ADVANCEMENTS IN HARDENING THE CYBERSECURITY POSTURE OF NUCLEAR POWER PLANT DEFENCE-IN-DEPTH NETWORK ARCHITECTURE

C. NEAL
Polytechnique Montreal
Montreal, Canada
Email: christopher.neal@polymtl.ca

D. TRASK
Canadian Nuclear Laboratories
Fredericton, Canada
Email: dave.trask@cnl.ca

K. THIYAGARAJAN
Canadian Nuclear Laboratories
Fredericton, Canada
Email: karthik.thiyagarajan@cnl.ca

R. DOUCET
Canadian Nuclear Laboratories
Fredericton, Canada
Email: richard.doucet@cnl.ca

P. ADAMSON
Canadian Nuclear Laboratories
Fredericton, Canada
Email: peter.adamson@cnl.ca

M. DALEY
Canadian Nuclear Laboratories
Fredericton, Canada
Email: matthew.daley@cnl.ca

J. FERNANDEZ
Polytechnique Montreal
Montreal, Canada
Email: jose.fernandez@polymtl.ca

Abstract

Digital technologies are increasingly being used within Nuclear Power Plant (NPP) facilities, replacing original analog systems as older plants are upgraded or as part of largely all digital designs in new builds. This brings tremendous advantages to operating organizations including increasing the availability of data for decision making purposes and decreasing of costs and reductions to inefficiencies. However, the increasing level of digitization also increases the attack surface that could be exploited by cyber-capable adversaries. This paper provides an overview of the research efforts being conducted by Canadian Nuclear Laboratories (CNL) through its National Innovation Centre for Cyber Security (NICCS) in developing best practices and guidance on cybersecurity for NPP facilities and other critical infrastructure. Through the participation in the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008, entitled “Enhancing Computer Security Incident Analysis at Nuclear Facilities,” CNL’s NICCS has developed a Hardware-in-the-Loop (HIL) cyber range which simulates the physical processes of a Boiler Level Control (BLC) system along with its supporting computer networks. This cyber range provides an arena to analyze the effects of various cyberattacks against NPP physical processes and to experiment with incident response and detection techniques. This paper demonstrates the utility of such a cyber range in assessing the overall defensive posture of NPP against potential cyberattacks.

1. INTRODUCTION

Organizations increasingly depend up digital-based technologies for the reliable operation of Nuclear Power Plant (NPP) facilities through a myriad of Information Technology (IT) and Operational Technology (OT) systems. This enables the automation of industrial processes and heightens the exchange of information, while also providing the means for the business units to conduct their day-to-day tasks. This has numerous advantages; however, it also increases the attack surface which can be exploited by potential cyber-capable adversaries [1]. This paper presents the cybersecurity challenges behind protecting the various computer networks used to operate a Nuclear Power Plant (NPP) and an overview of the progress achieved at Canadian Nuclear Laboratories (CNL) and its National Innovation Centre for Cyber Security (NICCS) to combat this growing concern.

Computer networks, whether physically connected or wireless, are the core of all digital communications and processes within an NPP. These networks relay sensor values and control commands amongst digital devices as well provide a means to provide information to human operators. To protect these computer networks the International Atomic Energy Association (IAEA) considers a defensive computer security architecture (DCSA) known as the *Defence-in-Depth Architecture* [2]. In this paradigm, computer networks and control systems are strategically deployed through layers of securely defined levels and zones. The intention is to shield mission critical NPP processes from a cyber-intrusion by restricting the communications between the different levels and zones. This architecture provides the backbone for NPP network security, however as attacker capabilities continue to evolve, there is ongoing demand to find new innovations to protect NPP's computer network infrastructure.

On this front, CNL's NICCS has developed a cyber range with a reference DCSA that mimics the segmented computer networks typically found in an actual NPP facility. Uniquely, this cyber range models some of the physical processes of an operating NPP, specifically those processes related to the Boiler Level Control (BLC) system, using a Hardware-in-the-Loop (HIL) design.

The BLC model, which was developed as part of the NICCS' contribution to the IAEA Collaborative Research Project (CRP) J02008, entitled "Enhancing Computer Security Incident Analysis at Nuclear Facilities," integrates the HIL components with a software simulation of a Pressurized Water Reactor (PWR) in a feedback loop. With this experimental setup, cyberattacks can be conducted against the controllers managing the BLC processes, allowing the physical impacts of cyberattacks to be measured in real-time. This cyber range provides a venue to develop cyber-intrusion Anomaly Detection (AD) techniques and test the behaviour of digital devices under the presence of various cyberattacks. The capstone of IAEA CRP J02008 was an IAEA Agency Mission in July 2019 hosted by CNL at the NICCS in Fredericton, New Brunswick, Canada, where various cyberattack scenarios were carried out using the cyber range. These exercises provide a baseline for various cyber-threat detection mechanisms and are discussed in this paper.

The remainder of the paper is structured as follows. Section 2 provides an overview of the cybersecurity challenges faced when operating an NPP. Section 3 discusses the BLC cyber range. A description of the cyberattack scenarios conducted during the IAEA Agency Mission in July 2019 is discussed in Section 4. Lastly, Section 5 is a conclusion to the paper highlighting some suggestions for NPP cybersecurity defences and outlines future areas of research for data-enhanced cybersecurity of NPP processes.

2. NUCLEAR POWER PLANT CYBERSECURITY OVERVIEW

Cybersecurity is becoming an increasing concern for NPP facilities. Other critical infrastructures have come under attack with notable examples being the Stuxnet attack against Iranian uranium enrichment facilities in 2010 and the Triton malware infection against Triconex safety controllers in a Saudi Arabian petrochemical plant in 2017 [3]. A successful cyber-attack against an operating NPP could result in a loss of intellectual property as well as significant operational losses as the facility owners would need to demonstrate to their national regulator that the incident has been fully resolved and that the plant is safe to restart and begin normal operations. In addition, a successful cyberattack on an NPP could undermine the public's confidence in these facilities. This section provides an overview of how industrial processes controlled by digital components are susceptible to a cyberattack, how this is mitigated through Defence-in-Depth Architecture, and some of the threats facing an NPP.

2.1. Process Control in a Pressurized Water Reactor Nuclear Power Plant

An PWR NPP is an example of an Industrial Control System (ICS), where multiple physical processes are controlled and monitored using digital devices. To provide context, an overview of these processes is provided in Figure 1.

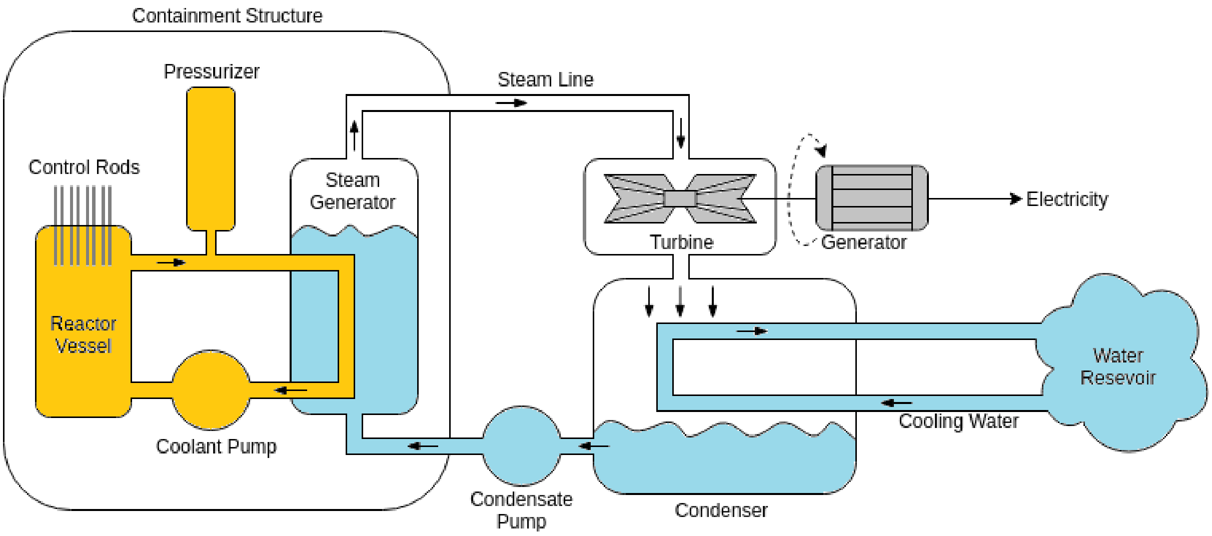

FIG. 1. Overview of a Pressurized Water Reactor

The process of fission occurs in the reactor vessel through the splitting of uranium atoms and is used to heat up water. The pressurizer keeps the heated water under pressure to prevent the water from boiling. The heated water is piped to the steam generator and is used to heat up water in a large boiler. The water in the steam generator evaporates into steam and travels through the steam line and is used to drive a turbine. The driving of the turbine is used to create electricity at the generator. The steam that drives the turbine is cooled into water in the condenser and is pumped to the steam generator to be reused [4].

These processes are automated using a variety of digital OT systems to invoke control over physical devices, such as switches and valves. OT refers to the hardware, software, and communications protocols used for the monitoring as well as controlling of industrial processes. In general, there are process values reported by sensors and control actions are invoked to drive the process towards some ideal setpoints. OT systems comprise things such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and communications protocols such as Modbus or OPCUA.

Traditionally, OT systems operated on isolated computer networks and cybersecurity was not a concern. With this perceived *air gap*, OT systems were not designed with security mechanism (e.g. authentication, cryptography) and the focus was on performance. However, with advancements in computational capabilities coupled with the increased complexity of ICS processes, OT systems have been increasingly integrated with traditional IT systems to support operations. There is now increased concern for protecting mission critical NPP processes from the possibility of cyberthreats [5, 6].

2.2. Defence-in-Depth Network Architecture

The Defence-in-Depth architecture is an approach recommended by the IAEA to partition an NPP organization’s computational infrastructure in levels of criticality amongst logical divisions with varying levels of access [2]. The levels range from 1 to 5, based on the severity of compromise to the overall operation of an NPP. Level 1 is the most critical with the most restrictive access, while Level 5 is the most open. An overview of these levels is provided in Figure 2:

— Level 1: Reactor Protection Systems

- Reactor control and safety systems
- No network connectivity
- No remote connections

— Level 2: Operational Control Systems

- Process control and safety systems
- Limited one-way connectivity from Level 2 to 3
- No remote connections

— Level 3: Real Time Supervision Systems

- Non-safety related controllers and engineering workstations
- Limited two-way connectivity between Level 3 and 4
- Remote connections on a case-by-case basis

— Level 4: Technical Data Management Systems

- Work management and configuration management systems
- Limited two-way connectivity between Level 4 and 5
- Remote connections for predefined workflows

— Level 5: Business Supporting Systems

- Business management systems, e-mail servers, and public website
- Connectivity to the Internet
- Remote connections and third-party access

FIG 2. IAEA DSCA Levels

To ensure these logical boundaries are adhered to, technical controls such as boundary protection devices (e.g. firewalls, data diodes) are used to control the flow of communications. Technical controls are augmented with operational controls such as restricting physical access to systems based on work function and authorization, enforcing a two-person rule when performing work in high security levels, and portable media and device management controls in order to prevent malware from being introduced through that attack pathway.

Security levels can further be segmented into zones in order to distinguish between different process functions. For example, in Level 2, the steam generation process is in a separate zone than the pressurizer and there is limited connectivity between the two processes. This subsection is by no means an exhaustive description of the Defence-in-Depth architecture paradigm, rather it is meant to provide the reader with the intuition for the need for such an approach and some of the safeguards that should be in place.

2.3. Threat Model

For an NPP organization, the viable attack vectors will vary depending upon the overall defensive posture of the computer systems and the training of the staff. Threat actors will vary depending on socio-political factors and there are different measures of what would be a successful offensive cyber-operation. The most severe cyberattack would be one in which OT components in one of the inner layers of the DCSA were compromised, causing a plant shut down by one of the multiple and independent safety shut down system which could have potential grid stability impacts in addition to significant economic losses. Other attacks may have the goal of performing reconnaissance on an NPP to exfiltrate intellectual property, lay the grounds for a future attack, or to project some other form of power.

This paper primarily focuses on defending attacks aimed at compromising OT components residing in Level 2 of the Defence-in-Depth architecture. Some of the controlled components at this level include the steam generator, pressurizer, coolant pumps, and turbines. An attacker does not have a direct connection to Level 2 from the outside, but still has a variety of entry points at their disposal.

An attacker can attempt to steal authentication credentials from personnel through targeted phishing emails or other social engineering strategies. Should this be successful, the attacker could log into systems and progressively gain access to security critical controls. This type of attack campaign would require a relatively weak defensive posture, where firewalls are misconfigured, passwords are reused, devices do not have recent patches, and other poor cybersecurity practices. A less direct approach would be to try and introduce malware into control system devices as they receive regular incremental upgrades. This could involve compromising source-code developed by third-party vendors or corrupting media used to install software onto devices. The most dangerous attacker would be an insider threat, as they have access and knowledge of the systems at potentially critical network segment levels. This type of threat actor may be driven by some personal motive, or they could be coerced, to perform some malicious actions.

Should an attacker gain access to Level 2 control systems, they may try and render devices inoperable (*bricked*), causing control systems to potentially fail. An attack may also try to send false information to controlling devices so that unintended situations may occur. For example, an attacker may alter the water level reported in a steam generator system to be higher than what it is in reality. This could cause regulating valves to restrict water flow and put the nuclear reactor in risk of not having a capable heat sink. An attacker would ideally mask any effects they are introducing into the system by changing the reported sensor values and present normal looking situations on display monitors. The attacker's aim would be to push the system into an undesirable state, such that one of the multiple and independent safety systems force a reactor shutdown, while presenting operations staff a system operating under normal conditions.

3. BOILER LEVEL CONTROL CYBER RANGE

In preparation for the cyberthreat challenges facing the nuclear industry, CNL's NICCS has been developing a cyber range to assess NPP DCSAs and to conduct training and incident response exercises. This cyber range reflects the IAEA's Defence-in-Depth network design principles and features a modelled BLC system integrated with a software simulation of PWR in a feedback loop. By conducting cyberattack experiments with this facility, NPP DCSAs and approaches to incident response can be explored, without putting any real-world operational systems at risk.

3.1. Hardware-in-the-Loop Setup

The CNL Cyber Range follows the Hardware-in-the-Loop (HIL) design principles. Since it is infeasible to replicate the entirety of IT and OT systems to operate an industrial control process, HIL proposes to reflect the operation of some specific portion of a system and integrating this with a mathematical representation (*i.e.* simulation software) of the larger system [6]. The CNL Cyber Range simulates a BLC system which is integrated with the larger Asherah Nuclear Simulator (ANS) developed as part of IEA CRP J0208. Written in Matlab/Simulink, the ANS simulation model calculates the physical dynamics, transients, and process values of a PWR NPP. These values are provided to PLCs in CNL's BLC system which adjusts the control of the water level in the boiler depending on the operating state of ANS. Process values generated by the BLC can be relayed back to ANS and create a HIL effect. An overview of this process is provided in Figure 3.

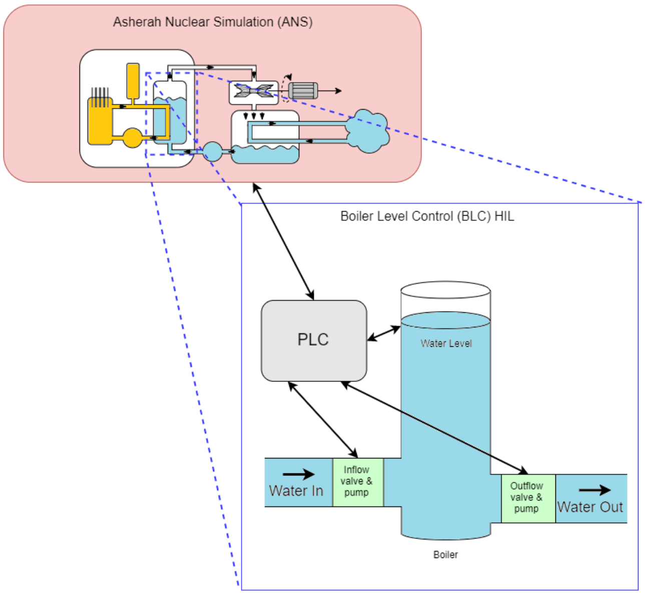

FIG. 3. HIL setup of BLC System. NPP Dynamics are computed with ANS and are passed to the scaled-down BLC system controlled by a PLC. The PLC issues commands to ensure the water level in the boiler is maintained.

The dynamics of a PWR NPP are calculated in real-time by ANS and is hosted on a server in the CNL laboratory. Some of the values from the simulator are forwarded to a PLC to control the water level into simulated water boiler. The PLC receives inputs such as the power being produced by the NPP and the desired boiler water level. The PLC controls pumps and valves to ensure that the water entering the boiler is in equilibrium with the water leaving due to steam generation. In this implementation, actual steam is not generated, instead water is pumped out of the boiler in relation to how much steam is being produced as calculated by the simulation. In this HIL setup, the OT components of a BLC at Level 2 in are reflected and can be used for cybersecurity experimentation.

3.2. IT/OT Integrated Cyber Range

The previous subsection provided a high-level overview of the HIL setup, this section provides a description of how the HIL BLC system is integrated into an IT/OT cyber range to reflect more realities of computer networks in an NPP. An overview of this is this setup is provided in Figure 4.

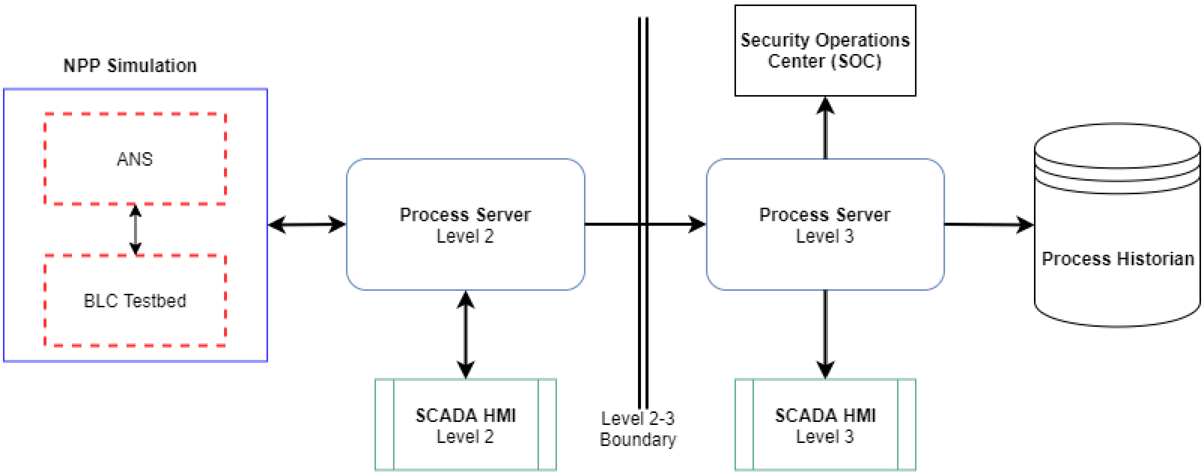

FIG. 4. Overview of Level 2-3 Components. Left hand side are Level 2 components; right hand side are Level 3 components.

The NPP Simulation is comprised of the ANS simulation and the BLC cyber range components operating in unison. This simulation generates values of the simulated physical processes and are sent to a Process Server.

The Process Server acts as a centralized aggregator of process values so that data can be homogenized and forwarded to its related control or business process. A SCADA Human Machine Interface (HMI) is connected to the Process Server for Level 2 operators to monitor and interact with the NPP processes. Some of this data is passed across the Level 2-3 boundary (comprised of firewalls and data diodes) to a Process Server on Level 3. A SCADA HMI is on Level 3 for operators to monitor NPP processes. A Process Historian captures all reported process values to maintain a record of NPP operations. A Security Operations Centre (SOC) is located on this portion of the network and is equipped with defensive cybersecurity applications. These defensive applications include Intrusion Detection System (IDS) and Security Information and Management (SIEM) tools. All process values and computer network packets are monitored by the SOC tools with the goal of detecting any malicious activities. The malicious activities could include the connection of some unknown devices or the transmission of illegitimate data packets.

4. CYBERATTACK SCENARIO EXERCISES

CNL’s NICCS hosted an IAEA Agency Mission in support of CRP J02008 from July 8-12, 2019, which saw 24 participants from 12 CRP organizations and 7 countries convene to engage in a weeklong cyberattack scenario workshop using the ANS model as the foundation. In the workshop three other PLC/HIL systems were connected to CNL’s Cyber Range and the ANS model. Several cyberattacks were conducted throughout the week to capture data logs of network traffic packets and physical process values.

The attack scenarios predominantly focused on disrupting the operation of several Level 2 processes. The attacked processes included altering the steam turbine to alter the frequency of generated power, preventing the pressurizer from properly functioning, and altering steam generation water levels. These attacks focused on rendering PLC devices inoperable by exploiting known vulnerabilities or performed a Man-in-the-Middle (MITM) attack to relay false information between the systems components. Attacks which did not directly affect physical processes looked at ways for an attacker to navigate to Level 2 to deliver a disrupt effect onto PLCs or to exfiltrate sensitive information.

The event culminated in a Red versus Blue team cyberattack scenario and incident response exercise to gain some insight into how humans may act in presence of an unknown cyberattacks in a simulated setting [7]. The meeting participants were separated into teams. The Blue team was composed of a group of SOC operators, a group of engineers with physical access to the HIL system, and a group of operators monitoring an HMI display. In the exercise an insider threat from the Red team executed an attack using a malicious USB device which spoofed Human Input Device (HID) commands (i.e. keyboard and mouse commands) to inject malware which disabled a PLC managing the BLC process and caused the water to go to an undesirable level.

This workshop proved successful at demonstrating both the capabilities of the ANS model and the capabilities of the NICCS Cyber Range in hosting an integrated HIL simulation and enabling realistic incident response exercises. Conducting attacks on the CNL Cyber Range provided scenarios to validate the capabilities of SOC tools to monitor for events within a DCSA and provided insights into best practices for the configuration and deployment of such tools in an actual NPP. Lastly, these exercises generated datasets which contain cyberattack actions leading up to a compromise in a physical system which can be used to further develop cyberattack detection strategies. These datasets have been shared amongst the IAEA CRP J02008 members and will be used to help drive future research.

5. CONCLUSION

The cyber threat landscape against NPP organizations is continually evolving and requires ongoing work to stay abreast of the capabilities of potential adversaries as well as for developing defensive techniques and architectures. This paper has outlined some of the major challenges facing an NPP organization in the face of this growing threat and how DCSAs can be used to mitigate some of these risks. The use of a HIL cybersecurity cyber range is an effective way to assess DCSAs recommended for deployment in NPP facilities.

The most effective defence to mitigate the likelihood and severity of NPP cyberattacks involves ensuring computer network access follows defensive best practices, while ensuring staff is trained to follow defensive-minded procedures [8]. This posture can be enhanced by deploying defensive applications in a SOC that can detect anomalous activity on IT/OT computer networks. Future work on detecting NPP cyberattacks can look at leveraging data science techniques to attribute unforeseen changes to physical processes to various network communications traffic to infer the presence of a cyberattack. This can lead to the development of data-enhanced anomaly detection techniques that could potentially operate in real-time.

This paper has also provided an overview of the specific capabilities of the CNL NICCS Cyber Range and how it has been used to conduct cyberattack experiments to assess the effectiveness of defensive techniques and to host Red versus Blue team incident response exercises. Participants indicated that conducting the incident response exercise in a physical cyber range provided a superior learning opportunity over table-based incident response exercises. As such, this incident response exercise had a number of significant outcomes:

- The need to have a common technical language that is understood by all parties involved. Incident response involves staff from the SOC, plant operations, engineering, maintenance, and so one. Each of these groups has their own technical terms and it is possible for verbal information being conveyed between parties to be misunderstood.
- The need to have diagnostic, response, and forensic procedures in place ahead of time for the systems or equipment being affected.
- The need to have physical security integrated into the response efforts. Cyber-attacks may incorporate a physical aspect, even if that physical aspect (as was the case with this scenario) is an insider initiating the cyber-attack.
- The ability to distinguish security events from process events. Is a process event an actual process event, or is it an indicator of compromise?
- The need for a robust communications infrastructure. For example, are there enough phone lines to handle the expected communications load?
- The ability to access urgency as the incident progresses. Can plant operations continue? Is there their time to conduct analysis and capture forensics data? Does the plant need to be moved to a safe shutdown state?

Ongoing research at CNL's NICCS will be used to identity how SOC tools can be used to automate response procedures and reduce the cognitive load of operators. This work will identify the types of plant data that can be collected and how this data can be collected without interfering with mission critical functions, distinguishing the importance of information so that impact and severity can be properly assessed while at the same time reducing false positives, improving the correlation of captured events to process events, the plant roles required for event response, and developing decision making assistance criteria such as when to shutdown processes versus continued operations.

REFERENCES

[1] MURRAY, G., JOHNSTONE, M.N., VALLI, C., "The convergence of IT and OT in critical infrastructure", Proceedings of the 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Australia, (pp. 149-155)

[2] IAEA, COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES (2017), https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst047.pdf (acc. 2019/10/31).

[3] KIRKPATRICK, K., "Protecting Industrial Control Systems", Communication of the ACM, vol. 62, no. 10, October 2019, pp. 14-16.

[4] DAHLHEIMER, J.A., TESTA, D., The Westinghouse Pressurized Water Reactor Nuclear Power Plant, Westinghouse Electric Corporation, Water Reactor Division, 1984.

[5] KNOWLES, W. *et al.*, "A survey of cyber security management in industrial control systems", International Journal of Critical Infrastructure Protection, vol. 9, pp. 52-80, June 2015.

[6] MCLAUGHIN, S. *et al.*, "The Cybersecurity Landscape in Industrial Control Systems", Proceedings of the IEEE, vol. 104, no. 5, May 2016, pp. 1039-1057.

[7] KICK, J., "Cyber Exercise Playbook", The MITRE Corporation (Technical Paper), January 2015, https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook (acc. 2019/10/31)

[8] STOUFFER, K., FALCO, J., SCARFONE, K., "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology (NIST), U.S. Dept. Commerce, Washington, DC, USA, NIST Special Publication 800-82, Revision 2 Initial Public Draft May 2014. http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf (acc. 2019/10/31)