VIRTUAL NPP

The overall architecture ties together the simulated physical process, the simulated OT and the simulated IT in order to provide a virtual NPP. For this, various communication flows are necessary. In the simplest case, the simulated OT requires information about the physical process as supplied by the simulated physical process. This data would, for example, be supplied to a Plant Historian residing within the simulated OT on Security Level 4. In addition, the HMI on Security Level 3 would require information about the underlying physical process. Since the HMI is able to control the process, this connection between Security Level 2 and Security Level 3 would have to be bidirectional. This structure can be seen in Fig. 4.

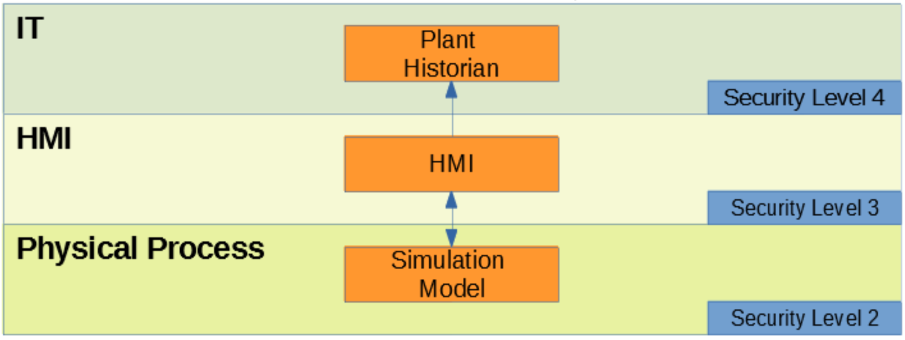

Fig. 4. Basic communication between the various components

More complex scenarios include an OT subsystem is part of the overall architecture. As shown in Section 4, these parts simulate control process in a greater detail and hence provide valuable opportunities for training and research. The OT itself can be either fully virtualized or include physical components, like a physical PLC if available. In each case, the OT portion is plugged into the communication. Hence, the communication flows become more complex. Here, the simulation of the physical process communicates directly with the OT in question, since the OT requires information about the physical process. Both communicate with the HMI. The basic structure for this communication can be seen in Fig. 5.

[11] https://sourceforge.net/p/scadabr/wiki/Home/

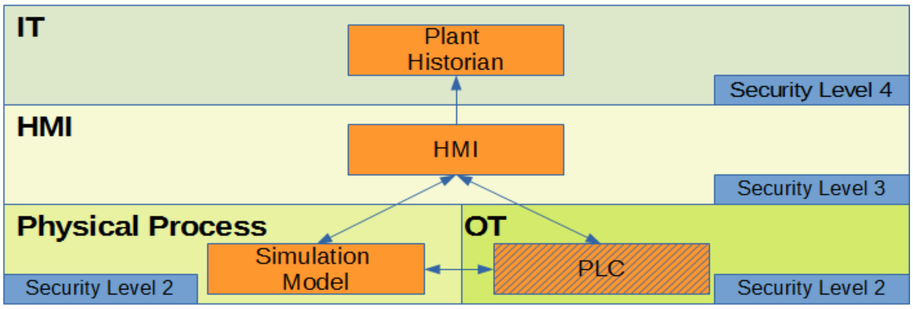

Fig. 5. Communication between the various components with inclusion of an OT portion ('Builder System')

In order to control this communication flow, it is necessary to define which data is communicated. For this, the current implementation uses I/O lists. This is a list of input and output provided by the various components. For example, each of the OT portions which could be plugged into the overall architecture, has an I/O List describing which data it needs from the simulation model and which data it provides to both the HMI and the simulation model. In order to facilitate easy extension while still using ICS protocols, OPC UA is used. The respective OPC UA tags are also part of the I/O list and hence, it is easy to change the OPC UA servers and clients to use a value provided by a plugged in OT component instead of a value provided by the simulation model. The complete communication of a deployed ASHERAH including an OT portion can be seen in Fig. 6.

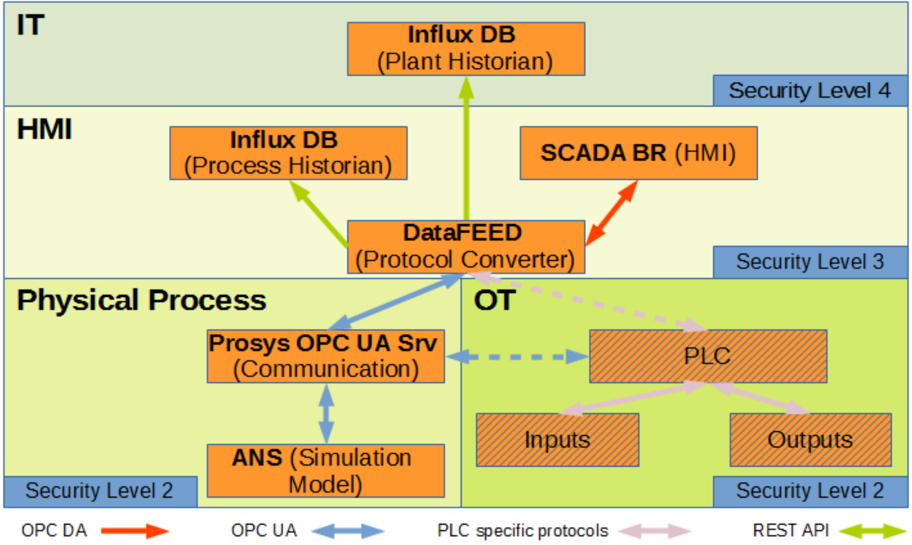

Fig. 6. *Communication between the various components of a fully deployed ASHERAH including communication protocols*

An OPC UA Server is used by ANS in order to communicate with the OT Portion and the HMI Portion. ANS communicates with the OPC UA Server using OPC UA. If the PLC inside the OT Portion is able to use OPC UA as well, it can directly communicate with this OPC UA Server. If not, protocol translation is required. This is handled by the DataFeed Protocol Converter which translates between OPC UA, OPC DA and various I&C specific protocols. On the OT side, the PLC (either virtualized/simulated or a physical device) communicates with the inputs and outputs - sensors and actors respectively (either virtualized/simulated or physical devices) - using I&C specific communication protocols. DataFeed is required to convert OPC UA communication into OPC DA communication which is used by the HMI. Both, the Plant and Process Historians, receive data about the physical process using one directional REST API communication.

8. SUMMARY AND OUTLOOK

This work presents an easy-to-deploy virtualised NPP including the business processes. The overall architecture consists of a simulator for the physical process, an OT portion including a PLC and attached sensors and actors, a HMI and the affiliated Historians, including the Plant Historian residing in the business zone. The simulator is built with a realistic architecture for IT and OT in mind, implementing the Security Zones concept (see [2] for details on the DCSA). In addition, a broad range of realistic communication protocols are used. The overall architecture is highly adaptable and extendable.

Hence, research into different aspects of NPP IT and OT is possible including the establishment of new security measures like anomaly detection for cyber attack identification or better security architectures.

As for the training aspect, ASHERAH offers a broad range of possibilities. A first glimpse of its potential was made available during the IAEA Training Course on Protecting Nuclear Facilities from Cyber-Attacks 2019 in the Republic of Korea. Here ASHERAH was used for a complex attack scenario including the infiltration of the business network by an APT, the exfiltration of sensitive data which led to the deployment of a tailored attack against the OT portion of ASHERAH. The virtualised NPP allowed the trainees to witness the effect of this attack on the attached OT portion (which acts as physical system during this training) as well as the control room. The architecture allowed for the creation of realistic attack indicators and a realistic incident response and incident recovery training.

However, there are still open issues. Current work focuses on making the overall software stack less reliant on licensed software while improving the performance.

ACKNOWLEDGEMENTS

We would like to thank everyone who has contributed to CRP J02008. ASHERAH stands as major output of this research project and was only possible with the input from all participants.

REFERENCES

[1] 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

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

[3] BUSQUIM E SILVA, R., FERREIRA MARQUES, A. L., CRUZ, J. J., SHIRVAN, K., KAZIMI, M.S., " Reactivity estimation during a reactivity-initiated accident using the extended Kalman filter", Annals of Nuclear Energy, vol. 85, pp. 753-762, 2015. https://doi.org/10.1016/j.anucene.2015.06.031

[4] BUSQUIM E SILVA, R.,"Implications of advanced computational methods for reactivity initiated accidents in nuclear reactors", University of Sao Paulo, 2015.

[5] BUSQUIM E SILVA, R., FERREIRA MARQUES, A. L., CRUZ, J. J., MARQUES, R.P., 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 – Austria, 2016.

[6] BUSQUIM E SILVA, R., SHIRVAN, K,. MARQUES, R.P., CRUZ, J. J., FERREIRA MARQUES, A. L., PIQUEIRA, J.R.C., "Advanced method for neutronics and system code coupling RELAP, PARCS and MATLAB for instrumentation and control" Annals of Nuclear Engineering, 2019. https://doi.org/10.1016/j.anucene.2019.107098

[7] 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).

[8] ALTSCHAFFEL, R. et Al, "A Simulated Steam Turbine Generator Subsystem for Research and Training", to appear in International Conference on Nuclear Security 2019

[9] IAEA,"Instrumentation and Control Systems for Nuclear Power Plants", https://www.iaea.org/topics/operation-and-maintenance/instrumentation-and-control-systems-for-nuclear-power-plants