SIMULATOR OF SMALL MODULAR REACTOR FOR CYBER SECURITY ASSESSMENT

RODNEY BUSQUIM E SILVA
International Atomic Energy Agency
Vienna, Austria
r.busquim@iaea.org

MICHAEL T. ROWLAND
Sandia National Laboratories
Albuquerque, USA
mtrowla@sandia.gov

GUSTAVO BERMAN
Comisión Nacional de Energía Atómica (CNEA)
Bariloche, Argentina
tavo@cab.cnea.gov.ar

PAUL SMITH
Lancaster University
Lancaster, United Kingdom
paul.smith@lancaster.ac.uk

RICARDO PAULINO MARQUES
University of São Paulo
São Paulo, Brazil
ricardomarques@usp.br

Abstract

This work presents the framework and status of the development of a basic principle integrated pressurized water reactor (iPWR) small modular reactor (SMR) simulator designed to be an open-source tool to support computer security academic studies, capacity building activities, innovative SMR concept of operations, and digital instrumentation and control. This simulator aims to provide a test environment for integration and evaluation of novel and emerging digital technologies in the nuclear sector such as artificial intelligence, digital twins and smart sensors. Reference plant processes will be simulated to investigate the safety-security interface, show the application of the IAEA computer security guidance, demonstrate the effects of cyber-physical (blended attacks) and cyber-attacks, and reproduce the relevant digital communication channels and network protocols. The simulator has been developed using a modular framework to allow further integration of passive and inherent safety features or the replacement of the iPWR core by an advanced reactor core. Software (Docker) containers are used to simplify replication and deployment of the simulator. Ease of replication and deployment provides for quick instantiation of single or multi-unit reactor sites in different physical locations for analyzing the impact of a centralized fleet management, and its nuclear security implications. Results from simulation and analysis of a potential strategy of redundant and independent communication channels between remote supervision centers and local control systems are discussed here.

1. INTRODUCTION

In the last few years, the interest in the design, development and deployment of Small Modular Reactor (SMR) technologies has increased due to benefits such as passive safety, increased operational performance (e.g., reliability), and potentially cost-certainty based on pre-fabrication of critical structures, systems, and components. As SMRs are designed to generate up to 300 MWe with the ability to load-follow (i.e., adjust output depending on the electricity demand), they should be an important player for shifting the energy production away from sources of greenhouse gases.

Currently, there are more than 70 SMR designs under development [1]. These designs consider passive and advanced safety features, modular-design, and flexible operations (e.g., heat production, electricity, hydrogen production). The SMR technologies include advanced water-cooled reactors, a proven technology based primarily on the existing fleet of light and heavy water reactors, and advanced reactors such as high temperature gas cooled reactor, molten salt reactors and liquid metal cooled reactors. Among these options, the small integral pressurized water reactor (iPWR) seems to be the most likely to be the first to gain regulatory approvals in multiple jurisdictions. The iPWR differs from existing pressurized water reactors (PWR) in that its core contains the primary circuit systems.

The deployment and operation of SMRs will rely on advanced digital systems for innovative modes of operation, remote and autonomous operation, multi-unit or multi-module plants, and common control rooms and systems. Digital instrumentation and control (I&C) systems can enhance the efficiency of SMRs operation and maintenance through real time monitoring and prognostics. For example, providing alerts of a failure due to system malfunction or to a cyber-attack. Use of artificial intelligence and machine learning may identify improvements and increase plant performance. However, these new digital technologies may increase the potential for cyber-attacks.

2. INTEGRAL PRESSURIZED WATER REACTOR "ASHERAH" NUCLEAR SIMULATOR (IANS)

An integral pressurized water reactor contains the main primary circuit components inside the reactor vessel. The idea of developing a nuclear reactor with integral primary circuit is not new [2] and its first designs dates from the 1950's. The current iPWR designs also include safety passive features, modularity, and integrated design. In addition, iPWR featuring new operational modes, shared control rooms and systems, and that are tailored for deployment in remote areas with minimal on-site staffing will rely on advanced digital technologies.

In this scenario, specialized simulators designed for cyber security evaluation will play an important role. Therefore, by leveraging the Asherah Nuclear Power Plant Simulator (ANS) [3] systems architecture, the Asherah iPWR (iANS) simulator has been designed. This simulator is suitable for computer security assessment for both information and operational technologies, incorporating features tailored for small modular reactors.

The simulator provides hardware and software in the loop (HIL) capabilities. These capabilities include not only sensors and actuators elements, but also field control devices and process control. Examples of components that may be integrated are field-programmable gate array (FPGA) and programmable logic controllers (PLCs). The iANS communication infrastructure includes information technology systems such as routers and switches, TCP/IP Ethernet interfaces, and human machine interface (HMI) and local panel unit graphical user interface (GUI).

Moreover, the iANS core, consisting of the primary reactor cooling pumps, the steam generator, pressurizer and control rods are contained inside the reactor pressure vessel. The balance of the plant has been designed based on the existing systems in the nuclear industry such as condenser and turbines. This simulator presents an overview of the plant's behavior, with sufficient fidelity to demonstrate the impact of a cyber-attack in one of the operational technology systems. It provides access to the main reactor physical processes variables. The modularity of its components will allow users to test different SMR configurations. The passive systems being considered are a gravity driven water injection system, passive decay heat removal system, and protection control system. The iANS will automatically trip the turbine and the reactor in case of abnormal behavior.

The iANS has been designed to have three communication channels:

1) Process Input/Output (Proc I/O) channel for plant inputs and outputs such as selected sensor and actuator physical signals that normally would be transmitted through 4 mA–20 mA electrical loops.
2) Control Data (Ctrl Data) channel for simulating network communications, i.e., network traffic in a real system, among the supervisory system and process controllers, thereby representing the network traffic in a real system.

3) Operational Data (Op Data) channel for simulating network communications required by remote support centers for monitoring and supervising.

A general iPWR heat cycle [4] is shown in Figure 1.

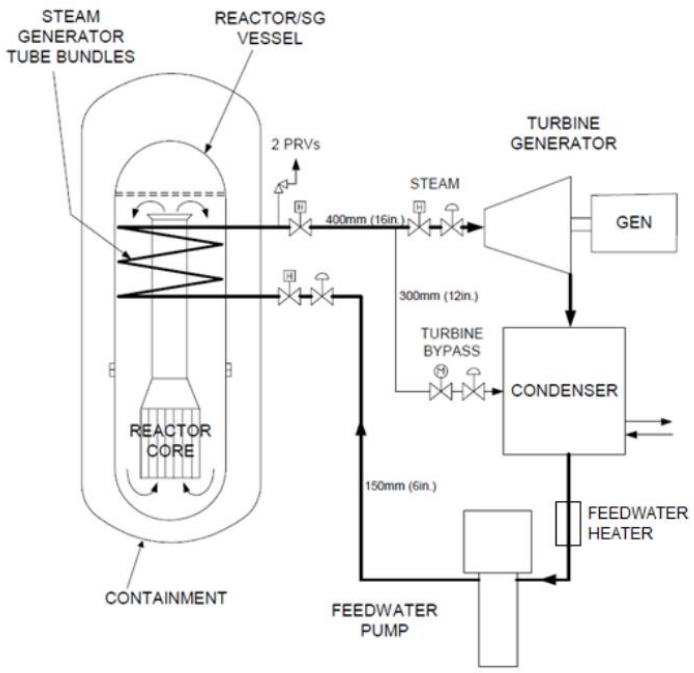

Figure 1 – iPWR water loop cycle

A key improvement of the iANS compared to the PWR Asherah NPP Simulator ("ANS") is the Operational Data (Op Data) channel, which should allow for exploration of remote monitoring and operation functions. This requires safe and secure communications channels that will not be in control of the operations all the time and assumes that inherent and passive safety features will not be compromised by cyber-attacks.

This Op Data channel allows for exchange of information about the plant process data, control system setpoint inputs, plant diagnostics and system health monitoring. In addition, it will allow investigation, from a cybersecurity perspective, of the supervisory control and data acquisition (SCADA) system that will play an important role connecting a remote location with a central command center. These features are related to diversity and redundance (availability), encryption (confidentiality), multiple layers of security in the physical, network and application layers (integrity). Important information, such as response times over long distances, performance of local and remote HMI and process historians, will be tested.

The modeling strategy includes separated modules for the following:

a) process control systems.
b) supervisory control system.
c) limitation system.
d) engineered safety feature actuation systems.
e) reactor protection system.

f) communication channels.

This approach enables or provides the following [5]:

1) Analysis of plant response to equipment and/or instrumentation failure due to cyber-attacks.
2) Analysis of impact to instrumentation and control of plant equipment and processes.
3) Core monitoring and radiation protection.
4) The use of software and hardware integration, including hardware-in-the-loop, for digital systems research.
5) Data acquisition support (useful for forensics analysis).
6) Computer security measure integration. This includes understanding the complexity of integrated network architectures which can aid the development, implementation, and assurance processes related to Defensive Computer Security Architectures (DCSA).
7) Support for the deployment of cyber-attack scenarios for "live fire" exercises.

Remote operation is a highly desired use case with notable economic implications for SMRs by enabling centralized control of multiple, geographically distributed reactor sites by a single organization. iANS will allow the investigation of centralized control and supervisory functions that could facilitate the operation of a fleet of standardized SMRs from a single control room. In addition, achieving remote operation requires substantial development in terms of communication frameworks, evaluation of secure protocols, cipher suites, flexible and agile DCSAs, and concurrent diverse and independent communication channels between remote operation centers and plant control systems.

Furthermore, reducing operator workload and errors may rely on visualization and decision support tools, potentially leading to increased automation or even autonomous operation of critical reactor components to provide operators with essential information for safe and secure plant operation. However, reliance on such tools would heighten operators' dependence on digital systems, consequently elevating computer security risks.

iANS has been developed with HMIs and interactive elements that are designed to enable monitoring, controlling and management of the SMRs operations. Through the HMI, a user would be able to access real-time data, adjust setpoints, and respond to alerts or alarms.

3. ADDRESSING APPLICATIONS FOR COMPUTER SECURITY OF SMR

The iANS simulator has been designed to allow the examination of scenarios that include features such as remote operation and maintenance, communication and control using advanced digital I&C systems, integration of advanced digital systems such as digital twins (DT) and artificial intelligence (AI)-based tools. This approach should be essential to implement and evaluate secure communication protocols.

The iANS will support the exploration of key areas relevant to both computer security and SMRs. For example, the communication between a centralized supervisory center and remote locations would require integration of data sources into a single unified architecture. iANS has been designed to exchange information using the OPC-UA data exchange standard IEC 62541 [6], which could address this issue. In addition, the simulator could allow the

research of data frameworks and offer insights into tools and technologies capable of streamlining the management of these SMR-related data structures.

Environments can be instantiated using multiple instances (i.e., “copies”) of iANS to investigate the cybersecurity risks associated with fleet management activities and operations. Potential risks that could be evaluated through use of these environments could be the disclosure of sensitive information during transmission over public networks or injection of unauthorized commands via remote masquerade attacks (i.e., adversary gains access to or control of an identity).

Environments could be adapted to replace OPC-UA communications with a variety of protocols. For example, Transport Layer Security (TLS) v1.3 could be leveraged within the simulator to secure communication between major endpoints of the control room and the reactor; however, a secure implementation requires server certificates and associated PKI infrastructure, requiring significant changes to OPC-UA and/or Op Data Channel. Alternatively, for these low-powered devices, the NIST-selected lightweight cryptography candidate ASCON [7] could be considered, as it already has referenced, optimized, and masked Assembly, Java, and C implementations publicly available. Extending iANS to investigate the viability of using these protocols and authenticated encryption with associated data (AEAD) cryptographic standards could ensure reliable operations, sufficient security, and enable remote operations and centralized fleet management.

The lack of robust security features in operational technology (OT) devices such programmable controllers, alongside the convergence of IT devices and protocols into OT systems, increases the potential for cyber-attacks. In this scenario, simulators offer the capability to generate logically coherent real-time data sets for supervisory systems, which are used to monitor and control real-world processes. This feature enables the evaluation of the potential facility impacts resulting from a cyber-attack on the simulated plant, including any cascading disruptions that may propagate across control systems, ultimately compromising operational integrity.

4. CONCLUSION

An integrated version of ANS (iANS), based on publicly available technical documents from the iPWR designs such as reference [8], holds significant potential for being equally valuable and potentially even more pertinent, given the characteristics of SMRs and their innovative operational modes. The proposed iANS design incorporates an Op Data channel serving as a communication channel for simulating network communications necessary for remote support centers involved in monitoring, maintenance, and supervision.

Computer security is a fundamental part of the design (i.e., cybersecurity by design) of advanced reactors, which provides a clear benefit that could enable remote access and management. However, the large number of reactors designs (iPWR, HTGR, Liquid Salt Cooled, Liquid Metal cooled, lead cooled) and the increased reliance on integration of digital technologies, will increase the demands on both designers and regulators. Simulators, and dynamic models, with analysis toolkits can reduce these demands through automation and enhanced visualizations of complex interactions and structure/filter of often excessive data volumes.

Computer security assurance activities, such as training and exercises, must account for the intricate relationship between safety and security inherent in OT systems. Leveraging simulated physical environments alongside virtual networks proves to be a potent strategy in tackling challenges specific to OT environments.

The proposed iPWR simulator has been developed to plug and play with analysis platforms to investigate cybersecurity and other design challenges. Finally, the development of iANS, a work in progress, could enable researchers, designers, and regulators to collaborate and share insights and approaches to optimize activities and improve outcomes that affect cybersecurity.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. Advances in Small Modular Reactors Technology Developments, IAEA Advanced Reactors Information System (ARIS), IAEA (2020).

[2] iPWR: Integral Pressurized Water Reactor https://www.ans.org/news/article-1915/ipwr-integral-pressurized-water-reactor/. Accessed on 29 February 2024.

[3] R. BUSQUIM E SILVA, J.R.C. PIQUEIRA, J.J. CRUZ, R.P. MARQUES. Cybersecurity Assessment Framework for Digital Interface Between Safety and Security at Nuclear Power Plants. International Journal of Critical Infrastructure Protection. Vol. 34 (2021).

[4] S. MODRO, S. MICHAEL et al. Multi-Application Small Light Water Reactor Final Report, Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, USA (2003).

[5] R. BUSQUIM E SILVA, M.T. ROWLAND, R.P. MARQUE. Evolution of the Asherah NPP Simulator Towards a SMR Cyber Assessment Tool. 2023 IAEA International Conference on Computer Security in the Nuclear World: Security for Safety.

[6] OPC UA Foundation. https://opcfoundation.org/. Accessed on 5 May 2024.

[7] National Institute of Standards and Technology. https://www.nist.gov/. Accessed on 5 May 2024.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY. Small Integral PWR Basic Principles Simulator, IAEA Specification (2015).