Contribution ID: **280** Type: **Paper**

Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment

Monday 10 February 2020 12:15 (15 minutes)

This work presents the development of a nuclear power plant (NPP) simulator suitable for cyber security assessment. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The Matlab/Simulink model, the Asherah NPP Simulator (ANS), simulates nuclear processes and controller' s system dynamics. ANS has been developed by the University of Sao Paulo, Brazil, under the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) Enhancing Computer Security Incident Response at Nuclear Facilities (J02008).

The ANS core design is based on a 2,772 MWt PWR Babcock & Wilcox (B&W), which is well known by several studies published after the Three Mile Island (TMI) Unit 1 accident [1]. The main NPP parameters may be found in the Nuclear Energy Agency/Organization for Economic Co-operation and Development (NEA/OECD) study [2]. The use of the TMI core facilitates the use of the previous developed RELAP/PARCS core model for benchmark, verification and validation activities [3] [4]. The ANS comprises the Nuclear Steam Supply System (NSSS): reactor core, pressurizer, reactor coolant pumps and u-tube steam generator (primary side); and the Balance of the Plant (BOP): u-tube steam generator (secondary side), turbine, generator, condenser, feed water system. The NSSS and BOP comprehends their subsystems'controllers where needed. Control logics used in real NPP have been implemented within software or hardware controllers.

The ANS can run standalone, i.e. within a computer or a virtual machine, or in a hardware-in-the-loop (HIL) distributed architecture test bed. It is the heart of a comprehensive simulation environment, the ANS Test Bed (ATB), with advanced instrumentation and control (I&C) capabilities. The ATB allows digital operational technology (OT) and information and technology (IT) researching and cyber security assessment.

ANS features include network connection by means of the open communication protocol Modbus and of the open cross-platform machine-to-machine OPC Unified Architecture (OPC-UA) protocol. The research team developed two ANS interfaces that allows communication among plant processes and any hardware embedded controllers or processes. The PROC I/O INTERFACE and the CTRL DATA INTERFACE are Matlab/Simulink drivers that send and receive signals to assigned equipment within the ATB. These interfaces may be user configured so any of the simulated subsystems can be replaced by their real counterparts. Therefore, the ANS processes and controllers'subsystems may be exchanged by programmatic logic controller (PLC), field programmable gate array (FPGA) or other real world physical equipment. Thus, specific sub systems, which perform dedicated safety or security functions within the plant, may be tested against cyber attack within the ATB. For example, the ANS integration capabilities include the exchange of the ANS pressurizer level controller by it is embedded real world physical counterpart within the ATB. Similar strategy can be applied to any controller or major process function.

Besides the ATB, a Configuration & Attack Terminal (CAT), integrated with the ANS, has been developing for attack initiation, data collection, data analysis and training purposes. The CAT preliminary cyber attack scenarios, implemented using the current ANS version, considered a model-based and hardware-based schemes. Besides I&C components, both preliminary schemes comprehend standard IT equipment. Exploratory results indicate that the ANS may be a valuable tool not only for digital research and cyber security assessment, but also for computer security measures development, training and information sharing.

REFERENCE

[1] U.S. Nuclear Regulatory Commission (NRC). 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] K.N. Ivanov 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] Busquim e Silva, R.A., "Implications of advanced computational methods for reactivity initiated accidents in nuclear reactors", University of Sao Paulo, PhD Thesis, 2015.

[4] 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.

Gender

Male

State

Brazil

Author: Dr BUSQUIM E SILVA, Rodney Aparecido (University of Sao Paulo,)

Co-authors: Dr SHIRVAN, Koroush (Massachusetts Institute of Technology); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo)

Presenter: Dr BUSQUIM E SILVA, Rodney Aparecido (University of Sao Paulo,)

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

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