Contribution ID: **644** Type: **Paper**

Beyond the Tank Level: Simulator and Hardware-in-the-Loop Supported Training for Computer Security of Nuclear I&C

In 2016 the International Atomic Energy Agency (IAEA) launched a Coordinated Research Project (CRP) on Enhancing Computer Security Incident Analysis at Nuclear Facilities (J02008). The primary objective of this CRP was to contribute to the improvement of computer security capabilities at nuclear facilities to support the prevention and detection of, and response to, computer security incidents that have the potential to either directly or indirectly contribute to a nuclear security event which adversely affects nuclear safety, nuclear security, or Nuclear Material Accountancy and Control

The majority of research activities undertaken as part of the CRP were centred around the description, construction, and utilisation of the Asherah Hypothetical Facility. The Asherah facility extends a plant model simulation of a Pressurized Water Reactor with capabilities for hardware-in-the-loop (HIL) and virtualised Operational and Informational technologies to allow the exploration of threat scenarios for training, exercise, and the testing and qualification of defensive computer security measures postulated for use in nuclear facilities.

In parallel to the creation of the Asherah Hypothetical Facility the Division of Nuclear Security's Information and Computer Security Programme embarked on developing a series of flagship International Training Courses (ITC) to educate participants with a hands-on focused approach to the protection of digital Instrumentation and Control (I&C) systems used in Nuclear Facilities.

The first iteration of the flagship ITCs was run in partnership with the United States of America's Idaho National Laboratory (INL). As the Asherah hypothetical facility was still in early development the USA ITC utilised a number of exercises running on a mock-up Spent Fuel Pool Cooling (SFPCS). The spent fuel pool cooling system demonstrated a tank level control system able to convey a postulated attack where the water level lowered to a point that heat build-up from decay could no longer be successfully removed from irradiated fuel.

The second iteration of the flagship ITC, will be hosted in partnership with the Korean Institute of Nuclear Accountancy and Control's (KINAC) International Nuclear Security Academy (INSA). For its capstone exercise INSA will utilise the Asherah Hypothetical Facility providing educators the ability to teach concepts that go beyond a simple tank level system - providing experience to the participants in protecting the diverse set of interconnected and inter-reliant facility functions leveraged in real world nuclear instrumentation and control systems that everyday support, control, and contain nuclear processes. The simulation of the hypothetical facility will be augmented with a hardware in the loop physical mock-up of a condenser and condensate storage system interacting with the simulated plant processes.

This paper through exploration of the participant feedback recorded in both iterations of the flagship ITC will explore the evolution of learning outcomes derived from the use of the Asherah Hypothetical Facility and the provided impact on participant knowledge retention, concept appreciation, and the effect on the ability of the course to deliver on it's overarching terminal objective.

Gender

State

Authors: HEWES, Mitchell (IAEA); Dr SMITH, Paul (Austrian Institute of Technology); BUSQUIM E SILVA, Rodney Aparecido (Brazilian Governement); LI, Jianghai (Institute of Nuclear and New Energy Technology, Tsinghua University.); SONG, JAE-GU (Korea Atomic Energy Research Institute)

Presenter: HEWES, Mitchell (IAEA)

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