Contribution ID: **515** Type: **Paper**

Nuclear Power Plant in a Box

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. This simulated nuclear power plant ASHERAH consists of components covering the underlying physical process, the Industrial Control System ("ICS") components supervising and controlling these processes 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 behavior of its digital assets, e. allows access to a broad range of data and f. customizable for the use in training scenarios.

The Purdue enterprise reference architecture [1] describes the structure of ICSs and the associated business systems in five different levels and three different zones according to their function. Within the Cell/Area-Zone, ICS functions are performed, while the Enterprise zone describes functions of classical IT-environments. Further information on NPP ICS architecture is defined by the IAEA's example implementation in the Nuclear Security Series Draft on Computer Security Techniques for Nuclear Facilities (NST047 [2]). This implementation 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) [1].

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.

On the lowest level, a complex simulation of the physical processes is performed in order to supply the respective ICS with realistic input and enable realistic communication behavior between computing units, the attached sensors and the (simulated) actors. This simulation is performed using a MATLAB Simulink model. Information about the simulated physical process is then passed on, using ICS communication protocols to the specific PLCs situated on Security Level 1-3 (or the Cell/Area-Zone). Currently, OPC UA and Modbus-TCP are employed to facilitate this communication. These physical input is then used to operate the given PLCs in a Hardware-in-the-Loop ("HIL") fashion. In this area, realistic subsystem setups are used, using various PLCs and local HMIs which communicate using realistic ICS specific communication protocols. The structure of the underlying MATLAB model allows the usage of real physical sensors and actors instead of the simulated ones during testing.

The Enterprise Zone is implemented by virtual machines configured byAnsibleto automatically deploy a broad range of various enterprise services. Some examples of the services on Security Level 5 are the internal and external email system, intranet and Internet access, web servers with proxies and network services (e.g. NTP, DNS, DHCP). On the Security Level 4 we implemented more specific services like work order management,change control management and plant historian services.

The overall architecture contains information flows from Security Level 1-3 to Security Level 4-5. Local HMI on Security Level 2 receive information from Security Level 1 components. A control Room HMI on Security Level 3 gathers the information from the various Security Level 2 system. A Process Historian on Security Level 3 and a Plant Historian on Security Level 4 make this data further available.

The proposed architecture allows for the use in training scenarios, as it allows easy deployment, replication and the inclusion of various attack scenarios. The scope of the proposed architecture allows for complex cyber attacks spanning various attack steps as well as localized attacks employing single devices within subsystems. The architecture allows for the collection of data for the purpose of training, test and potential investigation.

[1] Theodore J. Williams: The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: Instrument Society of America (1992)

[2] IAEA: COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES; https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst047.pdf (accessed 28/05/19)

[3] M. J. Assante, R. M. Lee:The Industrial Control System Cyber Kill Chain. (2015); https://www.sans.org/reading-room/whitepapers/ICS/paper/36297 (accessed 28/05/19)

Gender

Not Specified

State

Germany

Authors: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HOLCZER, Tamás (BME Crysys); BUSQUIM E SILVA, Rodney Aparecido (Brazilian Governement); Mr GYORGY, Peter (BME CrySyS); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg); HEWES, Mitchell (IAEA)

Presenters: ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg); HILDEBRANDT, Mario (Otto-von-Guericke-University of Magdeburg)

Track Classification: CC: Information and computer security considerations for nuclear security