Contribution ID: **294** Type: **Paper**

Development of Hardware-based Computer Security Controls for Advanced PWR Reactors

In advanced pressurized water reactors (PWR) as Korean APR-1400 and Russian VVER-1200, instrumentation and control (I&C) systems comprise of different data processing systems that utilize different network interconnections with different communication protocols. To provide data exchange between those several I&C systems, gateway devices play an important role in implementation of the I&C system of the plant in order to allow data transmission between different data systems based on different protocols. Currently, gateway devices, which are typically specific industrial computers, are incorporating software-based computer security functions to protect such data processing systems against potential cyber-attacks or intrusions which, if occurred, may disrupt the availability of such systems and/or integrity of data transmitted within the I&C systems and data networks. In 2016, IAEA introduced the application of field programmable gate arrays (FPGAs) in I&C systems of NPPs. FPGAs are hardware description language (HDL) programmable devices that have no processors or operating systems like that in computer-based (or software-based) systems such as programmable logic controllers (PLCs). FPGAs are being programmed by configuring its interconnections, which are typical digital logic circuits, so that the intended functions can be performed.

In this paper, hardware-based computer security controls, based on FPGA technology, are developed to perform computer security functions for protecting gateways devices. Although gateway devices are not safety-related systems, they provide, together with data diodes, a unidirectional data transmission from the safety side to the non-safety side of the plant main I&C system data networks. Such unidirectional data transmission should be maintained so that there is no data reversely transmitted back to the safety-related I&C systems. Plant parameters data is unidirectionally transmitted from the safety-related I&C systems to the gateway devices which collect and process such data and then forward it to the non-safety I&C systems. In addition, bi-directional data transmission and data acquisition existing between the gateway devices and non-safety I&C systems for the purpose of control and monitoring of the plant operation. Software-based computer security functions may be vulnerable to cyber-attacks or intrusions which, if occurred, may disrupt the availability of gateway devices causing failure of plant dynamic monitoring systems. FPGA-based computer security controls have the advantage of being software-free devices so that an insider or cyber-attacker will be unable to compromise or bypass its functions to initiate a malicious act against gateway devices. Typical FPGA-based computer security controls will be placed between the redundant safety channel gateway devices and non-safety I&C systems such as information processing systems. Such FPGA-based computer security controls are intended to function as data packet filter and malware scanner. Such computer security controls will similarly perform like a next generation firewall (NGFW) technology which combines traditional firewall function with other Ethernet data network filtering functionalities such as deep packet inspection (DPI), intrusion detection system (IDS) or intrusion prevention system (IPS).

The methodology of development such FPGA-based computer security controls functionalities are based on a digital comparator X-NOR logic gate circuit function where an input data will be compared with reference data. Reference data inputs will vary depending on the intended function. For data packet filtering, if a match exists between input data and reference data, it means a data packet is authorized to pass. For malware scanner, if a match exists, it means that malicious data is detected which may initiate a connection block to protect a gateway device against failure and being unavailable.

The intended FPGA-based computer security controls functionalities will be verified using synthesis HDL simulation tools. Further work is planned to develop a prototype of such computer security controls using a specific Ethernet type FPGA kit and then test it in an Ethernet-connected computer network environment lab.

Keywords: PWR; IC; computer security; FPGA

Gender

Male

State

Egypt

Author: Mr IBRAHIM, Ahmed Salah Mahmoud (Nuclear Power Plants Authority)

Presenter: Mr IBRAHIM, Ahmed Salah Mahmoud (Nuclear Power Plants Authority)

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