Contribution ID: **453** Type: **Paper**

Understanding Nuclear Cyber Security Measures, Risks and Consequences: from Tank Levels to Plant Processes

Monday, 10 February 2020 12:15 (15 minutes)

Cyber security has been object of study since the beginning of the digital era. However, until the 2010 Stuxnet case in the Iran's enrichment facility at Natanz, most of world's cyber security concerns were directed to the theft of sensitivity information. Due to its specially designed attributes, Stuxnet is considered the first "weapons grade computer virus"[1] [2] [3].
After the Natanz attack, digital specialists - and countries - changed their attentions to digital attacks against real world physical systems, most of them aiming sabotage. Therefore, in the last few years, cyber defense exercises and training courses improvised simplified test beds with information technology (IT) and operational technology (OT) equipment. However, due to the complexity of nuclear power plants (NPP), the University of Sao Paulo (USP), under the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) Enhancing Computer Security Incident Response at Nuclear Facilities (J02008), has been developing a hardware-in-the-loop (HIL) simulator, the Asherah NPP Simulator (ANS). The ANS allows a better understanding of a cyber-attack facility impact. Besides that, a control room human-machine-interface (HMI) has been developed by the Tsinghua University and integrated with the ANS. This HMI aims to allow training exercises under the operator perspectives. Other institutes, like the Austrian Institute of Technology (AIT) and the University of Magdeburg have been integrating and developing anomaly detection tools using the ANS.
The CRP J02008 coordination led to the definition of three main roles: 1) System Builders; (2 Threat Modelers; and 3) Capability Providing Organizations [4]. USP, AIT and Tsinghua University are system builders. Capability providers and threat modellers organizations are developing threat model/scenario approach for research of test cases to mimic good computer security practices in regulatory regimes
Many OT simulators use industrial tank liquid level controllers as cyber security training tool. Tank level controllers are common to industries such as energy, oil & gas, chemical and metallurgy. These controllers maintain the level of boilers, condensers or pressurized tanks. They usually work by having a piece of software checking and adjusting the balance between inputs and outputs: digital controllers simulate pumps and valves that maintain the level between predefined values. Therefore, tank level controllers are the tools-of-choice to represent the effects of a cyber-attack in a real world equipment.
However, NPP are complex systems that must be represented by complex simulators. With the massive use of digital technology, NPP are becoming more tightly integrated. Even analogue legacy processes have been including digital systems that needed to be well-suited to cyber security challenges. Therefore, the ANS is the heart of a HIL test bed where real control equipment can be interfaced with the model to determine the consequences of sabotage from the exploitation of vulnerabilities resulting in loss of confidentiality, integrity and availability.
The CRP J02008 research activities are based on the premise that, usually, existing simulators do not survive or provide accurate results of the effects arising from simulated cyber-attacks; are not designed to account for cyber-attacks; do not capture the data needed for intensive computer security forensics and analysis; and they do not allow hardware/software integration for testing purposes. Therefore, preliminary research results suggest that going from tank levels to facility functions the development of computer security measures to prevent and protect against cyber-attacks on this equipment and systems.

REFERENCES

[1] Sklyar, V. Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities. Information & Security, Vol.28, No. 1, pp. 98-107, 2012.

[2] Stuxnet: Leaks or Lies? http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies. Accessed on May 12, 2019.

[3] Busquim e Silva, R.A.; Marques, A. L. F. Digital Instrumentation & Control (I&C) Systems and Cyber Security: Is Supply Chain the Weak Link? International Conference on Nuclear Security: Enhancing Global Efforts, Vienna-Austria, 2013.

[4] Rowland, M.T.; Busquim e Silva, RA. IAEA Coordinated Research Project on Enhancing Incident Response at Nuclear Facilities. 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies. Orlando-Florida, 2019.

State

Brazil

Gender

Male

Primary authors: Dr BUSQUIM E SILVA, Rodney Aparecido (Brazilian Governement); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Dr PAUL, Smith (AIT Austrian Institute of Technology GmbH); Mr HEWES, Mitchell (International Atomic Energy Agency); Mr PURVIS, Scott (International Atomic Energy Agency); Prof. LI, Jianghai (Tsinghua University.); Dr ALTSCHAFFEL, Robert (Otto-von-Guericke University of Magdeburg)

Presenter: Dr BUSQUIM E SILVA, Rodney Aparecido (Brazilian Governement)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

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