Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors

Ayodeji, Abiodun; Mohamed, Mokhtar; Li, Li; Di Buono, Antonio; Pierce, Iestyn; Ahmed, Hafiz

Progress in Nuclear Energy

DOI:
https://doi.org/10.1016/j.pnucene.2023.104738

E-pub ahead of print: 01/07/2023

Publisher's PDF, also known as Version of record

Progress in Nuclear Energy 161 (2023) 104738

Contents lists available at ScienceDirect

Progress in Nuclear Energy

journal homepage: www.elsevier.com/locate/pnucene

Review

Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors

Abiodun Ayodeji [a,*], Mokhtar Mohamed [b], Li Li [c], Antonio Di Buono [d], Iestyn Pierce [b], Hafiz Ahmed [a,**]

[a] Nuclear Futures Institute, Bangor University, Bangor, Gwynedd, LL57 1UT, United Kingdom
[b] School of Computer Science and Electronic Engineering, Bangor University, Bangor, Gwynedd, LL57 1UT, United Kingdom
[c] Global Research Center, Wolong Electric Group Co., Ltd, Schwalmstraße 289, 41238, Mönchengladbach, Germany
[d] National Nuclear Laboratory, Central Laboratory, Sellafield Seascale, CA20 1PG, United Kingdom

ARTICLE INFO

Keywords:
Cybersecurity
Nuclear power plant
Networked systems
Control system
Sensors
Actuators

ABSTRACT

The development life cycle of conventional nuclear power plants (NPPs) needs to be optimized if the energy produced by advanced reactors and small modular reactors is to be competitive. One of the proposed optimisation initiatives is the digitalization of nuclear facility control and instrumentation. Digitalization of nuclear control and instrumentation will improve plants' performance and cost competitiveness. However, it could also introduce cyber security challenges. To create a strong cyber-defence for critical digital assets in nuclear facilities, an extensive analysis of threats and vulnerabilities in systems, networks, and devices is necessary. This article examines recent research that analyses the digital assets at nuclear power facilities for threats and vulnerabilities. This work synthesizes and categorises potential attack propagation paths in digitalized nuclear facilities based on five different surfaces: direct network path, programmable logic controllers, sensor/actuator signals, and indirect propagation paths such as attacks that exploit human factors and the supply chain. The work's main contribution is it provides a state-of-the-art understanding of the relationship between attack propagation paths, associated vulnerabilities, and current security controls. Based on the literature review, a framework for developing an attack-resilient control system for NPPs is suggested, which would be helpful for a security-informed design of reactor control systems. The discussion on nuclear cyber risks, vulnerabilities, attack routes, and defence methods offers a cutting-edge understanding of the security challenges in digitalized nuclear facilities. The suggested framework is an essential foundation for future research direction, towards a secured and resilient digitisation of nuclear power plant control systems.

1. Introduction

Nuclear power reactors are an important component of clean, net-zero energy systems, particularly in the context of energy independence and national security. Moreover, the ongoing Russia-Ukraine war has also shown the importance of energy independence, and the significance of including energy security in strategic national security policy. Nuclear reactors are well-positioned to ensure an all-weather, low-carbon, uninterrupted supply of electricity and heating, and the new generation plants are built to ensure safe, and economic power generation (Bodel et al., 2021).

The demand for better engineering system performance has prompted the development of advanced technologies with the corresponding integration of digital technologies and expansion in the interconnectivity of many physical systems. The integration of digital technology would also increase the effectiveness of critical infrastructures including smart grids, industrial production systems, and new-generation nuclear power plants. Although these technologies improve energy systems' dependability, efficiency, flexibility, and ability to be controlled and supervised remotely, they also make infrastructures more susceptible to cyberthreats that may result in serious safety incidents. Because of the unacceptable consequences of successful attacks on vital national infrastructures, cyber security controls are becoming more common.

* Corresponding author.
** Corresponding author.
E-mail addresses: ayod_abe@yahoo.com (A. Ayodeji), hafiz.ahmed@bangor.ac.uk, hafiz.h.ahmed@ieee.org (H. Ahmed).

https://doi.org/10.1016/j.pnucene.2023.104738
Received 13 December 2022; Received in revised form 4 April 2023; Accepted 11 May 2023
Available online 20 May 2023

Following the emerging trend in Industry 4.0 and industrial systems digitalization, digital instrumentation and control (DI&C) systems, and devices such as programmable logic controllers (PLC), and ethernet/IP networks, are being leveraged for improved communication and control operation, particularly in non-safety applications in the nuclear industry. This inadvertently elevates cyber security as one of the biggest challenges in nuclear facilities. Concerns about cyber security in NPPs were also raised by previous notable attacks on nuclear facilities around the world, such as the cyber-attack on an Iranian fuel enrichment facility, the Davis-Besse NPP in the USA, and the attacks on computer networks at Korea Hydro & Nuclear Power. This led researchers to develop tools to analyse NPP cyber security and to mitigate and minimise the risk.

Recently, many studies have analysed the security challenges against digital process control systems, and the controls needed to mitigate any serious incidents. Several studies have also been done to analyse potential attacks on distributed control systems (DCS) common in large industrial facilities. However, although promising, these techniques cannot be directly extended to critical facilities such as nuclear power plants. First, the nuclear cyber-attack surface is increasingly getting complex because of globalisation and decentralised manufacturing and supply chain of nuclear reactor components. Vendor-specific vulnerabilities could be inherited by modern plants with digital control and instrumentation, and these inherited vulnerabilities make it difficult to propose a one-size-fits-all solution to nuclear cyber security. In addition, the deterministic network traffic in nuclear facilities differs from the dynamics observed in the conventional information technology (IT) network, and signatures are not available for most ICS-targeted malware in nuclear facilities as such information is controlled. Hence IT solutions cannot be directly applied to nuclear plant control systems.

Secondly, assessing vulnerabilities in nuclear digital assets is increasingly complex due to the need for configuration-specific assessments that consider interconnected devices, connection types, network architectures, and protocols. To simplify the vulnerability assessment and study the dependency effects of new digital devices, virtual engineering approaches can be leveraged. However, virtualization requires high-fidelity models of the physical process and the control networks, which is complex. Moreover, the nuclear reactor is highly nonlinear, with parametric uncertainties. From a research perspective, this makes nuclear reactor modelling a challenge, as issues such as the spatiotemporal characteristics of neutron transport in the core, delay neutron precursor, lumped versus grouped thermal-hydraulic modelling, reactivity feedback introduced by the temperature change, control rod, Xenon oscillation and chemical shim need to be duly considered to obtain a robust plant model. Also, the distributed nature of the nuclear control systems makes it difficult to directly apply the solutions proposed to simple, linear systems. In addition, studies that enumerate the threat and attack landscape in digital control and instrumentation in nuclear facilities are limited, and no work critically reviews the existing frameworks, evaluation testbeds and nuclear digital instrumentation and control attack propagation paths from the systems, network, and human reliability perspective.

This work addresses these gaps by reviewing previous studies that analyse the threat and vulnerability in DI&C components and networks that constitute modern control systems. This work also synthesizes and categorises potential attack propagation paths in digitalized nuclear facilities: network connectivity/communication channel, programmable logic controller, sensors/actuators, human-target and the supply chain. Further, the work also discusses the relationship between these attack paths, related vulnerabilities, and existing evaluation tools and security controls. This work makes a significant contribution by putting forth a proposal for creating an attack-resilient digital control system and cyber security analysis of crucial digital assets at NPP, which can be used to factor cyberattacks into the reactor control design basis threat. The present study advances understanding by.

1. Synthesising and reviewing the literature on nuclear cyber security.
2. Categorising nuclear cyber-attack paths and the protection frameworks and systems.
3. Suggesting a framework for a robust cyber security evaluation of NPP digital control systems, as a potential future research direction.
4. Extending the application of the framework for nuclear cyber security design basis threat.

This work does not consider artificial intelligence (AI)-based protection techniques, which have been studied extensively in the literature (Ayodeji et al., 2020). Interesting progress has also been made in designing useful machine learning-based tools for anomaly detection in industrial control system (ICS) networks (Arnold et al., 2022), and controllers (Zhang and Coble, 2020). However, most of these proposed approaches are hypothetical and not yet scalable in real plants, to the best of the authors' knowledge. This is because AI techniques are as good as the data used in their development, and there is limited open-source, validated nuclear data to build a robust data-driven model. The current work discusses the critical platform necessary to develop and curate high-fidelity data useful for the AI community. The state of the art in machine learning-based tools for nuclear digital asset protection, accompanying issues and challenges have been comprehensively discussed in (Ayodeji et al., 2020).

2. Nuclear process control basics

To conduct an effective vulnerability assessment, detailed knowledge of devices, components, systems, and networks within the plant, as well as an understanding of both hardware and software components and their interaction is required (Peterson et al., 2019). This section briefly describes the fundamental unit of a nuclear power plant and the interaction of the components that make up the process control systems (PCS).

In its basic form, the nuclear power plant is composed of systems, structures, components, networks and devices that interact to ensure that heat generated from the fission of uranium fuel is transferred efficiently from the reactor core, via the steam generator (for pressurised water reactors, (PWRs)) to the turbine. The heat exchange between the primary fluid and the secondary fluid is used to boil water in the steam generator, and the steam is used to drive turbines that are connected to electric generators. The steam is condensed and returned to the steam generator as secondary fluid. To keep the uranium fuel 'cooled', and to confine the fission products in the core, several process and safety systems are tightly coupled. Although all the process systems are tightly coupled, each of the processes is controlled independently by a set of devices and networks. Fig. 1 shows a simplified illustration of the coupled systems and their architecture.

Fig. 1 above shows a typical architecture of nuclear process control systems in a conventional PWR. As an illustration, the figure assumes a PLC-based controller, instead of the conventional hardwired PI controllers used in NPPs. PLC-3 shows the control system that monitors and regulates the water level in a PWR steam generator. In its basic form, the level control system comprises a sensor, an actuator (power-operated feedwater valve), a controller, and the protocols that enable communication between the three devices (conventionally field buses such as Modbus Profibus etc). To complete a control step, the sensor senses the water level in the steam generator, by converting the level analogue indicator to a serial electric signal (electric current between 4 and 20 mA, or voltage between 0 and 10 V) sent to the controller. The controller compares the sensed level with a setpoint (typically determined by the operator) and compensates for the error between the measured level and the setpoint. A control signal is automatically generated by the controller to the actuator (conventionally valves, motors, breakers, etc), via the communication channel. The actuator completes the control action by accurately locating the valve (plug) in a position dictated by the signal from the controller.

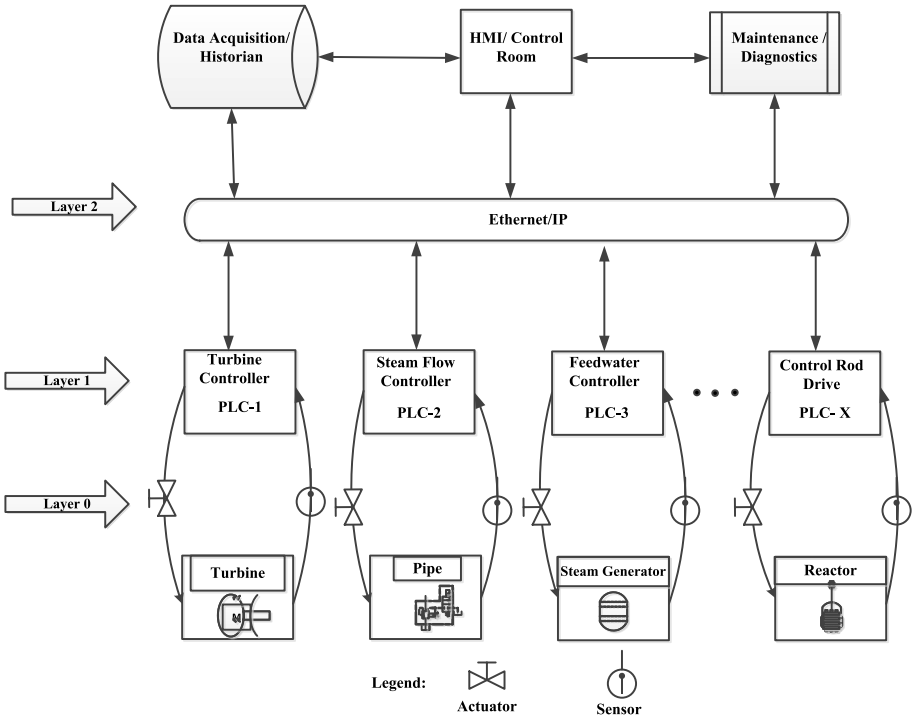

Fig. 1. A simplified digital distributed control system for a typical nuclear power plant (Ayodeji et al., 2020).

To enable the operator to monitor the current water level in the steam generator, a similar controlled variable signal is generated by the sensor and the manipulated signal from the controller is sent via the communication network to the operator's human-machine interface (HMI). The serial signals are first converted to a network packet, via a serial-to-ethernet converter that facilitates communication between level 0 and level 1 devices. Then the packets are delivered to the user interface in form of charts/graphs or digitally, depending on the HMI configuration. Analysing attack propagation paths that serve to facilitate system intrusion in nuclear DI&C is important, and this basic description of a typical control loop in the nuclear power plant serves to inform the nuclear ICS attack path categorised and discussed in the next section.

3. State of the art

3.1. Nuclear cyber-attack paths and the protection frameworks

To design a robust cyber defence for critical infrastructures such as NPPs, a detailed threat and vulnerability analysis is important. Also, understanding the DI&C attack surface in the nuclear power plant is critical in designing and implementing a cyber security solution. This section discusses recent works on threat/vulnerability assessment, as well as digital industrial control systems (ICS) cyber-attack path and recommended protection systems.

3.1.1. Threat and vulnerability assessment

To protect both wired and wireless digital I&C data, systems and networks from malicious intrusion, a thorough understanding of the capacity and motivation of the attacker are necessary. Attacks on industrial I&C could be carried out for technology theft, business espionage, cyber-activism, recreational hacking, by a disgruntled employee, or the probing of a nation-state or terrorist organisation (Hashemian, 2011). Any of these attackers may exploit system vulnerability by launching damaging attacks such as mimicking, man-in-the-middle (MITM) attacks, network spoofing, packet-sniffing and modification, sensor masking, and denial of service (DoS), or via malicious codes such as virus, worm, and ransomware. However different types of attackers have different motivations, capabilities and resources, and the sophistication of attacks also varies. Mere criminal behaviour should be distinguished from cyber-attacks that have national security relevance, and understanding the nature of the attacker/attacker profile is critical in the design and implementation of security measures for nuclear DI&C.

One of the most important challenges faced by modern DI&C is system exploits by well-motivated, well-resourced, sophisticated attackers such as nation-states (i.e., advanced persistent threats). The intended impact of cyber-attacks in nuclear ICS is also reflected in the complexity of the attack, as launching a catastrophic cyber-attack requires a sophisticated adversary (Kesler, 2011). Hence, comprehensive threat analysis and nuclear DI&C security evaluation tools are necessary for proper risk evaluation and protection. Towards a secure system, discovering system vulnerabilities is one of the first major steps. Incidentally, vulnerabilities in DI&C are not intuitive, which calls for specialised skills and tools. A vulnerability assessment is performed to identify and prioritize inherent weaknesses in cyber systems and components. In nuclear power plants, cyber systems are defined as critical digital assets (CDA) and networks that are responsible for Safety, Security, and Emergency Preparedness (SSEP) functions. Many tools and guidance documents have been presented for cyber vulnerability remediation, with little focus on the nuclear SSEP systems vulnerability identification. However, recent research works have explored models and methods for vulnerability identification in nuclear facilities.

Based on safety margin estimation, Wang et al. (2018) discuss an exploration approach to identify the most vulnerable components in NPPs to cyber-attacks. A Monte Carlo-driven engine was used to simulate and inject different types of cyber-attacks of different types and magnitudes. Then, safety margins are calculated and used for identifying the most vulnerable components in cyber-physical systems. A template for cyber-attack classification that reflects the characteristics of NPPs has been presented in (Kim et al., 2020). A systematic approach is proposed to evaluate and validate the cyber security conformance for digital instrumentation and control systems in NPPs. The authors discussed the attack taxonomy that could enable strategic responses against cyber threats at NPPs, and the taxonomy classification includes the attack procedure, attack vector, physical access, network access and

consequence. Varuttamaseni et al. (2017), also studied the impact of a DoS attack on the reactor protection system, using the TRACE code. The work discussed the low pressurizer pressure trip safety signal under attack and analysed the response of the plant to a trip delay of 1 s. Several potential cyber-attack scenarios on NPPs are investigated for the analytic study following the South Korean case in December 2014 (Cho and Woo, 2017). A comparison between different terminologies such as accident, terror, general and cyber terror, and a list of cyber terror types for NPPs are presented and discussed in (Kim, 2014). A few complementary points of various cyber security methods were identified in the analysis and suggested to be considered to enhance the cyber security of NPPs.

Several stealthy attacks have been identified as potential threats to digital instruments in industrial systems. Industrial control systems are also susceptible to false data injection (FDI) attacks, which could introduce subtle variations in real signals, making them difficult to detect by conventional anomaly detection systems (Sundaram et al., 2022). In the context of control systems for nuclear reactors, two key threat scenarios involving false data injection attacks have been envisaged (Li et al., 2018a). These scenarios are intended to create control commands that deviate the reactor state from its intended operational range for malicious purposes. The first scenario involves the initiation of an event through the falsification of sensor readings. The second scenario involves the manipulation of the normal reactor response to an event by altering the underlying controller logic (Li et al., 2018a). Both scenarios pose significant risks to the safe and reliable operation of nuclear reactors. To address the threat of FDI attacks, Li et al. (Sundaram et al., 2022) proposed an algorithm designed to detect falsified signals through the use of process information derived from the physical model of the plant. The algorithm was validated using data obtained from the RELAP 5 code. In addition, to ensure real-time monitoring and resilience to noise, the authors optimized the denoising algorithm and assessed its efficacy in identifying a triangle attack carried out by a malicious insider on a nuclear plant (Li et al., 2022).

An event classification scheme is presented in (Vaddi et al., 2020) to distinguish between fault-induced safety events and cyber-attacks for NPPs. The Dynamic Bayesian Networks with Conditional Probability Tables methodology is used to identify the nature of the abnormal events (safety events or cyber-attacks). It is assumed that the sensors' measurements and the input to the component are correct all the time. A cyber security risk evaluation model for digital instrumentation and control systems for NPPs using a Bayesian network and event trees is proposed in (Park and Lee, 2019). Using historical data and online measurements, the evaluation model informs research on cyber threats to nuclear DI&C. The method is also used to estimate nuclear DI&C probabilistic safety and to analyse frameworks for cyber-attacks on NPPs (Park and Lee, 2019). A comparison and analysis of various methods used in the applications of cyber security to critical systems in NPPs are presented in (Son et al., 2019). Ahn et al. (2015) proposed scenario graph modelling to develop cyberattack scenarios in NPPs. The model utilises directed acyclic graphs with attacker, event and goal nodes that represent the threat, the exploited vulnerability and the consequence of the exploit respectively. The graph also has edges that represent the relationship between nodes. The scenario graph was used to analyse the cyber incident at David Besse, Hatch and Brown Ferry NPPs, and the cyber-attack on the Iranian Natanz enrichment facility.

A detailed overview of cyber security vulnerability assessment in nuclear facilities is presented by Peterson et al. (2019). The review details the cyber-vulnerability incidents at nuclear installations and other critical facilities and gives the context for vulnerability assessment improvements that must be made. The paper also analysed vulnerabilities within the context of the modernization of digital instrumentation and control systems. Moreover, the work discussed approaches developed to mitigate cyber risk at NPPs, and it enumerated the limitations of the United States National Regulatory Commission (U.S. NRC) guidelines. Apart from widely recognized network penetration testing software and open-source tools, limited studies are dedicated to developing active tools for ICS vulnerability identification. To bridge the gap, a Systems Modelling Language (SysML) that enables vulnerability extraction from an industrial control system model was developed in (Lemaire et al., 2014). The SysML is a Model-Based Systems Engineering (MBSE) tool that supports the system development life cycle. The tool uses logic theory for vulnerability extraction, which is then included in the system model for further analysis. Users can also specify information about the component, product and version, and the tool uses the ICS-CERT vulnerability database and the NIST, ISA, ISO's ICS standards as system independent reasoning inputs. The application has been demonstrated on a few industrial ICS. However, there are no use cases for nuclear DI&C.

3.2. Categorization of NPP DI&C attack propagation path

In critical industrial facilities, cyberattacks naturally progress to physical impact. The cyber-space provides a convenient and replicable channel through which an attacker could access and damage the physical system. The attack propagation paths, as used in this work, are defined as the potential route a threat actor could leverage to achieve their goals. Different from attack surfaces (classified as the network connectivity, portable media and equipment, physical access, etc), that aid the adversary to access processes, networks, data, or systems, attack propagation paths are the layered steps the threat actors could take to exploit or compromise digital assets.

To defend systems that make up the nuclear DI&C, analysing the plant, inherent attack paths, and the consequence of successfully exploiting the attack paths on critical digital assets is important. Towards understanding the attack paths and their inherent vulnerabilities, this section categorises common components, systems and networks susceptible to cyber-attack, and the methods/techniques that have been proposed to protect them.

3.2.1. Direct attack propagation paths

3.2.1.1. Communication network and protection systems. Real-time controlled variables (such as temperature, pressure, flow, and level) and the corresponding magnitude of the manipulated variable are sent to the operator, for easy condition monitoring and control of the process. The sensor readings are transmitted to the controller (input), and the control signals (output) are sent to the actuators via traditional communication protocols (e.g. Fieldbuses). The communication network is used to transmit the sensor and control data to the operator HMI, via the serial-to-ethernet converter, to enable human operators to monitor and respond to the continual flow of I&C data. For efficiency reasons, NPP owners are modernizing legacy systems. The modernised nuclear DI&C have seen increased utilisation of digital hardware, TCP/IP network protocol with accompanying network cards, IP address configurations and software. Nuclear ICS modernization has also seen the connection of the traditional ICS communication protocols (e.g. Modbus, Profibus, DNP3, IEC61850, etc) with the TCP protocol to enable a serial-to-ethernet data transfer, and these connections have introduced an extra attack surface in the system. Cyber exploits of the serial-to-ethernet convertor have been previously reported in (Weiss et al., 2022). Other attacks intended to mask real-time measurements (e.g. DoS, DDoS attacks) or to corrupt/replace measured signals (e.g. Man-in-the-middle attacks) have also been reported for ICS.

One of the most important network security evaluation models is the Bayesian Network, a graphical model used to represent variables and their dependencies. BN is a directed acyclic graph with nodes and vertices that define connections, directions, and accompanying probabilities. To design an optimal defence strategy for control systems, Li et al. (2018b) used a multilevel Bayesian Network to distil the attack paths, evaluate the attack progression and propose countermeasures for

attacks on the Tennessee Eastman process (Li et al., 2018b). Vaddi et al. (2020) also present a dynamic Bayesian Network approach to classifying cyber-attack-related abnormalities in nuclear control systems. The work utilises both the physical and network layer information to infer hidden, unobservable states of the plant and the nature of the abnormal event. Similar to the Bayesian Network approach is the attack tree method that has been proposed to evaluate the cyber security of a nuclear power plant (Ayodeji, 2014). The attack tree method was used as a directed acyclic attack-defence model of nuclear plant ICS network vulnerabilities, and a metric (Return-on-Attack) was used to quantify the attack benefits for a successful exploit of each node. From the attackers' perspective, the most attractive attack paths are identified, and security measures are implemented. Similar approaches have also been proposed to secure enterprise and related networks (Akinola et al., 2015). Detailed discussion on the utilisation of directed acyclic graphs as attack-defence models and their applications in critical industrial control systems can be found in (Ayodeji, 2014; Kordy et al., 2014). Although graph-based security models are effective in evaluating system interconnectivity, revealing casual relation and root-cause analysis, it is ineffective in large networks, as the method could suffer from node explosion.

3.2.1.2. Programmable logic controllers (PLC) and protection system. Another type of attack path in the digital ICS is the controller itself, as most of the legacy electromechanical relays are being replaced with devices with memory and programmable microprocessors. The PLC provides flexible configuration and digital communication. However, the software-based PLC also introduces potential vulnerabilities, as attackers can execute arbitrary malicious codes on the controller to directly alter the control functions. Unlike traditional IT devices, software patches on and frequent updates of PLC programs are not well suited for control systems, as control systems require online and real-time availability and patch management requires system reboot and restarts, change verification and validation, and may consume a significant computing resource. Moreover, such security patches may violate certification/regulatory requirements, as large industrial systems also have some legacy systems. Several researchers have proposed different kinds of hardware-based (solid-state), software-based and hybrid protection systems for controllers to make them robust enough to perform control functions under attack. This section discusses PLC vulnerabilities, proposed security analysis tools and protection systems.

Following the Stuxnet attack, different PLC cyber security issues have been discussed (Shin et al., 2017). As PLCs are one of the main devices used to implement control functions, security procedures against cyber threats have also been proposed (Shin et al., 2017). To detect malicious modifications in firmware in programmable logic controllers, Dunlap et al. (2016) proposed a timing-based side-channel analysis, an approach that compares device fingerprints to detect anomalies. The proposed approach is tested on an Allen-Bradley ControlLogix PLC, using the task monitor to collect timing measurements on the analogue/digital inputs and outputs, and the network traffic data. A receiver operating characteristic curve is used as the metric, to determine the false-positive rates. A false sequential logic attack on the control network is also discussed by Li et al. (Kordy et al., 2014). The work presents a scenario where an attacker disrupts the physical process via a logic attack on the sensor, actuator and controller of a SCADA system (Li et al., 2016). The attack modelling, physical impact analysis, and defence measures for a chemical process are discussed in the study.

Zhao et al. (Zhao and Smidts, 2020) simulate a replay attack on an NPP's linear quadratic regulator. The work demonstrates how an attacker could compromise the controller by launching an attack that replays recorded sensor output to the controller, demonstrated with a pressurised water reactor simulator. The attack detection technique proposed was two chi-squared tests that separate the replay attack from other anomalies. A cyber security framework to protect programmable logic controllers (PLC) in Korean NPPs is also proposed by (Song et al., 2014). The concept and development of the framework involve identifying all the cyber assets, accompanying vulnerabilities, and developing security requirements for the module based on the evaluation results.

A survey on cyber security of industrial control devices that are used in critical infrastructures, such as nuclear and thermal plants, water treatment facilities, and power generation is presented in (Bhamare et al., 2020). Because industrial control systems have been integrated with information technology devices, and the ICS have become a part of cloud-based environments, the authors of (Dunlap et al., 2016) suggest data-driven techniques to enhance cyber-security in critical infrastructures. Zhang et al. (Zhang and Coble, 2020), propose a robust localised cyber security kit for PLCs in NPP. The approach involves an embedded empirical model in the PLC hardware, for cyber-attack detection and inferencing. However, the work did not discuss the resource requirement of the models, as such models could consume a significant computing resource and could impede the PLC software from operating at its peak efficiency.

Several literature have also proposed solid-state devices to replace the software-based PLC in nuclear I&C. Field programmable gate arrays (FPGA)-based devices have been proposed to replace conventional PLC in nuclear I&C (Sklyar, 2012). FPGAs have specific advantages such as simple design, uniqueness, and the use of hardware description programming language. FPGA-based PLC hardware circuits also require no extra operating system, better encryption, faster parallel function execution and better security (Elakrat and Jung, 2018). However, cyber security assessment of FPGA-based systems is subjective and lacks robust analysis of coupling effects. Moreover, proposed FPGA-based nuclear reactor control systems lack comprehensive security requirements, assurance, conformance and standards (Illiashenko et al., 2016). That is, regulatory and certification bodies, developers and end-users of FPGA-based systems for nuclear DI&C lack a harmonised approach for its security assurance, considering the context-specific operating environment.

3.2.1.3. Sensor/actuator and protection systems. There are classes of attacks that are designed to render targeted devices inoperable. In critical infrastructures like NPPs, most of these attacks are directed toward corrupting sensed signals or injecting fault and corrupted signals to the actuator or rendering the actuator inoperable. This is because of the potential payoff in exploiting level-0 devices, and the closeness of these devices to the physical system. This section discusses recent works that discuss targeted attacks on ICS sensors and actuators, and their limitations.

Coupled attack monitoring and mitigation game-theoretic approach for sensors in a cyber-physical system under attack has been proposed (Zhou et al., 2019). The approach is implemented with two different algorithms that monitor and mitigate sensor attacks. He et al. (2021) presented an attack-resilient control solution that uses predefined boundaries to guarantee system stability. The work utilised Markov jump systems to model additive and multiplicative sensor and actuator attacks in a closed-loop control system. The requirements for securing hardware, firmware, software, and system information associated with digital instrumentation and control systems at NPPs are also discussed in the paper. A technique for analysing the ability of attackers to control and mask measurements (unobservable states) is discussed in (Vaddi et al., 2020). The paper demonstrated how an attacker can design an attack to maximise the impact on the unobservable states while minimising the possibility of detection. Kalman decomposition method was used to identify unobservable subspaces, accounting for process measurements the attacker can manipulate but that cannot be observed.

There are storing and updating rules that guide modern PLC inputs from sensors. These rules can be disrupted during a sensor attack that masks the readings for current time steps forcing the controller to use stored process values for the control function. To properly identify specific sensor measurements that need to be protected, and the

required security-incidence response time before major damage, Krotofil et al. (2014) proposed a method to time DoS attacks on sensor signals. The work used a non-parametric cumulative sum (CUSUM) to detect changes in measured signals, and the approach is evaluated on the Tennessee Eastman process (Krotofil et al., 2014). Adapted CUSUM-based approach and finite moving average (FMA) detection rule is also used by Van et al. (Van Long et al., 2015), applied to detect a stealthy attack on sensors in a SCADA water treatment plant. The work develops a unified statistical model and Kalman filter to generate residuals from process transient changes. To detect covert attacks, the work used the worst-case threshold selection that accounts for measurement noise and compared the performance of CUSUM with FMA rules.

To study the effect of retrofitted digital instrumentation and control systems and to identify their potential weaknesses in a notional PWR, Denman et al. (2016) simulated a cyber-induced oscillation of the flow rates in high-pressure and low-pressure injection pumps. The study shows that a compromised integrated DI&C system can cause an accident sequence that would normally be considered an extremely low-probability event. The study also demonstrates test cases for retrofitted DI&C. Many researchers have also proposed mathematical/statistical tests for cyber-attack detection, such as the chi-squared test utilised to detect replay attacks on sensor signals (Zhao and Smidts, 2020). Maccarone et al. (2018) also present a technique for analysing observability attacks on sensors and actuators. Using a state-space representation of the system, the work discussed the combinations of sensor omissions that would mask subspaces controlled by attackers. The appropriate attack input signal is created, and the system response is analysed. Huang et al. (2009) also described integrity attacks such as the minimum, maximum, additive and scale attacks on industrial sensors. The work investigates the effect of these attacks and compares them with a DoS attack on a chemical reactor. The work concludes that a DoS attack in isolation has relatively little impact on the system's steady state, but could have a significant impact when combined with other integrity attacks.

3.2.2. *Indirect attack propagation paths*

3.2.2.1. Insider threat/Human-targeted attacks and protection program. Human reliability issues are some of the most complex security issues being addressed towards a secure nuclear DI&C. The complexity of analysing human subjective vulnerability has been the major detriment in curbing human-targeted attacks and insider involvement. External threat actors could collude with or radicalise knowledgeable insiders or leverage insider vulnerability to access and exploit critical control systems. Moreover, unintentional misuse and erroneous operation could create novel vulnerabilities or impede safety functions. Protection systems such as firewalls, data diodes and intrusion detection systems could be easily bypassed via the authorised access the insider possesses.

Cyber-attack could also induce misoperation in nuclear power plants, which presents the operator as an additional attack surface for cyber intrusion. This is a scenario where an attack on a non-safety critical system in the plant leads to an inadvertent operator's action that affects the safety-critical system's availability. Depending on the plant's status, operators can override automatic control functions via manual operations, and attackers can directly spoof or corrupt either the HMI or the sensor signal, thereby misleading the operator into sending an incorrect control signal. Such a scenario of human error under a system cyber-attack is discussed in Kim et al. where the human error (omission or commission) leads to arbitrary operator action that affects the nuclear SSEP systems (Kim et al., 2017).

Globally, there is a lack of publicly available data on insider case studies in nuclear facilities, which has significantly limited researchers from leveraging realistic scenarios to create robust pattern recognition and insider causal path analysis (Camp and Williams, 2020). A few insider threat case studies in radiological and nuclear facilities, and recommended protective measures are presented in (Hobbs and Moran, 2015). The incidents are presented as a learning tool for teaching and situation analysis in nuclear and radiological facilities. Camp and Williams also proposed the counterintelligence approach (Camp and Williams, 2019) to mitigate insider threat, which involves the use of counterintelligence insights and indicators to characterise/profile potential insiders. The work compares the elements elicited from counterintelligence case studies and the implications for insider threat mitigation. Other proposed approaches to mitigate insider threat include strengthening nuclear security culture (Khripunov and Speicher, 2018), improving human reliability programs (Baba et al., 2022), and the balance of technology, policies, procedures, and training.

Country-specific regulatory frameworks have also been designed to curb insider threats. For instance, the Germans use the two-person principle as a form of access control against insider attacks (Lochthofen and Sommer, 2015). The principle mandates two people to be present in rooms that house security-sensitive systems. Among other user identification and restricted access measures, protection racks, barriers and data access control measures are also implemented. Some countries have also adopted the two-person principle, which is useful in checking third-party insider threats, as the vendor's maintenance staff could access server rooms for maintenance purposes. However, for the two-person principle to be efficient, the selection criteria need to be defined, as the two-person approach is not collusion-proof. One of the most widely-used guidance documents for nuclear facility insider threat is the IAEA's best practice series (International Atomic Energy Agency and I, 2020). The document provides implementation guidance on the evaluation techniques for the preventive and protective measures against insider collusion, protracted theft, and sabotage.

The insider threat prevention and control measures in literature are mainly on surveillance, intrusive vetting, peer observation and reporting. However, we hypothesise that this could create a low-trust environment, hence, benchmark studies on insider threats that consider the (psychological) effect of these countermeasures on staff confidence, satisfaction, turnover, and performance are required. Besides, since human reliability issues are similar across cultures, country-specific and other critical industry measures against insider threat need to be analysed, and the strength needs to be consolidated as an international strategy for nuclear insider threat mitigation. In addition, more research efforts are needed in mitigating insider threats through non-intrusive technology and data analysis.

3.2.2.2. Supply chain and protection systems. The nuclear supply chain comprises a complex network of global stakeholders, suppliers and activities that presents it as one of the largest cyber-attack surfaces (Eggers, 2021). The geographical spread of nuclear suppliers is justified by the need for a high-quality and affordable product, timely delivery, specialised and proprietary equipment, components, and services. Incidentally, the spread has also made it difficult to assure the security, authenticity, and trustworthiness of nuclear equipment and components.

Conventionally, supply chain integrity is one of the security assurances relied upon by NPP ICS. NPP owners use vendors that are authorised and trusted. However, the changes in the geopolitical landscape and growing concerns with advanced persistent threats and national security challenges have refocused attention on the need to secure hardware and software sourced from the global supply chain. Amid cases of counterfeit, suspect items and supply chain compromise, nations are shifting away from over-reliance on supply chain integrity as a cyber-security measure and are actively considering the possibility of hardware compromise via supply links or inadvertent/intentional cyber-exploits/advanced persistent attack of level 1 and 2 devices and networks introduced directly to the component through the supply chain. The U.S. Department of Defence (DoD) listed the supply chain as one of

the four primary attack vectors used in an asymmetric blended cyber operation against critical installations (Nissen et al., 2018). There are indications of adversaries exploiting critical supply chain vulnerabilities to install embedded malware that creates a backdoor for data exfiltration, data tampering, false data injection or product quality degradation, and counterfeiting, in ways that make attribution difficult (Nissen et al., 2018).

Several systems, service acquisition policies and procedures, and defense in-depth strategies have been recommended for protection against supply chain threats. The DoD also recommends measures that span legislation and regulation, policy and administration, acquisition and oversight, and programs and technology, with near, medium and long-term actions (Nissen et al., 2018). Other measures recommended to protect DI&C against supply chain threats include establishing trusted distribution paths, pre-agreement supplier review, vendor validation, and tamper-proof products or tamper-evident seals on acquired products requirements (USNRC and 5.71, 2010). These measures significantly limit the spread of the supply chain attack surface. However, NPP owners still rely on vendors for equipment maintenance and life cycle support. This gives vendor staffers access to critical digital assets during routine maintenance, which poses another insider threat attack surface and of a significant cyber security concern.

Moreover, implementing sweeping regulations across the global supply chain is impractical as such a move may be counterproductive or in conflict with local regulations. Hence, the supply chain has presented itself as a critical attack surface that warrants protective measures. A supply chain cyber-attack surface and the accompanying threats and vulnerabilities have been discussed (Eggers, 2021). The discussion spans supply chain assurance, and programs to ensure nuclear I&C's confidentiality, integrity, and availability. To ensure the life-cycle protection of DI&C, the proposal was to evaluate the risk of cyber threats during components design, development, installation, maintenance, and repair.

The nuclear cyber security attack propagation path discussed above is not exhaustive, as new paths could be created depending on the network architecture, topology, and security control. The network attributes could create novel attack paths which are beyond the scope of this work. Some of the known vulnerabilities and attack paths, as well as references to the works that detailed the exploits, and their protection measures, are summarised in Table 1 below.

3.3. Nuclear facility cyber security controls, frameworks, and evaluation testbeds

To ensure adherence to ICS security standards in nuclear facilities, a vast number of documents have been produced on cyber security controls and regulatory frameworks, especially in countries with civil nuclear power programs. Several government agencies have also published guidelines and regulations to protect critical ICS. The international electrotechnical commission (IEC) established requirements for the development and use of digital instrumentation and programmable control systems in nuclear power plants (IEC 63096). Adapted from ISO/IEC 27001:2013 that guide information security and management system, the IEC 63096 also details the functional safety, cybersecurity controls, risk management framework, as well as the life-cycle implementation needs for nuclear digital I&C and programmable devices (Rowland et al., 2021; Watson et al., 2018). The improved cybersecurity controls in IEC 63096 and the recommendations for coordinating the functional safety and cyber security requirements in the context of nuclear digital infrastructure have been discussed (Yang, 2022). Other cybersecurity evaluation programmes and working groups have also established a common position on the cybersecurity features of digital I&C in NPPs(Watson et al., 2018; Collet and Lorin, 2018).

The U.S. NRC has extensive regulations in place to ensure cyber security at nuclear power plants, and they provide centralised oversight and inspectors are on-site at all U.S. nuclear plants. The commission also issues cyber security guidelines and programs that promote safety,

Table 1
Attack propagation paths, known vulnerabilities and potential payload.

Attack paths	Known vulnerabilities	Potential payload	References
Communication Network	Hardware: • Unsecured USB and PS/2 port, Keyloggers Software & configuration: • Weak network security architecture; weak Dataflow controls • Poorly configured security devices • Encryption, exhaust network bandwidth to generate latency; buffer overflow; DNS poisoning	Session hijacking; message flooding; eavesdropping; Reconnaissance; message spoofing; Rogue server; Remote procedure call, etc.	(Li et al., 2018b), (Ayodeji, 2014), (Akinola et al., 2015), (Weiss, 2010), (Weiss et al., 2022)
Programmable controller	• No anti-malware/ anti-virus measures • Unsecure ICS protocols • Encryption issues • Open-access technical documents • Open programming interface; unused tags or operands. • Malware on engineering workstation	Authentication attack; Firmware modification; Ladder logic modification, False sequential logic attack; stealthy data logging; Replay attack; DoS; Remote memory dump; Remote shell access; side-channel attacks; etc.	(He et al., 2021), (Makrakis et al., 2021)
Sensor and Actuator	• Tampering, Sabotage, Electromagnetic interference, Replay attack, perceptual data corruption; • Information leakage; Resonance Node outage, masking, etc	RHR valve attack, Accumulator valve attack, PORV attack, DoS, MITM, Access attack, Reconnaissance; energy exhaustion attack; false data injection;	(Alvaro et al., 2009), (Ashibani and Mahmoud, 2017), (Vaddi et al., 2020)
Human factor	• Inadvertent mal-operation. • Unintentional misuse; inappropriate sharing of data; device/media exposure • Untrained operator • Possible collusion; loss of situation awareness. • Insider access via maintenance staff • Human error, sabotage, radicalisation, espionage, etc.	Viruses; Malware; Man-in-the-middle attack; Social profiling; HMI attack; hardware theft; dumpster dive; etc.	(Kim et al., 2017), (Camp and Williams, 2019), (Camp and Williams, 2020), (Hobbs and Moran, 2015)
Supply chain attack	• Hardware tampering • Software tampering • Firmware tampering • Installation of devices containing a backdoor • Software patch/ update	Reconnaissance attack via BIOS, bitstream or microchip or configuration files; Reverse-engineering, IP theft; side-channel attack; Trigger & payload Trojan insertion; DoS;	(Nissen et al., 2018), (Eggers, 2021), (USNRC and 5.71, 2010), (Eggers and Rowland, 2020)

(continued on next page)

Table 1 (*continued*)

Attack paths	Known vulnerabilities	Potential payload	References
		spoof credentials; hijacked software update; Malicious substitution, insertion; Tool alteration	

security, and emergency preparedness functions at nuclear power plants (USNRC and 5.71, 2010). The National Institute of Standards and Technology (NIST) has also published a guideline for security best practices for U.S. federal agencies (Shackelford et al., 2015). Cyber security controls and implementation guidelines were issued by the Department of Homeland Security for U.S. nuclear reactors. The guidelines are designed to assist in characterising cyber security posture, identifying gaps, and communicating risk management approaches (Christensen et al., 2021). Similarly, in the UK nuclear industry, the Office for Nuclear Regulation regularly issues security assessment principles as part of the Technical assessment guides (Guide, 2021) for the cyber-physical security of UK nuclear plants. The German approach (termed the GRS-best-practice approach) is based on the internationally-recognized graded approach that involves zoning computers according to four security levels, and applying similar security measures for each zone (Lochthofen and Sommer, 2015). The measure also involves the prohibition of data links in a high-level security zone and a secured data link in lower-level zones. Although this may present a common vulnerability to the computers in the same zone, as each zone has a single-entry point, it also has the advantage of being less intrusive and having easier security checks. The applicability of security mechanisms and standards defined by the international standardisation committees has been discussed in (Moreira et al., 2016). A practical security control implementation scheme for nuclear facilities in the development phase is suggested in (Park et al., 2016). It introduced four main activities, a cyber security team organisation, security assessment, security verification and validation during software development, and security evaluation.

The regulatory frameworks discussed above detail important cyber security controls in NPP. However, to properly consider the peculiarity of nuclear digital I&C, risk needs to be redefined in the context of I&C cybersecurity, and a formalized vulnerability assessment methodology needs to be created (Peterson et al., 2019). Moreover, most of the security controls are generic and lack the details about the NPP cyber security evaluation process that informs the standards. The evaluation process should typically include the threat assessment and vulnerability analysis for all attack surfaces discussed in Section 2. To bridge the gap, several NPP cyber security evaluation testbeds and emulators are being developed. More recently, many research institutes have established hardware-in-the-loop (HIL) testbeds to simulate different cyber-attacks to develop robust solutions to protect NPPs. Zhang et al. (2020), propose an architecture for nuclear power plant cyber security solution based on a HIL testbed. This architecture consists of a data collection and extraction system, a multilayer cyberattacks detection system, a causal analysis system with dynamic risk assessment, a cyberattack response system, and the main control room display system to provide a solution for prevention, detection, and response to cyberattacks on NPPs. The architecture was evaluated by simulating cyber-attacks on NPP DI&C.

The Sandia National Laboratory also developed a dynamic cyber-risk evaluation tool for cyber failure and time-sequenced cyber-risk analysis (Wheeler et al., 2017). The tool is composed of network and communication modelling tools – Sceptre and Hacker. exe – and a process model developed with Melcore code. The tool allows novel attacks to be launched and exploits integrated into the NPP accident sequence simulator. An experimental testbed based on the Emulab tool and Simulink was also proposed for the security evaluation of both cyber and physical assets (Genge et al., 2012). The coupling effect and the performance were evaluated on a water plant and the Tennessee Eastman process. The University of New Mexico's Institute for Space and Nuclear Power Studies in collaboration with Sandia National Laboratories has been developing a Nuclear Instrumentation & Control Simulation platform as presented in (El-Genk et al., 2021). This platform is to investigate the response and identify vulnerabilities of digital instrumentation and control systems for NPPs to potential cyberattacks. The developed pressurizer model which is linked to the pressure and water level control PLCs can be used to conduct cyber security investigations.

One of the most comprehensive nuclear power plant cyber security evaluation tools found in the literature is the Asherah Nuclear Simulator (ANS). The simulator is a full-scope mathematical model of a two-loop 2772 MWt pressurised water reactor nuclear power plant implemented with MATLAB/SIMULINK (Silva et al., 2020a). The communication link is modelled using open platform communications – universal architecture (OPC-UA) common in SCADA systems, with support for Fieldbus communication protocols. The attack initiation, data collection, storage, analysis and simulation control capability are enabled by the simulator. Also, the ANS has hardware-in-the-loop (HIL) capability that enables physical system/device integration. This HIL capability has been explored by Neal et al. (2020), to study attack impact on a boiler-level control system. The boiler level control system is a physical system that replaces the steam generator in the ANS, and attacks on the water level control PLC are considered.

The Asherah nuclear power plant simulator is also used (Silva et al., 2021) to simulate realistic cyber-attack scenarios and to evaluate the functional impact of these attacks on digital instrumentation and control systems for NPPs. Two realistic cyber-attack scenarios have run in the hardware-in-the-loop for a safety-security cyber-physical assessment. These scenarios show the need to consider the plant performance, related digital equipment, and all data communications to highlight possible cyber threats on digital instrumentation and control. The ANS is an important tool towards comprehensive cyber security evaluation of nuclear DI&C. However, the ANS scope is limited. First, considerable work needs to be done in implementing the ANS as a testbed, as the network configuration and other peripheral devices are not modelled. Moreover, controllers are also limited, as controller performance was not a fundamental requirement (Silva et al., 2020a). In addition, it is critical to be able to distinguish process changes from cyber-attacks and random faults, as the countermeasures and consequences are different (Ayodeji et al., 2020; Ayodeji). While ANS capability is extendable to component faults, its developmental requirements lack this capability.

4. Discussion

The opportunity presented by nuclear facility control system digitisation resolves interconnectivity and interoperability issues with legacy ICS systems. It also enables easier implementation of security controls, as opposed to the inferior security practices in legacy automation systems resulting from the cost and difficulty in retrofitting contemporary security measures. Considering the system interaction at various levels in nuclear facilities, cyber security concerns are best addressed by a comprehensive national and international security standard with a clear implementation procedure, informed by a detailed ICS security evaluation system. The reviewed literature has shown that there is a disconnect between the technical approach to cyber security and the regulations/policies that govern it. First, although the nuclear sector is heavily regulated with well-established security best practices, the implementation of the available standards depends on individual ICS characteristics. This makes the application of standards and guidelines use case dependent, which reinforces the need for a common position on the best approach to secure nuclear cyber assets. In addition, literature shows that several research projects are focused on securing high-level communication networks, while others are advocating for the highest security measures on the devices and low-level protocols that directly

interact with the physical layer (i.e., sensors and actuators). Supply chain, insider threats and human reliability concerns have also been raised, and interesting approaches proposed to secure NPPs from such attack surfaces.

The proposed approaches have prospects, however, there are some limitations. First, the proposed approaches are globalized, with little discussion on the localisation concept. Many research works are focused on securing a particular aspect of the control systems, without considering the consequences/impact on the adjacent, safety-critical systems. Secondly, most of the proposed tools/methods are designed to secure the systems against well-known, well-understood attacks. Incidentally, NPPs are high-stake systems, and attacks on such systems are almost always from well-organised and resourced attackers capable of developing novel attacks. Another factor that constrains the implementation of most of the proposed techniques is the low-fidelity models used in the proof of concept. Many of the case studies use simple industrial systems and open-source penetration testing tools which are too aggressive for ICS environments. For instance, several cyber security tools are applied to industrial tank liquid level controllers as the system of choice (Silva et al., 2020b), which does not represent the complexity of the nuclear power process system or the heightened consequence of a successful NPP attack.

Modelling a nuclear power plant is a complex process that involves integrating different sub-models which creates instabilities that are rarely considered in cyber-attack demonstrations and proof of concepts. These subtle abstractions in models are critical to properly study the system behaviour under attack. Moreover, a detailed threat/consequence assessment is necessary to ensure the graded approach to the proposed security measures. This is also to ensure that the protection strategy does not constitute additional complexity or vulnerability that may further affect NPPs' safety Also, the demand for NPP flexible operation and integration with other renewable sources will introduce additional complexity in the control of modern NPP DI&C, and a successful exploit of the nuclear process that results in a sudden plant shutdown would impact the grid stability.

Proposed NPP cyber security framework.

Conducting cyber security evaluation on real-world nuclear DI&C is unsafe and developing a full-scope physical testbed for research and development (R&D) purposes is expensive. Nevertheless, to design an adequate cyber security measure, there is a need to develop the capacity to emulate the components, devices, and networks in digital ICS, study the vulnerabilities and dependency issues, simulate potential attacks, evaluate the consequences of a successful attack, and design an appropriate security measure.

The testbeds and frameworks discussed in Section 3 present a solid foundation for vulnerability analysis, testing, validation and security regulation of ICS. However, most of the test beds are not designed to emulate, simulate, and defend the level 0 and level 1 device that is critical to the nuclear SSEP functions. Moreover, the testbeds are limited in functionality, as they cannot mimic the distributed control in real-world NPP and observing reactor system response to attacks is difficult. Besides, access to most of the testbeds is restricted and the testbeds are purpose-built without detailed information about their use and results (Ani and Watson, 2021). This makes independent validation difficult and has created a poor landscape of case studies specific to nuclear DI&C.

Towards shrinking the NPP attack propagation path and developing a testbed that can support evidence-based security controls, this section discusses an R&D framework for developing an attack-resilient control and cyber security of nuclear DI&C (termed attack-resilient control framework, ARCF). This framework involves distributed process control systems that mimic the configuration in the nuclear plant. Based on the ANS, the ARCF would be developed with a full-scope process model, fieldbus communication protocol, controllers, sensors, and actuators. However, the framework deviates from the ANS primary functionality, as the ARCF will prioritize the development of attack-resilient digital controllers, with a greater focus on the level 0 and level 1 components. As the system with the highest cyber security priority, the ARCF framework describes a concept for emulating digital control systems and designing known and novel attacks to study the vulnerability, system response and attack consequences on the plant, as shown in Fig. 2.

The framework shown in Fig. 2(a) describes cyber-physical experimentation and a test platform for the security and safety analysis of devices used for control functions (sensors, actuators, controllers, and their networks). First, a distributed mathematical model of each PCS in a generic PWR would be used, as implemented in ANS. The distribution would follow the control architecture of a real-world plant, as shown in Fig. 1. The model will address common modelling issues such as spatiotemporal neutron transport, delay neutron precursor, thermal-hydraulic, and reactivity feedback.

Secondly, a software-based PLC would be configured, programmed and integrated to mimic the steady-state operation of the process control systems. Away from the existing testbeds, the ARCF will have an inference system to differentiate between a cyber-attack and a random system fault, using a dedicated inference engine implemented in a data historian as shown in Fig. 2(b). This is important to ensure a cyber incident is not mistaken for a network glitch. The testbed will provide a platform where various cyber-attacks could be simulated on the sensor, actuator, controller and communication network. A Kalman filter would be developed to estimate the expected response $\widehat{y}$ of the system to the attack, and the expected response, $\widehat{y}$, would be compared with the real response y, for a particular process measurement. The residual t would be subjected to a statistical test to see if it lies within a threshold $\theta \leq t \leq \widehat{\theta}$. If the residual t is within the threshold, then the attack-resilient controller properly handles the attack. If otherwise, then other evaluations are done as shown in Fig. 2(b), and measures are applied based on the outcome of the evaluation.

4.1. The ARCF key objectives, scope, and application

The ARCF would enable a detailed analysis of the corresponding behaviour of the process system, and the connected devices. This also serves to create a robust platform to simulate different types of attacks and quantify the consequence on the controller functions, the SSEP, as well as the plant. The controllers' behaviour under each attack would inform the development of novel controllers that can perform SSEP functions under a similar attack. The emulation platform will also enable extensive simulation of different kinds of system faults and sensor anomalies resulting from random faults. The simulated faults and attacks will be the content of the fault (FCL) and attack (ACL) libraries as shown in Fig. 2(b). Then a data-driven classification model could be developed to discriminate between different kinds of attacks, and between attacks and faults in the ACL and FCL, based on the impact of the incident on the physical system. This consequence-based classification will be used to design security countermeasures and would inform the cyber threats that could be included in the reactor process control design basis threat. The development of the ARCF proposed in this work would address the following attacks on nuclear DI&C level 0 and level 1 devices (Weiss, 2010).

1. Loss of View (LOV): The LOV occurs when the attacker has partial or total control of sensor or actuator signals. The LOV attacks can mask the system states from the operator, creating a misoperation risk. This has been reported to cause NPP (Davis-Besse) shutdown in the case of a Slammer worm attack on the HMI.
2. Manipulation of View (MOV); The MOV attack results in operators making the wrong decision based upon erroneous information from sensors about the current system state. This is a Man-in-the-Middle attack that compromises sensor signal integrity by substituting the real signal with spurious measurements that force the operator to

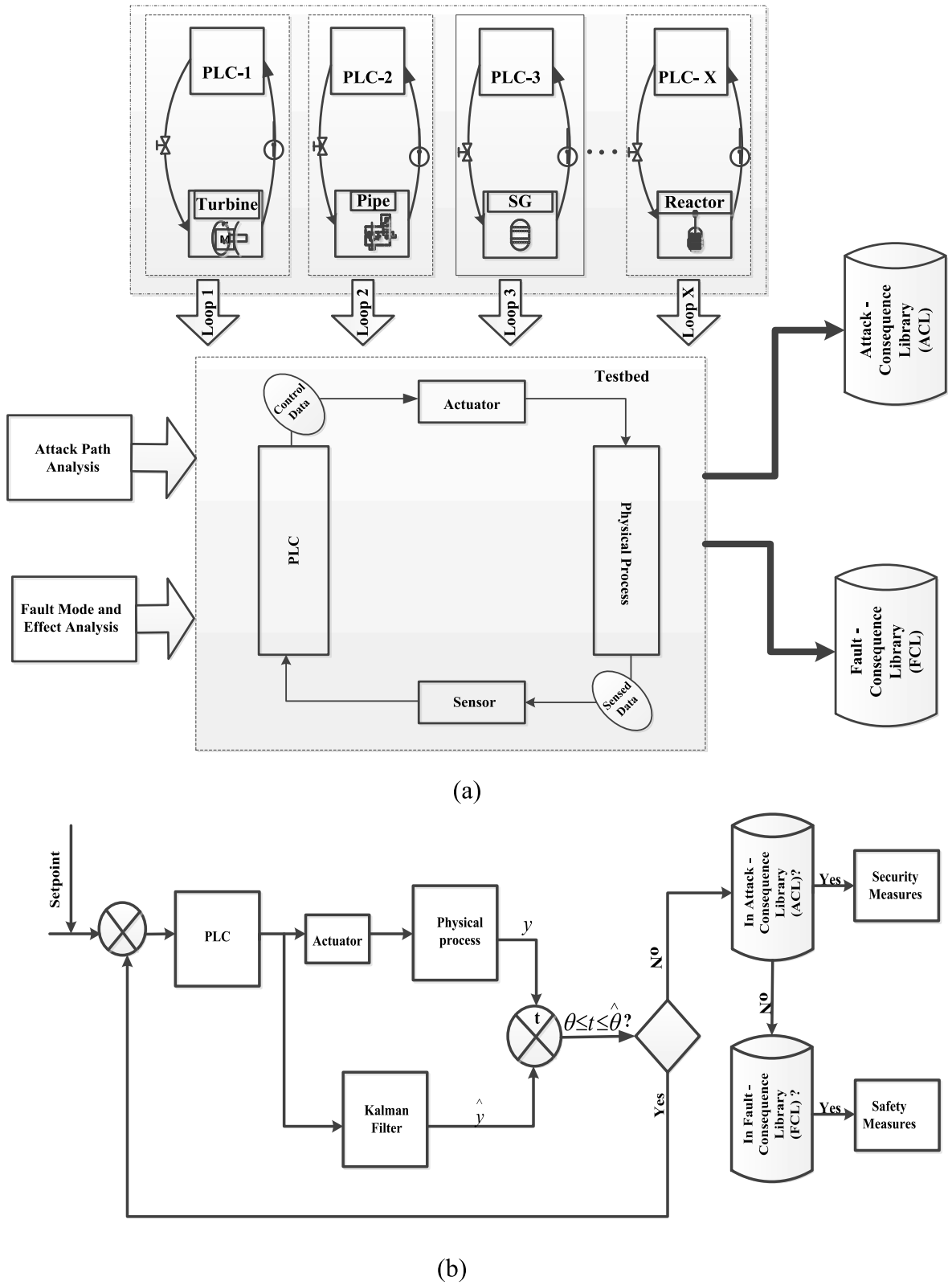

Fig. 2. The proposed framework for developing an attack-resilient control system evaluation tool with (a) ARCF testbed design, and (b) ARCF testbed implementation.

perform potentially harmful actions causing the operator to act erroneously due to signal manipulation.

3. Denial of Control (DOC): The DOC occurs when an attacker has partial or total control of the PLC. The DOC attack results in the PLC's inability to perform SSEP functions. The attack is also capable of denying the operators access to SSEP systems, aided by malware or worms that caused hardware failures, inadvertent setpoint change, or actuator damages.

The proposed ARCF would demonstrate the following capabilities.

1. Capability to formulate and simulate system faults.
2. Capability to formulate and simulate cyber-attacks (both novel and conventional attacks).
3. Capability to differentiate between system faults and cyber-attacks.
4. Capability to determine the optimal security strategy against high-consequence attacks.

As a major step to shrink the NPP DI&C attack surface, the activities required to develop the ARCF as depicted in Fig. 2 are distilled into the following nine tasks:

Task 1: Perform a comprehensive threat assessment for nuclear DI&C to understand the possible motivation and capability of the adversary.

Task 2: Perform a vulnerability analysis of the whole DI&C devices, both separately and jointly to ascertain common attack vectors.

Task 3: From a cyber security perspective, develop a complete model of each process control system and its networks (i.e., feedwater system, reactor core system, pressurizer pressure control system, nuclear steam supply system, power control system, etc.). This should provide the opportunity to simulate and emulate the DI&C components, devices, and communication protocols to properly study the system's weaknesses. Alternatively, implement the Asherah Nuclear Simulator in a virtual environment as a representation of the process control system.

Task 4: Develop a detailed fault consequence library (FCL) using updated literature on common faults or FMEA).

Task 5: Develop an attack and consequence library (ACL), first, from demonstrated vulnerability analysis, then using simulated attacks, build a comprehensive library of likely attacks on the system. The ACL is also useful to prepare for cyber-attack-related emergencies.

Task 6: Develop a data-driven model that can discriminate between contents in ACL and FCL. Distinguishing fault anomalies from attack signatures is critical to reducing the high false alarm rate.

Task 7: Design a novel controller that is resilient to the most consequential attacks.

Task 8: Evaluate the coupling effect and develop security measures for attacks that cannot be handled by the controller.

Task 9: Establish a nuclear DI&C baseline protective strategy for inclusion in the design basis threat.

The framework could be useful in developing a library of attacks that could affect the system's capability to perform the SSEP function. The proposed DI&C ARCF could also be used as a security testing tool for measuring the impact of security controls, patch/change management, verification and validation of new control system design and device upgrade, as well as a consequence-based asset prioritisation. In addition, analysis enabled by the ARCF could be used to identify the time interval between the attack and plant response, and the operational state of the reactor protection system (designed to initiate reactor scram in the event of abnormal plant operation). Based on the success and lessons learned from the ARCF, new cyber-attacks would be formulated to shrink the possibility of zero-day exploits. The ARCF could provide greater operator situational awareness, identify, and secure the most critical attack paths and respond to functional failures. It could also present an opportunity to devise a robust metric to quantify cyber risks and system security. The ARCF could also help incorporate critical attacks into process control system design basis threats and aid security by design approach to nuclear cyber security.

5. Conclusion

Digital transformation of nuclear facilities could unlock exponential improvement of facilities' performance and cost competitiveness. However, digital control and instrumentation in nuclear facilities could also have potential vulnerabilities that present cyber security challenges. Exploiting the vulnerabilities by a sophisticated threat actor may lead to the release of radioactive materials into the environment. This work presents a comprehensive overview of the existing body of knowledge on cyber security threats and defences for nuclear facilities. The work also examines the nuclear cyber security threats, vulnerabilities and inherent attack pathways that could aid malicious system intrusion. Analysis of existing nuclear digital I&C protection systems shows that the capability of the controllers to perform the SSEP functions under attack is not a prioritised research area.

Consequently, based on the analysis of identified gaps, the work suggests a conceptual framework for developing an attack-resilient control and cyber security analysis of NPP. This work serves to extend the existing knowledge on nuclear cyber security and provide a good foundation for future research in attack-resilient control of nuclear process systems. The work contributes to knowledge by analysing the relationship between attack propagation paths, associated vulnerabilities, and current security controls. The suggested framework for developing a robust cyberattack-resilient process control could guide researchers in evaluating novel controllers and developing new ways of protecting digital instrumentation and control in nuclear facilities.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgement

This work was supported in part by the Royal Society under grant SIF \R1\221035. The work of A. Ayodeji & H. Ahmed is funded through the Sêr Cymru II 80761-BU-103 project by the Welsh European Funding Office (WEFO) under the European Regional Development Fund (ERDF).

References

Ahn, W., et al., 2015. Development of cyber-attack scenarios for nuclear power plants using scenario graphs. Int. J. Distributed Sens. Netw. 11 (9), 836258.
Akinola, A.A., Kuye, A., Ayodeji, A., 2015. Cyber-security Evaluation for a Hypothetical Nuclear Power Plant Using the Attack Tree Method.
Alvaro, C., et al., 2009. Challenges for securing cyber physical systems. In: Workshop on Future Directions in Cyber-Physical Systems Security.
Ani, U.D., Watson, J.M., 2021. What makes an industrial control system security testbed credible and acceptable? Towards a design consideration framework. In: Proceedings of the 11th International Conference on Simulation and Modeling Methodologies, Technologies and Applications. SIMULTECH, 2021. SCITEPRESS.
Arnold, D., Ford, J., Saniie, J., 2022. Machine learning models for cyberattack detection in industrial control systems. In: 2022 IEEE International Conference on Electro Information Technology (eIT). IEEE.
Ashibani, Y., Mahmoud, Q.H., 2017. Cyber physical systems security: analysis, challenges and solutions. Comput. Secur. 68, 81–97.
Ayodeji, A., Machine Learning Approach to Industrial Control System Health Monitoring and Cyber Security: Similarities, Conflicts and Limitations.
Ayodeji, A., 2014. Cyber-security Evaluation for a Hypothetical Nuclear Power Plant. University of Port-Harcourt.
Ayodeji, A., et al., 2020. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. Nucl. Eng. Technol. 52 (12), 2687–2698.
Baba, M.S., et al., 2022. A review of human reliability programs for nuclear security. J. Nucl. Mater. Manag. 49 (4), 64–77.
Bhamare, D., et al., 2020. Cybersecurity for industrial control systems: a survey. Comput. Secur. 89, 101677.
Bodel, W., Butler, G., Matthews, J., 2021. Nuclear energy for net zero: a strategy for action. District heating 1, 2.
Camp, N., Williams, A.D., 2019. Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat Mitigation in Nuclear Facilities. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
Camp, N., Williams, A.D., 2020. A New Approach to Insider Threat Mitigation: Lessons Learned from Counterintelligence Theory. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
Cho, H.S., Woo, T.H., 2017. Cyber security in nuclear industry–Analytic study from the terror incident in nuclear power plants (NPPs). Ann. Nucl. Energy 99, 47–53.
Christensen, D.N., et al., 2021. Technical Guide for Implementing Cybersecurity Continuous Monitoring in the Nuclear Industry. Pacific Northwest National Lab. (PNNL), Richland, WA (United States).

Collet, J., Lorin, A., 2018. Multinational design evaluation programme: 10 year-achievements. In: Topical Issues in Nuclear Installation Safety. Safety Demonstration of Advanced Water Cooled Nuclear Power Plants. Proceedings of an International Conference vol. 2.
Denman, M.R., et al., 2016. Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model. Sandia National Lab. (SNL-NM), Albuquerque, NM (United States).
Dunlap, S., et al., 2016. Using timing-based side channels for anomaly detection in industrial control systems. International Journal of Critical Infrastructure Protection 15, 12–26.
Eggers, S., 2021. A novel approach for analyzing the nuclear supply chain cyber-attack surface. Nucl. Eng. Technol. 53 (3), 879–887.
Eggers, S.L., Rowland, M., 2020. Idaho national lab.(INL), Idaho falls, ID. In: Deconstructing the Nuclear Supply Chain Cyber-Attack Surface (United States).
El-Genk, M.S., Altamimi, R., Schriener, T.M., 2021. Pressurizer dynamic model and emulated programmable logic controllers for nuclear power plants cybersecurity investigations. Ann. Nucl. Energy 154, 108121.
Elakrat, M.A., Jung, J.C., 2018. Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network. Nucl. Eng. Technol. 50 (5), 780–787.
Genge, B., et al., 2012. A cyber-physical experimentation environment for the security analysis of networked industrial control systems. Comput. Electr. Eng. 38 (5), 1146–1161.
Guide, O., 2021. Effective Cyber and Information Risk Management, vol. 1, p. 15. CNS-TAST-GD-7.
Hashemian, H., 2011. Nuclear Power Plant Instrumentation and Control. Nuclear Power–Control, Reliability and Human Factors. InTech, pp. 49–66.
He, H., et al., 2021. Adaptive attack-resilient control for Markov jump system with additive attacks. Nonlinear Dynam. 103 (2), 1585–1598.
Hobbs, C., Moran, M., 2015. Insider Threats: an Educational Handbook of Nuclear and Non-nuclear Case Studies. King's College London, pp. 1–40.
Huang, Y.-L., et al., 2009. Understanding the physical and economic consequences of attacks on control systems. International Journal of Critical Infrastructure Protection 2 (3), 73–83.
Illiashenko, O.A., Broshevan, Y.V., Kharchenko, V.S., 2016. Cybersecurity case for FPGA-based NPP instrumentation and control systems. In: International Conference on Nuclear Engineering. American Society of Mechanical Engineers.
International Atomic Energy Agency, I, 2020. Preventive and Protective Measures against Insider Threats: Implementing Guide. IAEA.
Kesler, B., 2011. The vulnerability of nuclear facilities to cyber attack. Strategic Insights 10 (1), 15–25.
Khripunov, I., Speicher, C., 2018. Nuclear security culture as a tool to address insider threat. In: International Conference on Physical Protection of Nuclear Material and Nuclear Facilities. Summary of an International Conference. Annex. Supplementary Files.
Kim, D.-Y., 2014. Cyber security issues imposed on nuclear power plants. Ann. Nucl. Energy 65, 141–143.
Kim, H.E., et al., 2017. Systematic development of scenarios caused by cyber-attack-induced human errors in nuclear power plants. Reliab. Eng. Syst. Saf. 167, 290–301.
Kim, S., et al., 2020. Cyber attack taxonomy for digital environment in nuclear power plants. Nucl. Eng. Technol. 52 (5), 995–1001.
Kordy, B., Piètre-Cambacédès, L., Schweitzer, P., 2014. DAG-based attack and defense modeling: don't miss the forest for the attack trees. Computer science review 13, 1–38.
Krotofil, M., et al., 2014. CPS: driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals. In: Proceedings of the 30th Annual Computer Security Applications Conference.
Lemaire, L., et al., 2014. A SysML Extension for Security Analysis of Industrial Control Systems.
Li, W., et al., 2016. False sequential logic attack on SCADA system and its physical impact analysis. Comput. Secur. 58, 149–159.
Li, Y., et al., 2018a. Development of Defenses against False Data Injection Attacks for Nuclear Power Plants. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
Li, X., et al., 2018b. A dynamic decision-making approach for intrusion response in industrial control systems. IEEE Trans. Ind. Inf. 15 (5), 2544–2554.
Li, Y., et al., 2022. Real-time monitoring for detection of adversarial subtle process variations. Nucl. Sci. Eng. 196 (5), 544–567.
Lochthofen, A., Sommer, D., 2015. Implementation of computer security at nuclear facilities in Germany. Prog. Nucl. Energy 84, 103–107.
Maccarone, L.T., D'Angelo, C.J., Cole, D.G., 2018. Uncovering cyber-threats to nuclear system sensing and observability. Nucl. Eng. Des. 331, 204–210.
Makrakis, G.M., et al., 2021. Vulnerabilities and Attacks against Industrial Control Systems and Critical Infrastructures arXiv preprint arXiv:2109.03945.
Moreira, N., et al., 2016. Cyber-security in substation automation systems. Renew. Sustain. Energy Rev. 54, 1552–1562.
Neal, C., et al., 2020. Advancements in Hardening the Cybersecurity Posture of Nuclear Power Plant Defence-In-Depth Network Architecture.
Nissen, C., et al., 2018. Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. MITRE CORP MCLEAN VA.
Park, J.W., Lee, S.J., 2019. Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants. Nucl. Eng. Technol. 51 (1), 138–145.
Park, J., Suh, Y., Park, C., 2016. Implementation of cyber security for safety systems of nuclear facilities. Prog. Nucl. Energy 88, 88–94.
Peterson, J., Haney, M., Borrelli, R., 2019. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. Nucl. Eng. Des. 346, 75–84.
Rowland, M.T., Quinn, E.L., Sladek, J.A., 2021. Development of a New IEC Technical Report on Cybersecurity Risk Management for I&C and ES in Nuclear Power Plants. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
Shackelford, S.J., et al., 2015. Toward a global cybersecurity standard of care: exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ 50, 305.
Shin, J., Son, H., Heo, G., 2017. Cyber security risk evaluation of a nuclear I&C using BN and ET. Nucl. Eng. Technol. 49 (3), 517–524.
Silva, R., et al., 2020a. Development of the Asherah Nuclear Power Plant Simulator for Cyber Security Assessment. International Conference on Nuclear Security, Vienna, Austria.
Silva, B., et al., 2020b. Understanding nuclear cyber security measures, risks and consequences: from tank levels to plant processes. In: Third International Conference on Nuclear Security: Sustaining and Strengthening Efforts. ICONS, 2020.
Silva, R.B., et al., 2021. Cybersecurity assessment framework for digital interface between safety and security at nuclear power plants. International Journal of Critical Infrastructure Protection 34, 100453.
Sklyar, V., 2012. Cyber security of safety-critical infrastructures: a case study for nuclear facilities. Inf. Secur. 28 (1), 98.
Son, J., Choi, J., Yoon, H., 2019. New complementary points of cyber security schemes for critical digital assets at nuclear power plants. IEEE Access 7, 78379–78390.
Song, S., et al., 2014. A Case Study on Cyber-Security Program for the Programmable Logic Controller of Modern Npps.
Sundaram, A., Li, Y., Abdel-Khalik, H., 2022. Denoising algorithm for subtle anomaly detection. Nucl. Technol. 208 (9), 1365–1381.
USNRC, 5.71, 2010. Cyber Security Programs for Nuclear Facilities. US Nuclear Regulatory Commission, Washington, DC.
Vaddi, P.K., et al., 2020. Dynamic bayesian networks based abnormal event classifier for nuclear power plants in case of cyber security threats. Prog. Nucl. Energy 128, 103479.
Van Long, D., Fillatre, L., Nikiforov, I., 2015. Sequential monitoring of SCADA systems against cyber/physical attacks. IFAC-PapersOnLine 48 (21), 746–753.
Varuttamaseni, A., Bari, R., Youngblood, R., 2017. An Approach for Evaluating the Consequence of Cyber Attacks on Nuclear Power Plants. Brookhaven National Lab. (BNL), Upton, NY (United States).
Wang, W., et al., 2018. A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. Reliab. Eng. Syst. Saf. 175, 24–37.
Watson, V., et al., 2018. Example of graded and lifecycle phase-specific security controls for nuclear I&C and EPS use cases. In: International Conference on Nuclear Engineering. American Society of Mechanical Engineers.
Weiss, J., 2010. Protecting Industrial Control Systems from Electronic Threats. Momentum Press.
Weiss, J., Stephens, R., Miller, N., 2022. Changing the paradigm of control system cybersecurity. Computer 55 (3), 106–116.
Wheeler, T., et al., 2017. Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis (LDRD 17-0958) FY17 Report. SAND2017-10307. Sandia National Laboratories, Albuquerque, NM.
Yang, A., 2022. Discussion on functional safety and cyber security of I&C system in nuclear facilities. In: International Conference on Nuclear Engineering. American Society of Mechanical Engineers.
Zhang, F., Coble, J.B., 2020. Robust localized cyber-attack detection for key equipment in nuclear power plants. Prog. Nucl. Energy 128, 103446.
Zhang, F., Hines, J.W., Coble, J.B., 2020. A robust cybersecurity solution platform architecture for digital instrumentation and control systems in nuclear power facilities. Nucl. Technol. 206 (7), 939–950.
Zhao, Y., Smidts, C., 2020. A control-theoretic approach to detecting and distinguishing replay attacks from other anomalies in nuclear power plants. Prog. Nucl. Energy 123, 103315.
Zhou, Y., et al., 2019. A secure control learning framework for cyber-physical systems under sensor attacks. In: American Control Conference (ACC). 2019. IEEE.