
Proceedings Paper:
Ahmed, A., Comert, M. and Ahmed, H. (2025) A hardware-in-the-loop framework for remote monitoring of safety critical systems. In: Peltonen, E., Hyrynsalmi, S., Wagner, I., Rellermeyer, J. and Mohan, N., (eds.) IoT '24: Proceedings of the 14th International Conference on the Internet of Things. IoT 2024: 14th International Conference on the Internet of Things, 19-22 Nov 2024, Oulu, Finland. ACM, pp. 279-284. ISBN: 9798400712852.

https://doi.org/10.1145/3703790.3703823

A Hardware-in-the-Loop Framework for Remote Monitoring of Safety Critical Systems

Arslan Ahmed
Nuclear AMRC
The University of Sheffield
Derby, United Kingdom
arslan.ahmed90@gmail.com

Mert Comert
Nuclear AMRC
The University of Sheffield
Rotherham, United Kingdom
m.comert@sheffield.ac.uk

Hafiz Ahmed
Nuclear AMRC
The University of Sheffield
Derby, United Kingdom
hafiz.ahmed@sheffield.ac.uk

Abstract

This paper presents a hardware-in-the-loop (HiL) testbed for remote monitoring of safety-critical systems. The testbed creates a secure environment for remote operations by establishing a communication link using open platform communication unified architecture (OPC-UA) industrial protocol resilient to cyber-attacks. The testbed uses a hypothetical Asherah nuclear power plant (Asherah NPP) by incorporating its physics, control systems, instrumentation, and communication networks to be controlled by a remote controller device, a Siemens S7 1500 programmable logic controller (PLC). The HIL capabilities of the testbed allow real-time assessment of industrial communication networks by integrating hardware, simulating data flow with malicious scripts, and identifying vulnerabilities. The testbed is particularly useful for predictive maintenance procedures and efficient operation of nuclear power plants, ultimately improving the cybersecurity of instrumentation and control systems in safety-critical applications. An internet of things (IoT)-based framework of the proposed HiL testbed for remote monitoring of safety critical systems has also been proposed at the end of the paper.

Keywords

Nuclear Power Plant, Hardware-in-the-Loop, Remote Monitoring, IoT, Safety Critical Systems, Instrumentation and Control, Industrial Communication.

ACM Reference Format:
Arslan Ahmed, Mert Comert, and Hafiz Ahmed. 2024. A Hardware-in-the-Loop Framework for Remote Monitoring of Safety Critical Systems. In *14th International Conference on the Internet of Things (IoT 2024), November 19–22, 2024, Oulu, Finland*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3703790.3703823

1 Introduction

Safety critical systems (such as the nuclear power plants) are subject to stringent regulations and safety standards due to the potential risks associated with their operations [2, 3, 10, 12]. These facilities must adhere to rigorous inspection and safety processes to mitigate the likelihood of severe accidents [13, 14]. To address this challenge, the IAEA through its Nuclear energy series has published several reports on on-line monitoring of the nuclear power plants for improved performance, good engineering and management practices which are suggested by its Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI) in 2003 [11]. A well-designed interface between operators and plant systems can enhance overall safety and operational efficiency because human supervision alone is prone to errors and inefficiencies. In this regard, an online monitoring of these systems can play a vital role to improve performance, condition monitoring, diagnostics, and further to adopt predictive maintenance procedures by involving hardware-in-the-loop (HIL). An efficient interface between humans and machines through the human-machine interface (HMI) can be crucial for preventing human errors and for assisting operators in managing unforeseen events effectively before they become big problems, keeping the plant running smoothly [8, 9].

This paper addresses the previously mentioned issues by developing a hardware-in-the-loop testbed for remote monitoring of safety critical systems. The main purpose of this testbed is to adopt a safe environment for remote operations by establishing a secure communication link resilient to cyber-attacks [1, 4]. To achieve this, a dynamic testing environment has been created having the physics, control systems, instrumentation, and communication networks of a pressurized water reactor (PWR). The PWR is the safety critical system which replicates a simulated version of a hypothetical nuclear reactor. The PWR used here is the Asherah nuclear power plant (Asherah NPP) simulator [7]. The hardware-in-the-loop capabilities of the testbed will facilitate real-time assessment of industrial communication networks. This will involve integrating hardware devices, simulating data flow, and assessing the vulnerabilities introduced by these devices in real-time. Utilizing an innovative and customized control-oriented model, the proposed testbed aims to enhance the cybersecurity risk assessment of PWR instrumentation and control systems by proactively identifying and addressing potential vulnerabilities or cybersecurity concerns [6]. For this purpose, the project uses an industrial standard communication protocol (e.g., OPC-UA) [16], ensuring the safety and reliability of remote operations through a secure link (wireless/wired) to enable safe predictive maintenance procedures and efficient operation of nuclear power plants.

The paper is organized as follows: Section 2 discusses the methodology used to implement the framework of the HIL architecture for remote monitoring; section 3 discusses the physical implementation of the proposed architecture given in section 2 and also presents the experimental set-up and the results; section 4 presents a case for the IoT implementation of the proposed HIL testbed. Finally, section 5 concludes this paper.

IoT 2024, November 19–22, 2024, Oulu, Finland

ACM ISBN 979-8-4007-1285-2/24/11
https://doi.org/10.1145/3703790.3703823

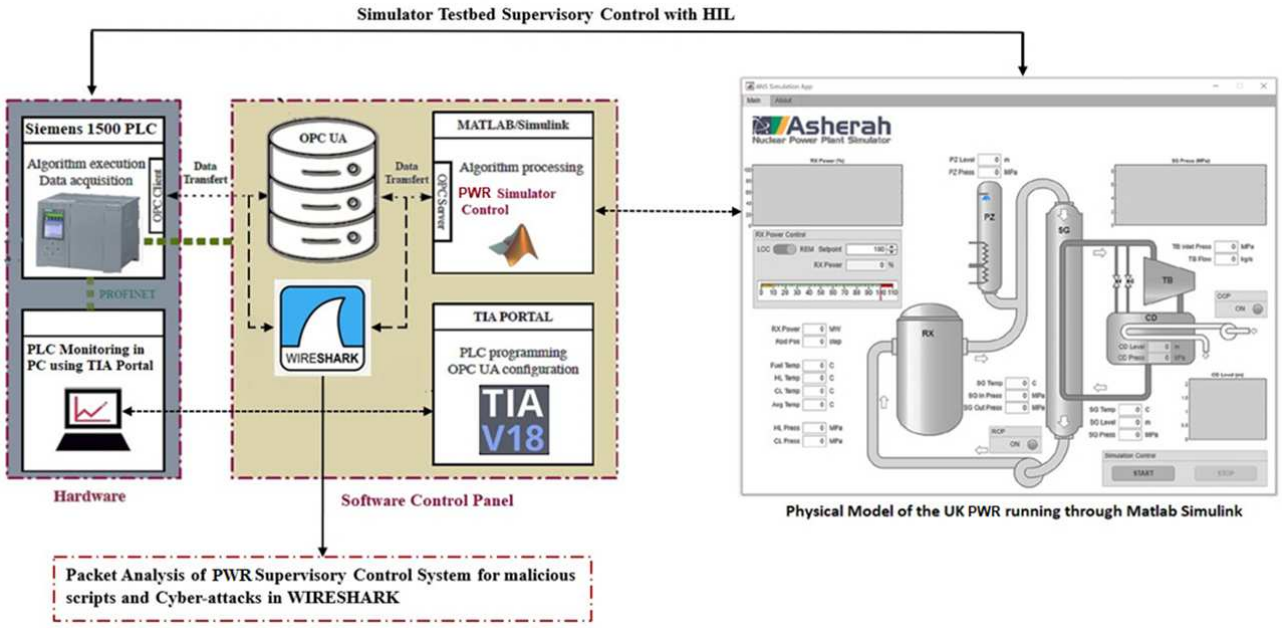

Figure 1: Architecture of HiL framework for remote monitoring of safety critical systems (Asherah NPP Simulator). The Siemens S7 1500 PLC is the remote controller device.

2 Methodology

The open platform communication unified architecture (OPC-UA) protocol is a widely adopted industrial communication protocol that can enable supervisory control for different devices, systems, and applications in the industrial automation domain [5, 15]. Establishing OPC UA communication involves setting up a server and a client to enable data exchange between them. In the proposed HIL testbed, the Asherah nuclear simulator (ANS) serves as a OPC-UA server for communication with the Siemens S7 1500 PLC client to incorporate the supervisory control with the HIL. The ANS frontend is run and controlled by MATLAB Simulink. To analyze any malicious activity between the ANS and the S7 1500 PLC communication link, the Wireshark is used to observe network traffic. The framework of the proposed HIL testbed is shown in Fig. 1.

The functions of the testbed is divided into three components; the hardware part - which consists of the Siemens S7 1500 PLC and the PC running all the necessary software; the software control panel - which consists of the OPC-UA link between the PLC and Asherah NPP simulator, the Wireshark which is analyzing the packet communication between the PLC and the ANS, the TIA portal V18 which is used to program the PLC and, the MATLAB/Simulink environment on which ANS is running; the Asherah NPP simulator - which mimic a safety critical system and on which the supervisory control is to be implemented through a remote controller device (Siemens S7 1500 PLC).

The steps followed to establish the OPC-UA communication between the client (siemens PLC) and server (Asherah NPP simulator) for supervisory control are:

- `Setting Up OPC-UA Server`: The variables in the ANS are configured to make them available to OPC-UA clients. Security settings such as certificates, user authentication, and access control policies are defined in the OPC-UA server to access the OPC UA client.
- `Configuring OPC-UA Client`: OPC-UA protocol is activated in the Siemens S7 1500 PLC to serve as a client. The S7 1500 PLC is configured to connect to the OPC-UA server using the server's endpoint URL.
- `OPC-UA server and client end-to-end encryption`: Connection is established through the OPC-UA server's endpoint URL which is used in the client. The connection is authenticated using the appropriate credentials and settings to make sure that it is prone to cyber-attacks.
- `Browsing and Accessing Data`: Once the connection is established, the OPC-UA client can browse the server's address space to discover available nodes (variables).

The overall process can be summarized as follows: The simulated version of the ANS gather data from various sources within the plant, including sensors, control systems, and other equipment. OPC-UA enables bidirectional communication, allowing the simulator to not only collect data but also send control commands to various plant components. OPC-UA incorporates robust security features such as encryption, authentication, and access control mechanisms. This ensures that sensitive data remains confidential and that only authorized users can access and control the simulator components. This facilitates real-time monitoring and control of plant operations within the simulator environment by involving HiL which is an S7 1500 PLC in our case.

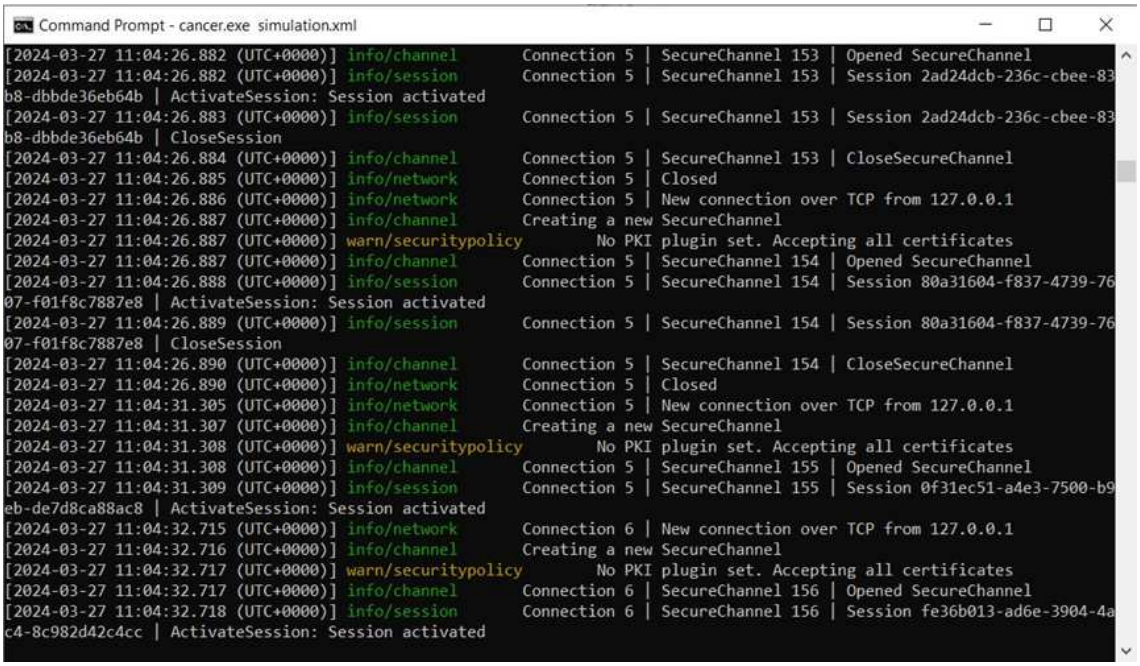

Figure 2: Setting up of OPC-UA communication link in ANS at IP address 127.0.0.1 and port no 53530.

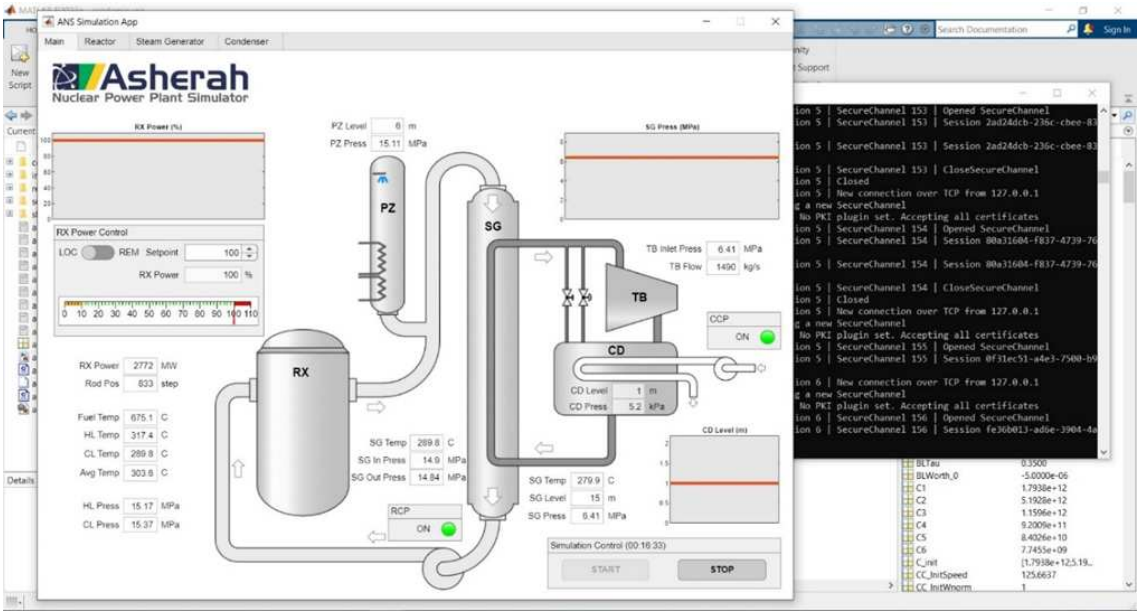

Figure 3: Front-end of the ANS (PWR-type).

3 Experimental Set-up and Results

This section experiments with the physical HiL testbed using a hardware S7 1500 PLC to validate the working of the proposed architecture shown in Fig. 1. First, the OPC-UA communication has been initialized in the Asherah NPP simulator (ANS) by establishing a connection over IP address 127.0.0.1 and using port 53530 as shown in Fig. 2. The ANS will now serve as an OPC UA server and will communicate with any client over the aforementioned IP address and port. Once, the OPC-UA communication has been initialized, the ANS front-end GUI is then started in MATLAB environment as shown in Fig. 3. This ANS front-end shows a simple PWR with reactor core marked as Rx, pressurizer PZ, steam generator SG, Turbine TB and condenser CD. The Rx values in the GUI

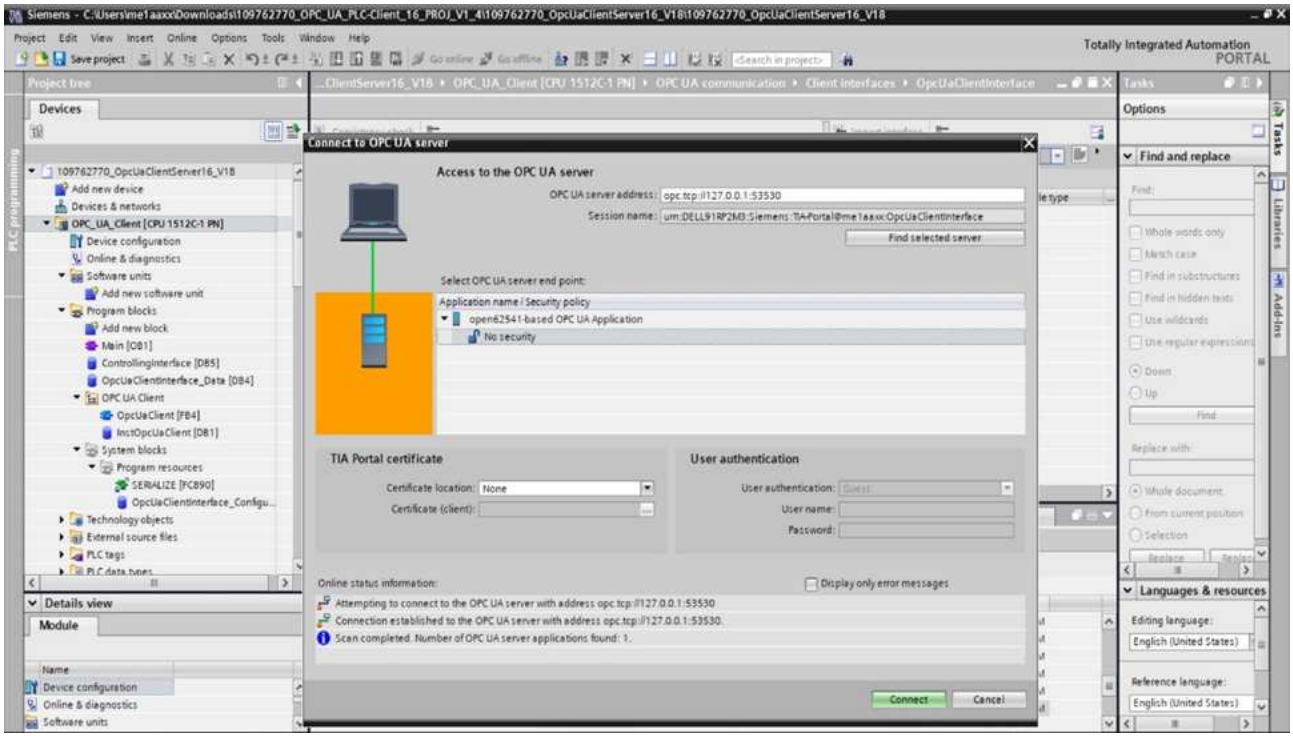

Figure 4: Connection setup between the OPC-UA client (S7 PLC) and OPC-UA server (ANS).

Figure 5: Siemens S7 1500 PLC connection set-up on the PC through ethernet cable.

can be used to control the generated power MW. Changing the Rx power level will also change all the other parameter values in the plant such as the temperatures, control rod positions, flow, steam generated etc.

The next step is to set-up the supervisory control through HiL to control the simulator parameters. This is done by using a Siemens S7 1500 PLC which is used as a remote controller device. The PLC is programmed through TIA portal v18 which will establish OPC-UA communication between the PLC and the Asherah NPP Simulator (ANS) and, retrieve the simulation parameters from the ANS into the TIA portal which are then controlled by the PLC. The PLC is connected to the PC through an ethernet cable. The PLC has already been configured in the TIA portal to act as an OPC UA client. Fig. 5 shows the overall physical testbed model having Siemens S7 1500 PLC as an HiL component and ANS as a safety critical system.

At this point, the ANS has been initialized as an OPC-UA server and the S7 1500 PLC is set as an OPC-UA client. A successful OPC-UA connection is then established between the server and client through the TIA portal over the IP address 127.0.0.1 and port 53530 as shown in Fig. 4.

The ANS simulation parameters are then accessed through TIA portal as shown in Fig. 6. This window in the TIA portal which shows both the server interface and client interface is used to set the plant values (e.g., Rx power, control rods, plant power, pump flow, pump inlet temperature etc) from the client side (S7 1500 PLC) to initiate the supervisory control. Initially, to check the validity of the HiL testbed for remote monitoring, some ANS parameters were controlled through the PLC such as the generated power and temperatures and the plant was also shut down using the PLC controller. All these operations were successfully implemented using the PLC to implement remote control operations.

4 An IoT implementation for the proposed HiL framework

The industrial internet of things (IoT) involves applying IoT technology in industrial environments, focusing on the instrumentation and control of sensors and devices that interact with cloud-based systems. The digitalization of nuclear control and instrumentation through IoT can enhance plant performance and cost efficiency, but it may also introduce cybersecurity risks. The proposed HiL framework in Fig. 1 is implemented over an ethernet connection where

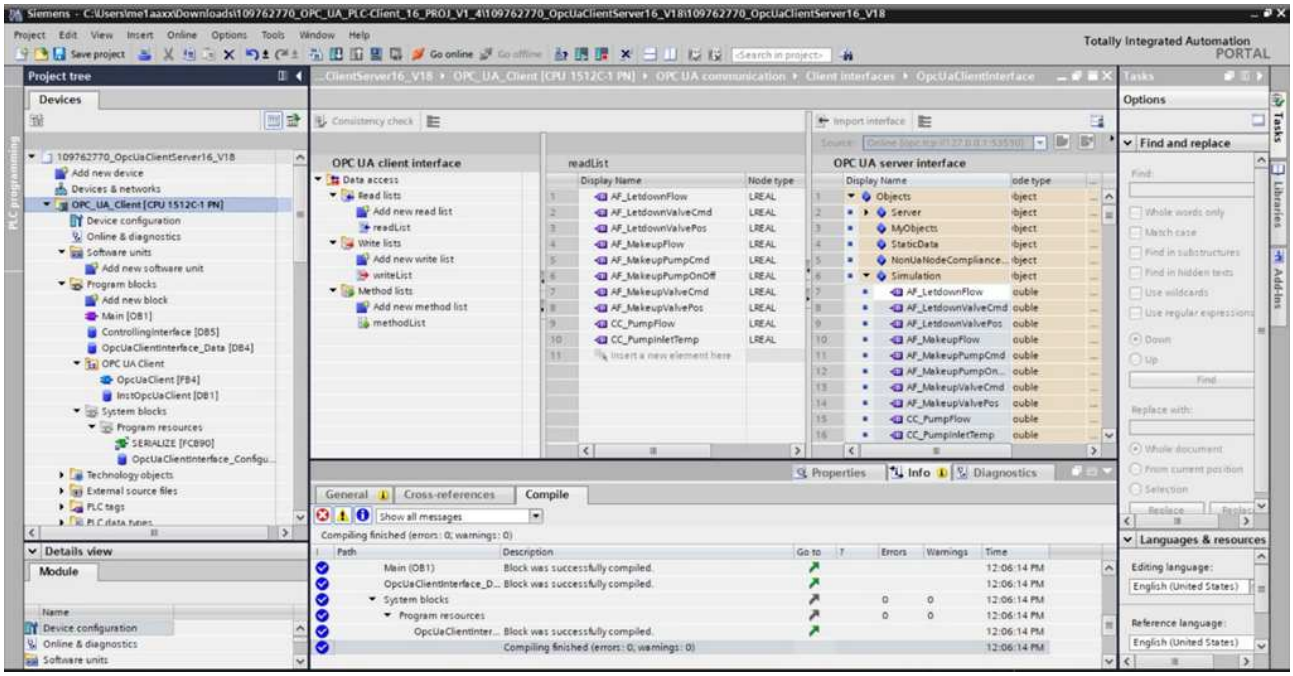

Figure 6: Supervisory control for the ANS SMR implemented through TIA portal with Siemens S7 1500 PLC as the remote controller device.

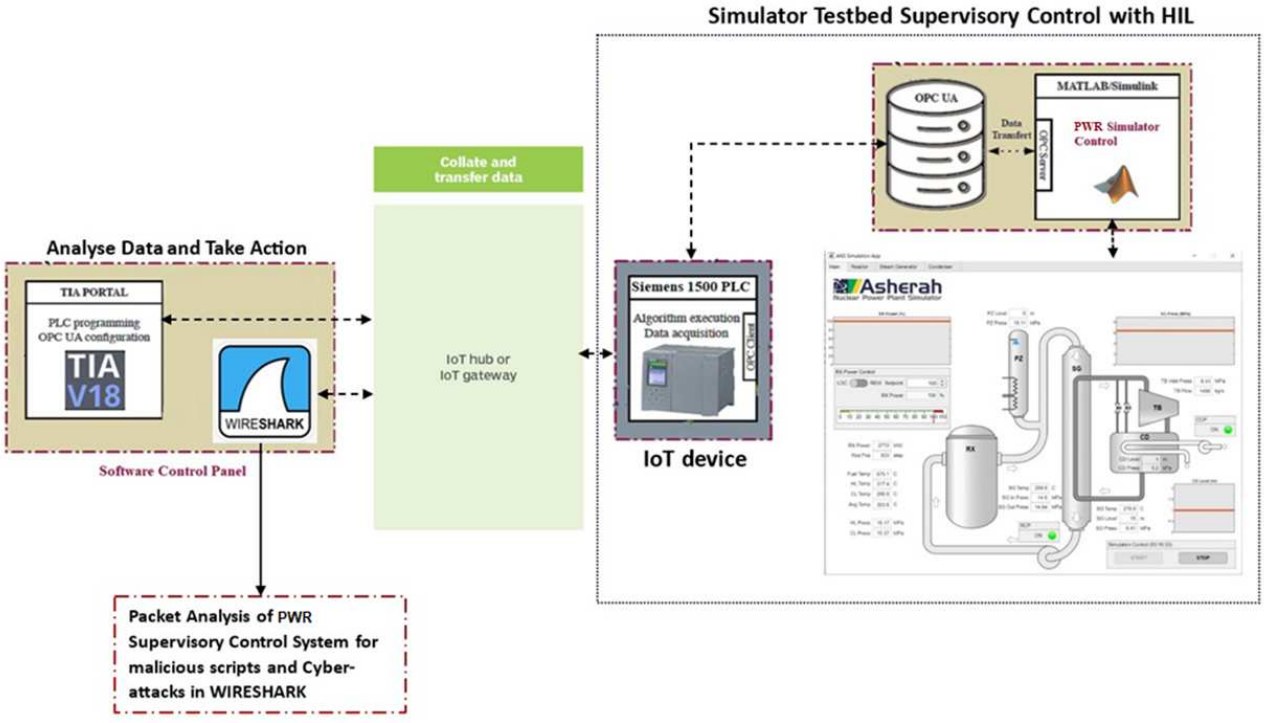

Figure 7: An IoT implementation of the testbed for remote monitoring of safety critical systems with HiL.

the data has been transferred to the remote controller device (S7 1500 PLC) however, the same framework can easily be transformed into an IoT system using a wireless/internet connection through a switch or modem which can be used as an IoT gateway for transferring data between the IoT enabled remote controller device and the user interface. To implement the HiL testbed in Fig. 1 through IoT, a proposed framework is shown in Fig. 7. In this figure, the simulated model of a PWR (Asherah NPP simulator) is connected to the Siemens S7 1500 PLC over an OPC-UA communication protocol.

It should be noted, since we are using a simulated version of a PWR, so it is running in MATLAB environment. In the real-world scenario, it can be replaced by an actual plant. The Siemens S7 1500 PLC is the IoT enabled device which takes control of the plant operations by communicating over the OPC-UA protocol. The IoT device is then connected to an IoT hub or gateway, which can be a modem and established wireless connection with the IoT device. The IoT hub then transfers the data to the software control panel, which acts accordingly by changing any plant parameter or shutting it down based on the data received over the IoT hub/gateway device. However, the proposed IoT set-up of the HiL testbed will be vulnerable to cyber-attacks. To establish robust cyber defenses for critical digital assets in nuclear facilities, a comprehensive assessment of potential threats and vulnerabilities across systems, networks, and devices is essential. In order to assess the cyber security threats for a possible presence of any suspicious/malicious script, Wireshark in the software control panel can be used as an analysis tool.

5 Conclusion

An HiL testbed for remote monitoring of safety critical systems is presented in this paper. The remote monitoring of these systems through HiL can be critical for digitalization as HiL allows realtime assessment of the plant's operations which can be useful for predictive maintenance and can reduce human errors. The OPC-UA industrial protocol used in this paper for the assessment of HiL testbed can be useful for safe operations of these plants and can reduce cyber security threats. An IoT architecture of the proposed testbed has also been discussed in the paper, which can set future directions for possible implementation of the proposed testbed through using industrial IoT devices.

Acknowledgments

This work is supported by the CHIST-ERA funded TROCI Project (CHIST-ERA-22-SPiDDS-07) through the UK's Engineering and Physical Sciences Research Council (EPSRC) under grant EP/Y036344/1.

References

[1] Brian Aamoth, William E. Lee, and Hafiz Ahmed. 2022. Net-Zero Through Small Modular Reactors - Cybersecurity Considerations. In *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*. 1–5. https://doi.org/10.1109/IECON49645.2022.9968304

[2] Saif Ahmad, Kamal Kayode Abdulraheem, Andrei Olegovich Tolokonsky, and Hafiz Ahmed. 2023. Active disturbance rejection control of pressurized water reactor. *Annals of Nuclear Energy* 189 (2023), 109845.

[3] Abiodun Ayodeji, Antonio Di Buono, Iestyn Pierce, and Hafiz Ahmed. 2024. Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system. *Nuclear Engineering and Design* 424 (2024), 113277.

[4] Abiodun Ayodeji, Mokhtar Mohamed, Li Li, Antonio Di Buono, Iestyn Pierce, and Hafiz Ahmed. 2023. Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. *Progress in Nuclear Energy* 161 (July 2023), 104738. https://doi.org/10.1016/j.pnucene.2023.104738

[5] Jonathan Tobias Da Silva, Andre Luis Dias, and Ivan Nunes Da Silva. 2023. A Survey on OPC UA Protocol: Overview, Challenges and Opportunities. In *2023 15th IEEE International Conference on Industry Applications (INDUSCON)*. 1523–1530. https://doi.org/10.1109/INDUSCON58041.2023.10375053

[6] R. A. B. e Silva, J.R.C. Piqueira, J.J. Cruz, and R.P. Marques. 2021. Cybersecurity Assessment Framework for Digital Interface Between Safety and Security at Nuclear Power Plants. *International Journal of Critical Infrastructure Protection* 34 (Sept. 2021), 100453. https://doi.org/10.1016/j.ijcip.2021.100453

[7] R. A. B. e Silva, Koroush Shirvan, José Roberto Castilho Piqueira, Ricardo Paulino Marques, et al. 2020. Development of the Asherah nuclear power plant simulator for cyber security assessment. In *Proceedings of the International Conference on Nuclear Security, Vienna, Austria*. 10–14.

[8] P.F. Fantoni, M.I. Hoffmann, R. Shankar, and E.L. Davis. 2003. On-line monitoring of instrument channel performance in nuclear power plant using PEANO. *Progress in Nuclear Energy* 43, 1–4 (2003), 83–89. https://doi.org/10.1016/s0149-1970(03)00017-9

[9] H.M. Hashemian. 2011. On-line monitoring applications in nuclear power plants. *Progress in Nuclear Energy* 53, 2 (March 2011), 167–181. https://doi.org/10.1016/j.pnucene.2010.08.003

[10] Thomas Hilburn and Janusz Zalewski. 1995. Real-Time Safety-Critical Systems: An Overview. *IFAC Proceedings Volumes* 28, 25 (Nov. 1995), 127–138. https://doi.org/10.1016/s1474-6670(17)44835-x

[11] International Atomic Eenergy Agency. 2008. *On-line Monitoring for Improving Performance of Nuclear Power Plants Part 1: Instrument Channel Monitoring*. Number NP-T-1.1 in IAEA Nuclear Energy Series. Vienna. https://www.iaea.org/publications/7790/on-line-monitoring-for-improving-performance-of-nuclear-power-plants-part-1-instrument-channel-monitoring

[12] John C. Knight. 2002. Safety critical systems: challenges and directions. In *Proceedings of the 24th international conference on Software engineering - ICSE '02 (ICSE '02)*. ACM Press, 547. https://doi.org/10.1145/581339.581406

[13] Pramod Kumar, Lalit Kumar Singh, and Chiranjeev Kumar. 2020. Performance evaluation of safety-critical systems of nuclear power plant systems. *Nuclear Engineering and Technology* 52, 3 (March 2020), 560–567. https://doi.org/10.1016/j.net.2019.08.018

[14] Nand Kumar Jyotish, Lalit Kumar Singh, and Chiranjeev Kumar. 2023. Reliability Assessment of Safety-Critical Systems of Nuclear Power Plant using Ordinary Differential Equations and Reachability Graph. *Nuclear Engineering and Design* 412 (Oct. 2023), 112469. https://doi.org/10.1016/j.nucengdes.2023.112469

[15] Santhana Pandiyan Muniraj and Xun Xu. 2021. An Implementation of OPC UA for Machine-to-Machine Communications in a Smart Factory. *Procedia Manufacturing* 53 (2021), 52–58. https://doi.org/10.1016/j.promfg.2021.06.009

[16] Santosh Kumar Panda, Mainak Majumder, Lukasz Wisniewski, and Jurgen Jasperneite. 2020. Real-time Industrial Communication by using OPC UA Field Level Communication. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vol. 1. 1143–1146. https://doi.org/10.1109/ETFA46521.2020.9211998