Cybersecurity in Industrial Control Systems: Issues, Technologies, and Challenges

Muhammad Rizwan Asghar

School of Computer Science, The University of Auckland

Qinwen Hu

School of Computer Science, The University of Auckland

Sherali Zeadally

College of Communication and Information, University of Kentucky

Abstract

Industrial Control Systems (ICSs) play an important role in today's industry by providing process automation, distributed control, and process monitoring. ICS was designed to be used in an isolated area or connected to other systems via specialised communication mechanisms or protocols. This setup allows manufacturers to manage their production processes with great flexibility and safety. However, this design does not meet today's business requirements to work with state-of-the-art technologies such as Internet-of-Things (IoT) and big data analytics. In order to fulfil industry requirements, many ICSs have been connected to enterprise networks that allow business users to access real-time data generated by power plants. At the same time, this new design opens up several cybersecurity challenges for ICSs.

We review possible cyber attacks on ICSs, identify typical threats and vulnerabilities, and we discuss unresolved security issues with existing ICS cybersecurity solutions. Then, we discuss how to secure ICSs (*e.g.,* using risk assessment methodologies) and other protection measures. We also identify open security research challenges for ICSs, and we present a classification of existing security solutions along with their strengths and weaknesses. Finally,

Email addresses: r.asghar@auckland.ac.nz (Muhammad Rizwan Asghar), qhu009@aucklanduni.ac.nz (Qinwen Hu), szeadally@uky.edu (Sherali Zeadally)

we provide future research directions in ICS security.

Keywords:
Cybersecurity in ICS, Industrial Control System, Risk Management Strategies, Threat Detection and Prevention, Vulnerability Assessment

1. Introduction

Traditionally, Industrial Control Systems (ICSs) have operated in isolated locations. The main focus of the traditional ICS is on system functions. Information and network security were not considered at the time of its design. However, this design has become very expensive to deploy, maintain, and operate remotely. With the development of Information and Communications Technology (ICT) and functional requirements, more ICSs have moved from an isolated network environment to a public network for enabling the remote control and supervision of infrastructures. At the same time, exposing insecure devices to public networks raises security issues as those devices are more vulnerable to external attacks [1, 2, 3]. To this end, several attacks against ICSs have been reported in the last decade. For instance, 12 people in Poland were injured from a security incident in 2008 [4] when a teenager caused four derailments with a modified television remote control. Another famous security incident is Stuxnet, a worm discovered in 2010 [5]. Stuxnet penetrated the Iranian nuclear power plant potentially through an infected USB and then propagated itself. Stuxnet broke the ICSs availability and caused the delay in power generation at the Iranian nuclear power plant. Then, a half decade later, hackers successfully compromised ICS systems belonging to three Ukrainian energy distribution companies and temporarily cut off electricity supply in December 2015 [6]. The existing security incidents [4, 5, 6] tell us that ICS security is closely connected with the real world, especially in power (including nuclear power), military, petroleum and petrochemical industry, rail transit, and other key infrastructures. Compared with traditional cyber attacks [7, 8, 9], which only bring economic losses to the victims or enterprises, ICS vulnerabilities may lead to unimaginable and catastrophic consequences, such as the uncontrollable explosion of nuclear power plants or power failure nationwide. As a result, ICS vulnerabilities can seriously affect industrial production, life and property safety in our daily life.

In the past, many studies have been conducted and there are several

security solutions [10, 11, 12, 13, 14, 15, 16, 17, 18] to defend against attacks on an ICS. The recent studies focus on the ICS security architecture [10, 11] and policies [12, 13], system vulnerabilities scanning [3, 15], authentication [14], access control [16], data encryption [17], and intrusion detection [18]. State-of-the-art technologies [19, 20, 21] are used to ensure Confidentiality, Integrity, and Availability (CIA) of ICSs. In this article, we comprehensively review methods and techniques that have been proposed in the last 15 years. Then, we provide a comparative analysis of these different approaches based on their deployment and maintenance costs. Moreover, we highlight the advantages and disadvantages of each solution.

The rest of this article is organised as follows. Section 2 explains some common ICS systems, describes the components in an ICS environment along with the standard communication protocols used in the ICS environment. Moreover, we discuss some security issues related to the existing ICS infrastructure based on the ICS platforms, hardware, and protocols. Section 3 provides a trend of ICS security developments over the past 20 years and discusses various approaches. Section 4 presents our taxonomy for cybersecurity in ICSs and describes various security features and dimensions that we consider in our taxonomy. Furthermore, Section 4 classifies existing solutions (described in Section 3) into three categories: security evaluation models, intrusion detection and defence solutions, and risk assessment and metrics solutions, and analyse them based on their specific characteristics. Section 5 provides a comprehensive comparative analysis of existing ICS solutions based on their strengths and drawbacks and highlights research directions for future work. Finally, Section 6 concludes the article.

2. Overview of ICS Security

An ICS comprises different types of controllers used to control industrial plants as well as monitor their performance in order to assure their correct operations [22]. Figure 1 presents a 2-layer ICS. First, the logical layer contains the knowledge of high-level process logic for performing the process supervisory management. The second one, the physical control layer, encompasses several types of sensors and associated control protocols used for providing the communication interface with sensors and actuators. Unfortunately, ICSs have been increasingly facing threats [1, 2, 3] in the past few years, *e.g.,* social engineering attacks, which refer to malicious activities that trick the user in providing sensitive information, say passwords or pri-

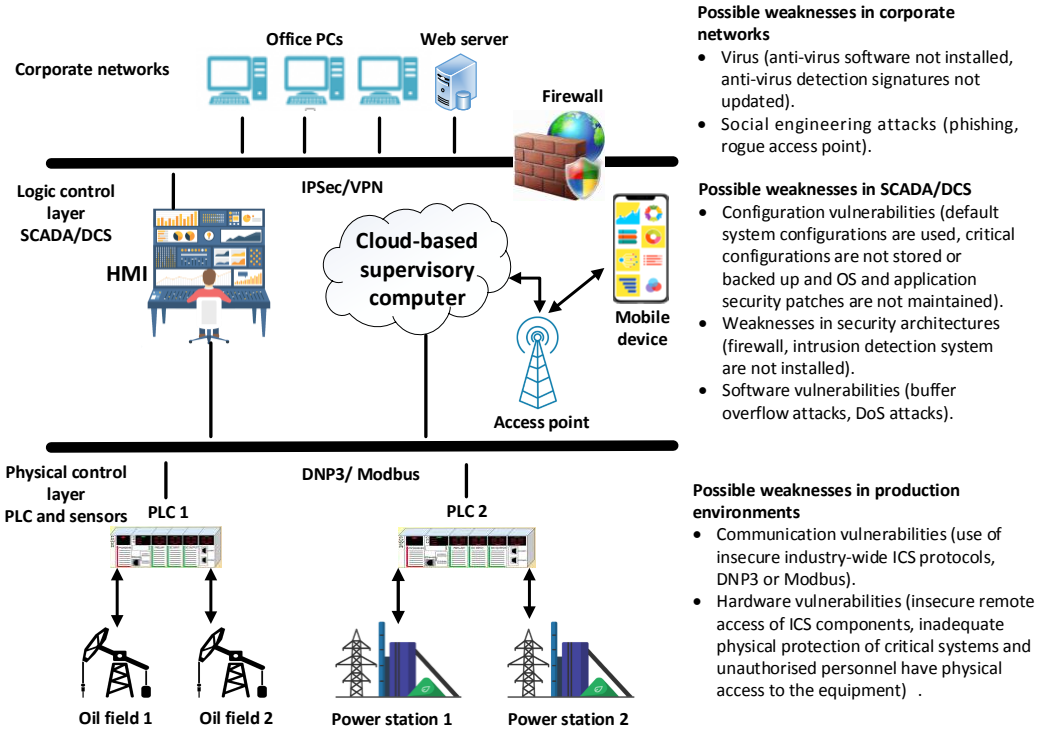

Figure 1: An overview of an Industrial Control System (ICS): A complete ICS infrastructure can be divided into three layers. At the corporate network layer, managers can remotely access a supervisory computer or a Human Machine Interface (HMI). In the logic control layer (*i.e.,* Supervisory Control and Data Acquisition (SCADA)/Distributed Control Systems (DCS) systems), system administrators use an HMI or a cloud-based supervisory computer to monitor the production status and send the command to update the control sequence. Furthermore, all control devices (*e.g.,* Programmable Logic Controllers (PLC) and sensors), protocols (*e.g.,* Distributed Network Protocol version 3 (DNP3)/Modbus), and production sites are categorised as the physical control layer.

vate keys. The stolen information can help hackers gain access to the target system and carry out a series of activities for bringing the system down.

In this section, we will describe the composition of ICS system types, devices, and communication protocols and highlight possible security risks.

2.1. ICS Components and Protocols

There are several types of ICSs. The well-known ICSs include Supervisory Control and Data Acquisition (SCADA) [23] systems, and Distributed Control Systems (DCSs) [24]. SCADA is designed for data acquisition and monitoring the production system. Furthermore, SCADA allows system administrators to control the remote sites via a centralised control system. Similar to SCADA, a DCS is formed by autonomous controllers that are installed across a manufacturing or production unit. A DCS system uses those controllers to monitor and supervise a unit remotely. However, SCADA is designed for managing the systems at multiple locations. A DCS is used to control production systems at one location. An ICS system consists mainly of a number of devices. One of ICS devices is a supervisory computer that communicates with the field controllers, *e.g.,* for collecting the information from each sensor and sending control commands to the controllers. Programmable Logic Controllers (PLCs) are the logic interface between the SCADA/DCS system and sensors. A PLC works with the supervisory system by receiving the control commands or returning the status of sensors. A Human Machine Interface (HMI) provides a Graphical User Interface (GUI) that allows a system administrator to interact with the controller hardware. An HMI displays the device status and historical data gathered by the sensors in the ICS environment. Moreover, an HMI allows system administrators to configure and deploy the new control algorithms to the controllers. In order to establish the connection between SCADA and PLCs, many ICS vendors have proposed specific communication protocols (such as Distributed Network Protocol (DNP3), which is widely used in electricity and wastewater treatment plants) that can be used for various ICS environments. SCADA systems use the DNP3 protocol to monitor and control the devices on site. Furthermore, Serial Modbus uses the high-level data link control standard to create a serial communication channel for PLCs. Moreover, Modbus-TCP uses the TCP/IP protocol to transmit data between PLCs and SCADA/DCSs.

2.2. ICS Vulnerabilities

In the last two decades, ICSs have been transformed and upgraded from a proprietary and isolated architecture to an open and standard platform, which is highly interconnected with the corporate and public networks. This development has opened up new opportunities (such as remote access to networks and ICS devices) but it has also made ICSs vulnerable to a wide range of cyber attacks [25]. The target of the attacks is not only security policies and procedures but also ICS hardware, software, platform, and network vulnerabilities. Figure 1 illustrates possible weaknesses in the ICS system. For example, if an employee's Personal Computer (PC) in a corporate network is infected by some virus due to no anti-virus software updated or installed at all, the whole ICS system can be affected via the Internet. Network configuration vulnerabilities (*e.g.,* the corporate network does not configure the access control lists properly in the firewall or sends the password in plain text) can also cause a system to be attacked and shut down. The attacks on ICS systems are not new. Looking at the report from Kaspersky [26], in 1997, only two vulnerabilities were published. However, this index increased to 19 in 2010. Since then, the number of vulnerabilities has significantly risen, 189 ICS vulnerabilities were found in 2015. In 2015 [6], 50% houses in Ukraine had electricity outage because of a cyber attack against the Prykarpattyaoblenergo power company. Another system intrusion attack was discovered in Kemuri Water company [27] when attackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water. Both incidents indicate that the intruders can find the vulnerable ICS components exposed to the Internet. As the number of ICS systems available over the Internet increases every year, it is crucial for ICS administrators to be aware of new vulnerabilities and threats, and actively improve the security of their ICS environments based on the existing technologies.

3. Review of ICS Security Solutions

Control systems have played an important role in critical infrastructures and industrial plants in the past few decades. However, microprocessors and embedded operating systems have started to replace the old physical controls, such as the relay controllers, while control systems are increasingly being connected to the Internet, thus making them more vulnerable than ever. In the following, we review existing ICS studies [10, 11, 12, 13, 14, 15, 16, 17, 18]

that highlight the cybersecurity incidents in the last two decades. Moreover, we present each incident and solution in chronological order to demonstrate the trends in ICS security research over the past two decades.

Requirements, Challenges, and Types. Cardenas *et al.* [28] report existing vulnerabilities in control systems that have been exploited. They present some standards for securing control systems including the North American Electric Reliability Corporation (NERC)'s cybersecurity standards for control systems [29] and the National Institute of Standards and Technology (NIST) guidelines [30] for ICSs. Basically, they identify three goals that these standardisation efforts are built upon: awareness of security issues in an ICS, helping control system operators in designing a security policy and recommending basic security mechanisms for prevention, and detection and response to security breaches. From a research point of view, they also differentiate between traditional Information Technology (IT) security and ICS security. The major differences they highlight include: (i) suitability of patching and frequent updates while planning the physical infrastructure set points; (ii) real-time availability provides a stricter operational environment than most traditional IT systems; and (iii) management of legacy ICS systems. They also identify some open issues, such as Maroochy Shire Council's sewage control system in Queensland, Australia [31] has been attacked in 2000. Stouffer *et al.* [22] provide an overview of an ICS, SCADA, and PLC as well as describe key components of an ICS. They list possible threats an ICS may face, such as inadequate policies and procedures for the ICS, no formal ICS security training, and no security audits of the ICS. Moreover, they define major security objectives, such as defining ICS specific security policies and procedures, performing risk and vulnerability assessment, and providing training and raise security awareness. They promote a defence-in-depth strategy for ICSs. They also describe adversarial threats to ICSs. For instance, Bot-network operators take over multiple systems to coordinate attacks and to trigger phishing, spam, and malware attacks. The phishers could be individuals or small groups that execute phishing attacks in an attempt to steal identities or information for monetary gain. Finally, they recommend some possible solutions. They suggest using a secure standard, which is an appropriate design for ICS environments. Besides, they suggest to move ICS networks away from enterprise networks. That way, if an enterprise network is under attack, the ICS network will not be affected. Furthermore, they discuss ICS security controls (*i.e.,* safeguards and countermeasures). Network

architecture, security controls, and risk assessment are among core aspects addressed by them.

Security Survey. Cyber attacks [1, 2, 3, 4, 5] have been continuously exposing industrial computer networks in recent years. Many security solutions [10, 11] in this field are based on detection and patch philosophy. In the past years, some studies [32, 33, 34] have assessed the existing industrial distributed computing system from the security point of view, such as Cheminod *et al.* [32] provide a detailed comparative analysis of a traditional IT system and an ICS. They differentiate both systems based on system characteristics, maintenance, upgrading, security practices and countermeasures, and also in terms of the impact of cyber attacks on both systems. They also discuss security requirements including confidentiality, integrity, and availability. Specifically, in an ICS, availability is the most important aspect whereas integrity and confidentiality come later. In contrast, in a traditional IT system, confidentiality is considered more important than integrity and availability. Besides, Cheminod *et al.* show how various aspects make an ICS critical as compared to an IT system and discuss risk assessment techniques for ICSs. For instance, a Hierarchical Holographic Model (HHM) [33, 34] is a methodology to decompose a complex system into separate subsystems according to requirements, each subsystem fulfils different needs. For instance, the technicians will have different views from the managers when discussing the long-term behaviour of the ICS system. Unlike HHMs, an Interoperability Input–output Model (IIM) [35, 36] is hierarchically decomposed into several subsystem. This infrastructure allows subsystems to interact with each other and share resources. Probabilistic Risk Assessment (PRA) [37, 38] covers two methodologies: deductive (backward) or inductive (forward) analysis. First, a deductive analyser analyses the affected system components. Then, it searches the attack or failure. An inductive analyser calculates all possible outcomes from a triggering event. In the context of ICSs, they review Intrusion Detection Systems (IDSs) in light of both performance and accuracy.

Syed *et al.* [39] present state-of-the-art results and trends of ICS security and challenges. They review some ICS solutions and highlight the opportunities to bring Cyber-Physical Systems (CPS) into our society. For instance, they discuss how to identify the ownership of access point in Mobile and Ad Hoc Networks (MANETs). Deng *et al.* [40] propose the public key infrastructure and identity-based cryptography to provide an authentication

service in MANETs. However, they point out that the solution requires a complicated certificate management process. In contrast, they present security concerns (such as combining the cyber-physical infrastructure with the healthcare system) of deploying CPS in our society. As a result, doctors can remotely monitor the essential parameters for diagnosing patients and conduct any necessary procedures or treatment based on the available information. They discuss the drawbacks once attackers compromise healthcare systems. One such drawback is that it could lead to life and financial losses. Finally, they highlight the challenges that need to be addressed for securing ICSs. These challenges include: how to reduce testing and integration time and costs in CPS and how to use cyber-physical infrastructure in green energy buildings and cities.

Sadeghi *et al.* [41] review security attacks, such as the Slammer worm [42] that completely stopped two critical monitoring systems of a nuclear power plant in the USA, which have occurred in the past two decades. They highlight attacks on ICSs that could cause physical damages and impact human life. Moreover, they describe the challenge of implementing security solutions in Cyber-Physical Production Systems (CPPS) such as the existing information security concepts are not suitable for CPPS as availability is a fundamental and real-time requirement for CPPS. The major challenge is how to keep the CPPS protected from the physical attacks, including invasive hardware attacks, side channel attacks, reverse engineering attacks, and other network attacks, such as Man-in-the-Middle (MitM) and Denial-of-Service (DoS) attacks. To address these challenges, they propose the use of a reliable security architecture, an integrity verification mechanism, and a secure user interface to manage physical devices.

Security Analysis. ICSs switch their operation from an isolated environment to other networks (*e.g.,* corporate networks and the Internet) for improving business processes. However, this change exposes the ICS to different types of cyber attacks. In the past, there have been several studies that suggest new solutions to mitigate these attacks [1, 2, 3, 4, 5], and there are studies that analyse the recent methodologies and research for measuring and managing those security risks [43, 44, 45, 46]. For example, Knowles *et al.* [43] provide a brief description of security standards, best practices, and guidelines. They discuss security metrics related to ICSs, such as Chew *et al.* [44] propose NIST800-55 that discusses how to evaluate the effectiveness of security programs. Stoddard *et al.* [45] introduce I3P metrics taxonomy

for ICSs. The I3P taxonomy categories security controls into 11 major areas and explains how ISO/IEC17799, ISA-TR99.00.01-2004(ISA-99), and the Information Security System Rating and Ranking (ISSRR) contributes to each of the major areas. They provide an overview of security research on ICSs and describe the European Union initiatives (*e.g.,* Framework Programmes – FPs in short) as well as academic research efforts. Finally, they share the current status of existing security standards used by the Process Control System (PCS) in the oil and gas industry. The found that only a few international or multinational (*e.g.,* EU-wide) standards address ICS security comprehensively.

Krotofil and Gollmann [46] present a survey on ICS security. They review the efforts of industrial researchers, which are grouped into diverse areas, such as secure control systems, simulations and modelling, IDS, and infrastructure and communications security.

Kisner *et al.* [19] provide a brief history of major developments in real-time DCSs. They discuss potential attacks and issues in real-time DCSs, and strategies to mitigate these attacks.

Lemaire *et al.* [20] propose an extension for the Systems Modelling Language (SysML) for enabling the extraction of vulnerabilities from an ICS model. Basically, a control system is initially modelled in SysML and then converted into an input for the proposed tool, which is a formal reasoning tool. The rules are based on the ICS-CERT vulnerability database and ICS security standards. They demonstrate that SysML enables users to quickly identify possible consequences of the attacks.

Leszczyna [47] presents a method for providing detailed information about the costs and resources required to develop, implement, and maintain an information security management system. Furthermore, Leszczyna proposes a security assessment scheme. This work considers a case study to explain the cost assessment for information security assurance activities. The proposed method is based on activity-based costing systems that consider activities as fundamental cost carriers and determine all activities of the security management process.

Vollmer and Manic [21] develop a self-configuring honeypot tool for the autonomous creation and update of a honeypot configuration as well as for monitoring and analysing the control system's network traffic.

They use Ettercap[1], an open-source network security tool. As a result, the proposed approach reduces operator interaction, minimises the impact of changing the existing infrastructure on the network, and increases security transparency.

Zimba *et al.* [48] investigate the danger of exposing ICSs to public networks. They design a multi-stage crypto ransomware attack and launch it by using the infamous *WannaCry* ransomware. The results obtained show that the attack can easily discover vulnerable nodes in different SCADA and production subnets. To this end, they recommend using a cascaded network segmentation with Demilitarised Zone (DMZ) in order to reduce the risk of exposing the devices connected to the production network.

Security Policies. A security policy indicates the rules of engagement for protecting organisations from the attacks. Several previous studies show that using security policies in an ICS can significantly address some existing issues [12, 13, 16]. For instance, Bertolotti *et al.* [12] propose a Role-Based Access Control (RBAC) model to address the growing demand in the ICS and SCADA areas for conjugating the high-level definition of policies with the low-level access control mechanisms in the system. RBAC specifies the high-level policy descriptions of policy characteristics. But Bertolotti *et al.* discover that RBAC was designed to deal with the high-level policy descriptions. However, if it is used to incorporate the details of system implementations in practice, it is less feasible. To address this issue, they propose this new RBAC solution. The new RBAC framework can refine RBAC policies into the actual system implementation, especially for the original access control mechanism. Moreover, they demonstrate that this solution can support different kinds of automatic security analysis.

Cheminod *et al.* [13] aim to help the high-level access control policy validation in the RBAC framework and the low-level security mechanism verification in the physical system. They propose a new approach that supports two distinct views: an RBAC based approach verifies the high-level policies specification and a low-level system description checks the correctness of the implementation of the policies.

Yalcinkaya *et al.* [16] use the Attribute-Based Access Control (ABAC) model to provide authorisation granularity, consolidate and monitor logging properties. The test results obtained demonstrate that this solution has

[1]https://www.ettercap-project.org

resolved the current and future ICS access control challenges.

Security Monitoring. Security monitoring refers to a process that collects and analyses data, logs, and/or traffic to identify security levels. The monitoring systems can help in avoiding economic losses resulting from unexpected attacks or failures, by improving system reliability and maintainability. Recently, many studies [49, 50, 51, 52] have applied this idea to ICS security. For instance, Auerswald *et al.* [49] design a course to help those who want to teach public policies, technical issues, and managerial principles. Their course is created based on the control systems' security, focusing on how to keep a critical infrastructure away from the attacks and how to recover quickly from attacks.

Salvadori *et al.* [50] present a digital monitoring and supervisory system to address the increasing demand for more efficient controlled electrical systems in the electric industry. The solution can work with both wireless and wired networks. The performance evaluation results demonstrate that the system can be used for monitoring and fault detection in electrical machinery as well as for extending network lifetime by putting a wireless sensor to the sleep state after transmission, regardless of the current battery capacity.

Gawand *et al.* [51] investigate how to detect and prevent attacks by analysing the complex data obtained from industrial plants. This solution analyses the trends of *convex hulls*[2] and the intersection in the controller's output, which can indicate an anomaly in a control system's behaviour.

Cruz *et al.* [52] present a shadow security unit to improve the communications security of current PLCs in ICSs. The idea is to integrate secure communication mechanism, authenticated access, and system integrity verification for addressing the limitation in PLCs. Besides, this new solution does not require significant changes to the existing control network.

Vulnerability Detection. Security vulnerabilities in ICSs may result in stealing of confidential data, breaching of data integrity, or affecting system availability. Thus, the task of detecting vulnerabilities in ICSs is one of the most urgent ones for now. In this direction, many studies [3, 15, 53, 54, 5] have focused on the full automation of the analysis that can discover known vulnerabilities in a network. For instance, the number of cyber attacks has been increasing especially when the traditional PLCs are being replaced with

[2]Convex hull is a computational geometric method.

personal computers. Cheminod *et al.* [3] design an automatic tool to reduce the number of cyber attacks caused by commodity computers replacing PLCs. Their solution analyses software vulnerabilities and provides a machine-readable description of vulnerabilities.

Stamp *et al.* [15] review the security incidents that occurred in the PCS for critical infrastructure. They identify most vulnerabilities caused by failures to identify and protect a security perimeter, build comprehensive security through defence-in-depth as well as budgetary pressure and employee attrition in system automation. Finally, they introduce effective mitigation strategies that include: improving security awareness, developing reliable and efficient security governance, and minimising security vulnerabilities through the careful configuration and integration of technology.

Attacks and Detection. Security systems play an important role in improving efficiency and reliability of ICSs. The traditional strategy is to deploy host-based or network-based security technologies to measure or analyse the well-known attacks from the past. However, a new attack can easily bypass this detection. As a result, how to design a system to detect new attacks has become a new research field. The traditional security mechanisms in the power system supervisory control or data acquisition systems are less secure because sophisticated attacks can bypass these security measures. Many existing studies [53, 54, 5] argue that there is a growing need for using a new cyber attack resilient control technique aimed at replacing the traditional cyber defence mechanisms for detecting highly skilled attacks. Sridhar and Govindarasu [53] propose a detection and mitigation technique based on the knowledge about the power system's operation. The solution was extended to an attack resilient Automatic Generation Control (AGC) that detects malicious data injection based on real-time load forecasts.

Drias *et al.* [54] conduct a detailed analysis of attacks on two of the most commonly used industrial control protocols, namely DNP3 and Modbus. They identify the security vulnerabilities in DNP3 and Modbus. They propose a taxonomy model that identifies attacks on both protocols. This solution simplifies the risk analysis related to cyber attacks on ICSs for both general and industrial control protocols.

Langner [5] provides a brief history of the first cyber warfare weapon ever, known as Stuxnet. He discusses the pre-requirements and steps for launching the Stuxnet worm. To detect and mitigate Stuxnet, Langner suggests not to use the vendor's driver Dynamic-Link Library (DLL) and to verify the

changes of an independent driver.

Morris and Gao [55] launch 17 attacks against SCADA by using the Modbus communication protocol in a laboratory setting. The attacks simulate four threats including reconnaissance, response and measurement injection, command injection, and DoS attacks. There is an experimental data set for each attack. This data was then subdivided into sub-classes based on attack complexity.

Huang *et al.* [56] evaluate the effects of launching combined attacks on a chemical reactor system. They discover that a DoS attack has a minimal impact on the system in a steady state, and the integrity attack aims to send false information from the sensor to the controller. As a result, the controller could process an incorrect action. In their study, Huang *et al.* analyse the case when an attacker launches the DoS attack combined with an innocuous integrity attack in the chemical reactor system. The results demonstrate that the combined attack can lead to serious consequences, such as a combination of the DoS attack and integrity attack can easily trigger the chemical reactor system moving to an unsafe state; consequently, it will increase the operational cost of the chemical reactor. So, they claim that attacks on control signals are more serious than attacks on the sensor signal. Further, they also investigate the economic consequences of attacking a target system, and discover that an attack on the plant economy involves a radically different strategy than an attack on plant safety.

Fleury *et al.* [57] create an Attack-Vulnerability-Damage (AVD) model to compare the attacks, vulnerabilities and damages in control systems. Furthermore, they use the model with an extensive survey of known attacks against control systems from industry, academia, and national laboratories. They suggest using this model to serve as a basis for developing a taxonomy of attacks against energy control systems.

Tupakula and Varadharajan [58] introduce a virtual machine monitor based solution for detecting attacks in critical infrastructures. Their solution monitors all the interaction on the systems and detects the attacks by comparing the system behaviours with the pre-defined security policies.

Yılmaz *et al.* [59] analyse a cyber attack detection solution in an experimental environment. They discover that signature-based prevention systems have the strength to detect well-known attacks. However, they are less effective to stop the new threats. In contrast, monitoring and detecting the network traffic in real-time can help network administrators to identify abnormal traffic. Then, they can adjust system norms and thresholds to prevent

malicious packets from infiltrating and damaging the system. Their experimental results demonstrate that detection-based solutions are more effective to detect new kinds of malware by continuous monitoring and behaviour-based testing of incoming and outgoing packets.

Authentication. Authentication is a core component to identify entities accessing sensitive or confidential information. To this end, many authentication solutions have been used for the PCS, such as Public Key Infrastructure (PKI), Internet Protocol Security (IPSec), and Transport Layer Security (TLS). However, these solutions have some deficiencies and cannot be directly applied to the control system. For instance, IPSec cannot be used for multicast transmissions. PKI's public key is dependent on the algorithms. As a result, it is not possible to change public key algorithms on top of pre-shared keys. Moreover, TLS does not support datagram traffic. To address these challenges, Chakravarthy *et al.* [14] discuss potential issues of maintaining a long-lived PCS. They address longevity needs of PCSs used in critical infrastructures by proposing new authentication protocols. The study demonstrates how to use the re-keying protocol to deliver fresher and stronger keys safely. Furthermore, the re-moduling protocol is robust against attackers who can determine the secure keys used in the current session.

Defence and Countermeasures. Previously, control system operational security gave communication security a low priority because the system was typically isolated from the external network. However, as more ICSs start to use corporate or public networks to share data, some cybersecurity issues have been detected, such as vulnerabilities in common protocols, backdoors and holes in the network perimeter. We review existing works that propose some defence strategies for addressing well-known ICS vulnerabilities. For example, Fabro and Nelson [10] briefly describe the contemporary control system architectures and identified the security challenges of configuring the control system as well as cybersecurity issues that need to be addressed. Finally, they recommend 'defence-in-depth' strategies that encourage organisations to use a multi-tier information architecture for maintaining control system networks. These strategies include: enabling remote access to facilities, providing public services for customer or corporate operations, and building a robust environment that requires connections among the control system domain, the external network, and other peer organisations.

The Process Control Security Requirements Forum (PCSRF) plays an important role in assessing the vulnerabilities in industrial process control

systems and establishing appropriate strategies for reducing IT security risk. By analysing the network architectures of computer-based control systems within process control industries, Falco *et al.* [11] summarise a general set of networking system architectures for industrial process control systems along with the vulnerabilities associated with these systems.

Fenrich [60] provides a high-level overview of IT security issues in ICSs. He discusses specific security threats followed by their potential consequences if they are used by attackers. He presents a comparison to show the differences between IT security and control system security. Moreover, Fenrich recommends several mitigation strategies for improving ICS security.

Harshe [61] proposes a Trustworthy Autonomic Interface Guardian Architecture (TAIGA) to enhance ICS security against reconfiguration and network attacks. This security solution consists of two parts: intrusion detection schemes and the backup controller. The intrusion detection scheme and conventional perimeter defences are employed to keep the ICS system away from the intruders. The backup controller works with a trigger mechanism whose main function is to monitor and prevent malware and switch to the backup controller before the attack occurs. However, because the backup controller and trigger mechanisms are embedded into the hardware, there is no way to reconfigure over the Ethernet channel.

Sainz *et al.* [62] use Software-Defined Networking (SDN) to enhance the security of industrial control networks. In their proposed solution, SDN switches block all traffic that is not explicitly specified in the flow tables. As a result, any unknown traffic is discarded.

Piedrahita *et al.* [63] use SDN to design an automatic incident response mechanism for ICSs. In their solution, if an attack is detected, the SDN controller reconfigures the routing that direct malicious traffic to an ICS honeypot network. Besides, if a sensor is compromised, the SDN controller can update the rules to drop the traffic from a compromised sensor.

Manson and Anderson [64] highlight some cybersecurity challenges that need to be addressed in a protection and control system. They discuss the most common cybersecurity issues in the protection and control system and recommend best practices based on their experiences. For instance, they suggest to keep security training for all employees and change the password regularly for improving security compliance, using SDN and protocol gateways to split large networks into multiple smaller, deterministic networks for stopping malicious traffic.

Introduction Detection System (IDS). An IDS provides the capability of monitoring systems activity and the ability to notify a responsible person when any malicious behaviour is detected. To this end, Coloured Petri Net (CPN) can assemble complex events from a stream of low-level events, such as system calls. Dolgikh *et al.* [18] use the CPN solution for bridging the gap between the low system views and program functionalities. Their proposed solution includes a mechanism capable of detecting hierarchical events with multiple links, such as one event has a relationship with multiple events. They demonstrate the possibilities of implementing the CPN solution in IDS approaches.

Zhou *et al.* [65] propose a novel multimode-based anomaly IDS to detect the intrusion in the control layer of the industrial process automation environment. The idea is to use complete multiple models of PCS that have been developed by integrating multi-domain knowledge to detect system anomalies and employs a Hidden Markov Model (HMM) to distinguish between an attack and a fault. Finally, they build a simulation platform to evaluate the performance and detection accuracy of the models they have developed. The experimental results show that the proposed solution yields good performance and few false alarms.

Lin *et al.* [66] develop a Modbus/TCP attack program against water level control and air pollution control along with a novel IDS solution. They argue that their proposed IDS approach could be used to mitigate the spoofing attack at the data link layer. They evaluate the solution with a variety of attacks.

Lin *et al.* [67] propose *Time Automata and Bayesian netwORk (TABOR)*, which is a graphical model that classifies anomalies if irregular patterns and dependencies are different from normal behaviour. This model uses time automata learning to discover the dynamic fluctuating behaviour of sensors along with the Bayesian network to identify dependencies between sensors and actuators.

An operation-based defensive architecture has been introduced to mitigate possible attacks on the Modbus control network. These attacks include: MitM and DoS attacks, replay attack, and unauthorised command execution attacks. However, a new challenge has been observed in the operation-based defensive architecture. The challenge is the inability of the system in detecting unauthorised remote access if the hacked device operates closely to its intended functions. In order to address the weakness of existing solutions, Robinson and Kim [68] propose a hybrid solution that integrates the

operation-based defensive architecture and the IDS. That is why, this solution is not only immune to the cyber infiltration but it is also strong in intrusion detection.

Nair *et al.* [69] propose a new approach that allows a network administrator to infer the malicious behaviours on an ICS device by monitoring network traffic emitted by an ICS device. They claim that when the CPU load of an ICS device reaches 70%, the machine will then slow down to generate the network traffic and its network traffic begins to exhibit noticeable delays. Moreover, they use the Machine Learning (ML) mechanism to learn normal resource usage from an ICS device, then monitor each ICS node for identifying deviations from normal resource usage. The advantages of using this solution include: no signature or rule updates are needed, no additional software needs to be installed on the ICS device, and it yields high accuracy.

Socio-Technical Security Analysis. In assessing the security posture of ICSs, existing studies focus on technical vulnerabilities [49, 20], the potential challenges from the social and organisational factors are often isolated. However, many attacks have used social engineers. Attackers might trick people in the target organisation to share their credentials for gaining access to sensitive information. Therefore, it is important to understand the challenges found at social (individuals) and organisational levels for the ICS deployment and maintenance. In this regard, Green *et al.* [70] design a method for understanding the technical, social, and organisation challenges across ICSs. They set up an empirical database to evaluate the new method and gain some insights into the organisational perspective on ICS security.

Green *et al.* [71] make use of a Mean Time-To-Compromise (MTTC) metric [72] to explore the potential impact of social engineering across a small European utility company. They find that the MTTC metric provides highly valuable insight into assessing ICS security but only to some extent in the overall security of ICSs. By allocating time estimations to social engineering attack vectors, they could provide the MTTC approach/metric with a more holistic perspective of ICS security.

To remove the boundary between Wireless Sensor Networks (WSNs) and an autonomic Digital Ecosystem (DE)[3], Vollmer *et al.* [73] describe a novel

[3]An autonomic digital ecosystem is a model for the future production systems, which enables the dynamic adaption based on user needs and environmental conditions. The whole design idea is to build the model on the notion of autonomic self-management by

implementation of the Autonomic Intelligent Cyber-Sensor (AICS) to identify anomalous network traffic as well as providing network entity information to the controllers outside the boundary of the sensor system. The network entity information could contain a list of IP addresses to monitor, information on network entities, and alerts on abnormal network traffic. The authors also deploy deceptive virtual hosts and implemented self-configuring modules these modules do what.

Risk and Assessment. Risk assessment can help the administrators to identify hazards and risk factors that have the potential to cause security issues or determine the appropriate strategy to eliminate the security issues or control the risk when the issue cannot be eliminated. Knowles *et al.* [74] interview ICS security engineers, analysts, and managers to access how to evaluate ICS security in the production. Most practitioners answered that the PASIV principles, covering Proximity, Accessibility, Safety, Impact, and Value, which are the most important factors to ensure the proper use of assurance techniques. *Proximity* requires that an assessor uses assurance techniques when evaluating the system on-site. *Accessibility* implies how to use assurance techniques to control the information that has high accessibility limitations. *Safety* means that the technique does not affect human and environmental safety. *Impact* indicates the assurance technique does not cause faults in live environments. Finally, *Value* means the outcome (*i.e.,* benefit) after applying an assurance technique for reducing security risks.

The PASIV principles are followed to ensure practitioners to use techniques safely. Furthermore, they provided a preliminary step that identifies assurance techniques that may be applied in different phases of the System Development Life Cycle (SDLC). Finally, they developed a mapping of assurance techniques to the high-level security families of ISO/IEC 27001:2013 that provides a reference and criterion for developing a holistic compliance standard for the security control in the future.

Green *et al.* [75] conduct interviews with security practitioners in order to identify the key phases applied to risk assessment. They also review current risk management approaches from both academia and industry as well as the challenges faced by these approaches.

A dynamic risk assessment system calculates ICS cybersecurity risk dynamically through analysis of real-time ICS data. Zhang *et al.* [76] propose

---

embedding exploitable control features within modules.

a Fuzzy Probability Bayesian Network (FPBN) approach to predict attack risks. In their solution, an FPBN uses fuzzy probabilities in order to address the limitation of insufficient historical data. Then, they introduce a new dynamic inference algorithm that can be used to reduce the impact of noise evidence caused by system faults. The overall results demonstrate the effectiveness of using the proposed approach in a chemical reactor control system.

Security Metrics. Security metrics provide insights for making an informed decision about infrastructure protection. Therefore, good metrics can lead to a good decision, while bad metrics can lead to bad security decisions. By reviewing the studies in the past, we observe a few cybersecurity metrics that have been proposed to improve the security in ICSs. A useful security metric can provide insight for managers to make better decisions that will lead to real security improvements. Boyer and McQueen [77] review seven abstract dimensions of security and provided one metric (or more) for each security issue. The metric defined is intended to identify the need for improved measurement tools because they are theoretically measurable and may become practical in the future as more advanced tools are developed. They demonstrate the impact of applying metrics to an operational control system as well as the further metrics under development.

Bustamante *et al.* [78] present several transitional IT standards aimed at protecting industrial and manufacturing enterprises from malicious activity. They suggest that some metrics from previous studies, such as Control Objectives for Information and Related Technologies (COBIT) and Project Management Body of Knowledge (PMBOK) [79, 80] could be used for enterprise strategy management, project management, ICS support and maintenance and ICS security guidelines.

Security decision-making plays an important role when attacks have been detected in ICSs. Many studies [81, 82, 83, 84] have focused on security decision-making in the past. However, these works have some weaknesses, such as the static decision-making solution allows the attacker to have a long time window, which improves the chance that the system could be attacked. On the other hand, the dynamic solution is based on the predefined rules that attackers can easily bypass. To solve the aforementioned problems, Qin *et al.* [85] introduce a novel dynamic decision-making solution that provides a security risk assessment method and indicates attack risk and degradation risk in the assessment result. Furthermore, a multi-step decision-making

approach architecture is formed by a state controller and an optimal defence strategy generator. The state controller ensures that ICS can be correctly degradation/upgradation as well as optimising the defence strategies. The optimal defence strategy generator chooses the best strategy to bring the system into an optimised state.

Trust in System-on-Chip(SoC). Nowadays, many ICS systems lack trust in software and hardware components. However, in order to avoid false data injection or rogue software, we need independent components to monitor and analyse malware. For this reason, Franklin *et al.* [86] propose the TAIGA platform to build trust between a PLC processor and a hardware-implemented interface controller. This architecture introduces malware resilience to the PLC for mitigating the following attacks: (1) malicious requests from the Master Terminal Unit (MTU); (2) false data injection; or (3) rogue PLC code [87].

Incidents and Lessons. Thousands of cybersecurity breaches against ICSs [1, 2, 3] have been discovered in past years: some large, many small, including some well-publicised ones [4, 5]. The vast majority of these attacks shared a primary objective, *i.e.,* bring the system down. By learning from previous attacks, system administrators can better understand the weaknesses of the existing defensive strategies and update security solutions to prevent attacks from happening again. To this end, Byres and Lowe [2] analyse the incident information from the British Columbia Institute of Technology (BCIT) industrial security incident database. They detect some events that occurred as a result of moving the SCADA systems from proprietary networks to public networks. The lessons that can be learned from these attacks are: (i) the threats originating from outside an organisation are likely to have very different attack characteristics compared to internal threats; and (ii) using open standards such as Ethernet, TCP/IP, and web technologies enable hackers to exploit vulnerabilities that exist in legacy networks and communication protocols. As a result, they recommended companies to reassess their security risk model by adding some security hardware.

Xu *et al.* [17] review and analyse some communication protocols that be widely used in an ICS. They point out security risks of using the protocols along with several attacks. For example, DNP3 [88] is an international standard developed to provide reliable data transmission and functions for ICSs. However, Xu *et al.* find that DNP3 lacks integrity, availability, and authentication, which can be attacked by MitM, DoS, and other attacks.

Moreover, they discuss the weakness of using Modbus [89], which is a standardised communication protocol between controllers and industry devices. Unfortunately, Modbus is vulnerable to spoofing or injection attacks because authentication and authorisation have not been considered in the original design. Xu *et al.* provide some solutions to mitigate such attacks. For instance, risk assessment can assess the impact or loss from a security incident, encryption algorithms can protect data integrity and confirm ownership of the data, and intrusion detection techniques can be used to detect abnormal behaviour.

Testbed Experimental Assessment of ICS security. The experimental testbed tools allow system administrators to simulate real control system hardware and software behaviours as well as evaluating the existing security solution by launching some well-known attacks in a virtual environment. For example, Genge *et al.* [90] review existing techniques that aim to enhance ICS security. They confirm the importance of defence-in-depth strategies and identify the security risk of software-defined-networking-enabled industry control networks. Finally, they argue that IP networking technologies can improve the security of ICS by deploying IDS/Intrusion Prevention System (IPS) and anomaly detection systems to analyse different network protocols and operating at different network layers.

Due to the lack of techniques to evaluate the security impact caused by both physical and cyber attacks, Genge *et al.* [91] present an experimental environment that allows users to simulate different physical hardware with real malware. The proposed approach set up a testbed that uses Emulab[4] to recreate cyber components. Besides, Simulink[5] is used for simulating physical processes.

To help reduce the security cost in the power grid, Nguyen [92] creates a simulation model that measures the economic impact of a cyber attack. Furthermore, the author highlights the dependence between the economic impact and the defence-in-depth strategies. To sum up, Nguyen's research results strengthen cybersecurity in the areas of power grids and methods,

[4]Emulab is a network testbed, giving researchers a wide range of environments for developing, debugging, and evaluating their systems: `https://www.emulab.net`

[5]Simulink is a graphical programming environment for modelling, simulating and analysing multi-domain dynamical systems: `https://www.mathworks.com/products/simulink.html`

simulation models, and recommend steps to increase the security of power grids.

Reaves and Morris [93] create a virtual testbed framework that contains independent ICS virtual devices, simulators, and logging devices. The idea is to use a laboratory test environment to simulate the network behaviour of an ICS. They find that virtual devices are capable of supporting many more protocols, which include Modbus/TCP and Modbus/ Remote Terminal Unit (RTU). The simulators simulate processes of a gas pipeline and a water storage tank control system. They also develop logging devices to create accurate captures of virtual system traffic and emulate the transmission characteristics of the medium.

Tao *et al.* [94] present a cloud-based platform that emulates network devices and simulates the physical layer. The network devices include HMIs and SCADA servers. The physical layer contains sensors, actuators, and other devices such as valves and generators. This platform is based on three modules: the first module provides a network interface to connect real devices; the second module allows users to configure the network resources; the third module links Simulink, which is widely used in the modelling and simulation of linear systems, non-linear systems, digital control, and digital signal processing. The proposed solution reduces the operational cost, and improves the authenticity of the security incidents when compared with the simulation software.

Green *et al.* [95] make an ICS testbed to simulate different equipments, such as sensors, controllers, actuators, and remote terminal units. They try to replicate end-to-end business processes, for example, observation and manual control of physical processes through HMIs, providing an interface to capture and store the data for further processing. Besides, by analysing the DMZ data, the long-term strategic planning can be made and the entire infrastructure can be supervised remotely. Furthermore, they also describe two common attack scenarios in the testbed environment, such as fuzzing, where the attacker randomly mutates well-formed inputs to test a program's resilience. Another example is memory modification that indicates modified data stored in memory.

By reviewing ten cybersecurity concerns associated with ICS, Vaughn and Morris [96] compare four types of ICS testing environments, which include implementation-based, emulation and implementation-based, federated simulation, and single simulation test beds. They highlight the federated simulation testbeds that can address the most important security concerns in

software and hardware development, implementation, and maintenance practices. They claim their solution is cheap to deploy. Moreover, they review virtual ICS test platforms and identify a set of weaknesses from the existing solutions that need to be addressed, such as how to make the communication protocols more robust, and make modern ICSs use application layer communication protocols, for instance Modbus/TCP, DNP3, and Profibus. However, many of these protocols were not designed with cybersecurity requirements in mind. For instance, digital signatures were not considered to ensure packet integrity. Additionally, there is a lack of cybersecurity tools for prevention and response to security incidents or vulnerability assessments for critical infrastructure ICSs .

Kalogeraki *et al.* [97] propose a Business Process Management Notation (BPMN) model to simulate a credible attack scenario in the maritime industry. They visualise operations and identify the interactions between SCADA systems in vehicular transportation systems. They present the BPMN model that can be used to emulate an attack scenario or a security risk that can occur in SCADA systems.

Green *et al.* [98] describe their experiences during the development of an extensive ICS testbed. They discuss how to overcome the labour cost and reduce the time to balance a range of design considerations such as Hardware-in-Loop (HIL), simulation, and virtualisation. They explain how to avoid typical pitfalls during the design and implementation of the testbed. Their solution addresses the issue of diversity, scalability, and managing complexity in the design phase of an ICS.

Process Control System (PCS). A PCS measures the system process, if something goes wrong, the system selects one of two operations based on the Settings. The first operation is to act immediately through actuators, for instance, adjusting the valves or pumps. The second operation is to send the alarm to system administrators. There several incidents [2, 99] about the system in the past. The number of security actions that are being taken by PCSs keeps growing. For example, Brundle *et al.* [100] outline and analyse the security challenges in securing PCSs and the response from the industry. These challenges highlight the need for process control and IT experts to build trust among them and work together. A well-defined security policy is foundational to any technical, procedural, or organisational security mechanism. Furthermore, they also point out the remaining issues, such as how to access and control remote embedded devices? and how to

reduce the cost of applying security solutions for smaller control systems? Moreover, they propose appropriate protection strategies to address these issues. For instance, these strategies include: security issue handling, security monitoring and evaluation, and maintenance.

4. Classification of Cybersecurity Solutions

In the previous section, we reviewed the ICS security solutions that aim to monitor and prevent the security risk in the ICS. Based on the primary goals of each solution, we classify the existing methodologies into three categories, we discussed each one in a subsection. That is, Section 4.1 describes security evaluation tools that provide safe experimentation with real malware test scenarios, the benefit of this is that users can spot security issues before the production. Section 4.2 highlights approaches for securing ICSs by introducing new components or by upgrading the existing architectures. Section 4.3 proposes standards, guidelines, and metrics for ensuring security protection implemented against evolving threats.

4.1. Security Evaluation Tools

As the demand for using scientific experiments to evaluate the impact of attacks against ICSs has increased, many researchers [10, 11, 12, 13, 14, 15, 16, 17, 18] in the ICS domain have proposed automated tools and environments that can simulate real control system hardware and software behaviours and provide a virtualised environment to model a single type of ICS, such as PLCs, DCSs, and SCADA [22, 52, 2]. Such autonomous tools can help system administrators to identify potential vulnerabilities of their ICSs' designs and enable them to develop solutions against identified vulnerabilities, and then distinguish between the normal and malicious traffic by using their private testing environments.

1. *Physical Devices* represent the actual devices in the ICS environment. A security evaluation tool [90] simulates different industrial environments, such as power systems, chemical systems, and hydraulic systems. The physical device comprises actuators, sensors, and hardware devices that perform the required physical actions on the system.
2. *Cyber Devices* provide capabilities for emulating PLCs or Master units' functionalities along with the industrial protocols such as Modbus,

DNP3, and Profibus [96]. As a result, users can use those cyber devices for acquiring data from the physical devices or for issuing the commands to the physical devices.

3. The Open Platform Communications (OPC) standard [101] is an industrial interoperability standard that was designed to allow different software packages to access data from a process control device. It defines a standard interface to reduce the amount of duplicated efforts in achieving specific requirements from different parties, such as integrating hardware manufacturers with their software partners, configuring SCADA and HMIs [102].
4. Vulnerability assessment allows administrators to identify all potential issues in the ICS environment [93]. The vulnerability assessment tools are able to: evaluate how resilient the network security is to attacks at the data link layer, monitor the network traffic in order to detect whether attackers can access sensitive information, discover the access control weaknesses, and analyse network infrastructure security levels.

4.2. Intrusion Detection and Prevention Technologies

Several studies [18, 65, 66, 103, 104] have focused on detecting and preventing attacks in ICSs. We classify these studies into two categories: intrusion detection and cryptography. The former classifies significant deviations from normal traffic as being malicious traffic. As a result, the various design approaches require a better understanding of normal behaviours and the states of the physical objects. The latter aims at creating a secure communication channel by protecting the traffic with encryption algorithms so that an attacker cannot read or modify the message without the private keys. So, this approach prevents adversaries from reading, modifying, injecting, and replaying network messages.

1. *Threat Detection* provides the capability of monitoring system activity and the ability to notify a responsible person when intrusion behaviours are detected. The systems can detect attacks based on the previous signatures, or upon detecting changes in configurations and activities.
2. *Threat Prevention* stops unauthorised modification and destruction of information, and the disclosure of malicious threats.
3. *Encryption* represents different encryption algorithms to translate a plaintext to an encrypted message that only allows authorised users to access it.

4.3. ICS Risk Management

Among the ICS security topics, security standards [12, 13, 11, 74] explicitly state the requirements to secure the ICS environment. The standards consist of policies, security concepts, security safeguards, and risk management approaches. The guidelines provide recommendations on the actions to be taken when attacks are detected. They also recommend the best practices and provide an overview of the most important security measures understandable by all users. The various metrics described in the guidelines can be used to evaluate cybersecurity strategies.

1. *Access Control Management* not only determines the users who can access the system but also sets the level of access permission. It ensures that only authenticated users can access and use specific applications, systems, and environments.
2. *Risk Management* is an assessment process that can be used to evaluate the impact of attacks. Besides, it also provides the best among many alternatives to minimise the impact of uncertain events.
3. *Security Metrics* are measurable properties that quantify the degree to which the security objectives of the system are achieved. Moreover, it analyses the relevant security attributes of ICSs.

Table 1: Comparison of the ICS solutions proposed in the past 15 years: we focus on each solution based on the research directions. We also show the cost of deploying and maintaining each solution. In the table, we use ✓and ✗ to indicate whether the proposed solution is related to the listed research direction or not, respectively. Moreover, we use "H" and "L" to indicate high and low costs of deploying/maintaining each solution, respectively.

Solutions	**Year**	**Intrusion detection & prevention**							**Security procedure**			**ICS simulators**			**Costs**	
	2003-2018	Security monitoring	Intrusion detection	Vulnerability detection	Authentication	Network layer solutions	Security architecture	Security policies	Risk assessment	Security metrics	Incidents and lessons	ICS equipment	ICS network devices	ICS attacks	Deployment cost	Maintenance cost
Stamp *et al.* [15]	2003	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Byres and Lowe [2]	2004	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	H	H
Auerswald *et al.* [49]	2008	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Boyer and McQueen [77]	2008	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	H	H
Cheminod *et al.* [3]	2009	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	H	H
Salvadori *et al.* [50]	2009	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Chakravarthy *et al.* [14]	2011	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Genge *et al.* [91]	2012	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	H	H
Bertolotti *et al.* [12]	2013	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	H	H
Cheminod *et al.* [13]	2014	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	H	H
Sridhar and Govindarasu [53]	2014	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	H	H
Tupakula and Varadharajan [58]	2014	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	H	H
Cruz *et al.* [52]	2015	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Gawand *et al.* [51]	2015	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Zhou *et al.* [65]	2015	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Genge *et al.* [90]	2015	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	H	H
Knowles *et al.* [74]	2015	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	H	H
Harshe [61]	2015	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Green *et al.* [95]	2016	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	H	H
Sainz *et al.* [62]	2017	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Manson and Anderson [64]	2017	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	H	H
Lin *et al.* [66]	2017	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Robinson and Kim [68]	2017	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Nair *et al.* [69]	2017	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Bustamante *et al.* [78]	2017	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	H	H
Green *et al.* [75]	2017	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	H	H
Xu *et al.* [17]	2017	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	H	H
Green *et al.* [98]	2017	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	H	H
Yılmaz *et al.* [59]	2018	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Piedrahita *et al.* [63]	2018	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Lin *et al.* [67]	2018	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	H	H
Qin *et al.* [85]	2018	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	H	H
Zhang *et al.* [76]	2018	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	H	H
Kalogeraki *et al.* [97]	2018	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	H	H

In Table 1, we classify the aforementioned solutions based on various features and costs. Specifically, we group the solutions based on the three categories that we define in this section. Some solutions are designed for providing a new security defence or a security detection approach, while others focus on a security policy or risk assessment. Furthermore, we discuss the cost of deploying these solutions to an existing ICS infrastructure along with the maintenance cost. From the perspective of deployment, if the solution is to optimise the existing hardware performance and does not change the existing infrastructure, we believe that the deployment cost is low and denote it using 'L'. On the other hand, if the proposed solutions need to replace the existing infrastructure or add a new device, we consider the deployment cost is very high and mark it 'H', because the new equipment needs time to integrate with the current system. Also, replacing the existing solution requires resources to test the new solution under different scenarios in the real environment. If we take all these factors into account, the deployment cost is very high. Typically, the cost for maintaining an optimised system is relatively low, because we already have existing maintenance steps and equipment. In contrast, for replacing a current solution or adding a new device, the maintenance cost will slightly increase, because all employees have to adjust from the current maintenance steps to new steps as well as the cost of purchasing new backup devices. According to our study, the environment and requirements of each ICS are different. For instance, some power plant security solutions [41, 92] are hard to apply to other areas because of the adjustments needed to accommodate different hardware and communication protocols in other control environments. Consequently, the costs of deploying and maintaining a new ICS security solution are high.

Table 2: An overview of ICS solutions: advantages and disadvantages.

ICS Solutions	**Advantages**	**Disadvantages**
Gegne et al. proposed solutions to simulate different ICS network hardware behaviour in a test environment [90, 91].	Gegne *et al.* filled the technical gap for evaluating the security impact caused by both physical and cyber attacks, their solutions simulate system behaviour in a test environment as well as ICSs security vulnerabilities.	The current study focused on the power sector and the chemical sector, no evaluation was made for other sectors. In addition, architectures and protocols need to be re-developed for new devices.
Green et al. [95, 98] created an ICS testbed to simulate different types of equipment, such as sensors, controllers, actuators, and remote terminal units.	Green *et al.* provided a GUI interface to simulate HMIs components and monitor the HMIs process.	Current solutions focus on cable networks, with limited support for wireless technologies and wireless sensors.
Kalogeraki et al. [97] proposed a BPMN model to simulate a credible attack scenario for the maritime industry.	Kalogeraki *et al.* used the BPMN model to evaluate security solutions or strategies against potential threats and vulnerabilities.	The solution only covers the maritime industry. Novel attacks cannot be simulated.
Many researchers used IDS solutions to detect attacks in various ICS infrastructures [65, 66, 67, 68, 69].	IDS can be used to monitor system activity, classify any abusive, abnormal, and malicious activity and notify a responsible person when any malicious behaviour is detected.	Novel attacks cannot be identified by signature-based IDSs and high false positives for anomaly detection approaches.
Many researchers [3, 12, 13, 58, 64] suggested to use different security policies for mitigating unauthorised access.	Those solutions can minimise the risk of data leak or loss as well as protect the organisation from "malicious" external and internal users.	The security policies are manually configured by system administrators; if a user misses one single area that should be protected the whole system could be compromised.
Data encryption solutions [14, 61] allow system administrators to encode sensitive data into another form in such a way that only authorised parties can access it.	Encrypted data maintains data integrity, ensures privacy, and reduces the risk of unauthorised data transfer from one device to another.	The drawbacks of using data encryption include high computation overheads as well as high costs for encryption solutions and securing maintaining security keys.
Security metrics [77, 78] provide insights to system administrators and can help them to make an informed decision about infrastructure protection.	The proposed solutions identify standard security requirements and the capabilities needed for secure solutions. Such solutions also offer a way to measure security strategies.	The existing security metrics solutions are tied to a specific security control mechanism. Furthermore, the metric-based solution has a built-in assumption that all vulnerabilities have the same impact assessment.
Risk assessment solutions [74, 75, 76] help the administrators to identify hazards and risk factors that have the potential to cause security issues.	The proposed solutions provide best practices to improve the quality of security by offering guidelines about how to identify the risk, how to analyse the risk, and how to evaluate the risk.	There are no uniform standards, and some standards and guidelines are not easy to understand by everyone.

5. Discussion and Future Work

We have learned several lessons from this survey. We grouped a set of cybersecurity solutions against ICSs into three categories: IDS, Risk Assessment and Metrics, and Security Simulation Tools based on their research directions and objectives. For instance, Zhou *et al.* [65] and Lin *et al.* [66] focus on the intrusion detection approaches. They propose a solution that trains on a set of normal network behaviours, and then use this model to detect anomalous behaviour in any traffic observed later. While, Knowles *et al.* [74] try to estimate and assess the security impact using a security risk assessment. Moreover, Genge *et al.* [90] claim that an ICS simulation environment is used to evaluate the system's vulnerability before releasing a solution to a production environment. Table 2 highlights the advantages and disadvantages of using each category in real-world. We provide an overview of different categories that aim to combine safety, cost, and security concerns. We have found that several ICS security solutions exist but there is still room for further research in multiple directions to improve existing solutions. For instance, the risk assessment methods for the SCADA system can be improved by addressing the context establishment stage of the risk management process. The false alarm rate of an anomaly-based IDS can be reduced by adding more training models to the existing solutions or by incorporating more samples to indicate normal network behaviours. We also identified other future directions, such as how to simplify the communication protocols in ICS networks and how to secure those smart devices.

5.1. Security Simulation Tools

The benefits of using simulation tools to evaluate the ICS solutions are undisputed. Users can easily build the DCS, PLC control system, or power grid dispatch systems in a virtual simulation environment. The simulation tool will automatically generate data and mimic real industry scenarios. Moreover, we recommend security countermeasures to address the potential security problems in the ICS design. All in all, the simulation tools provide an assessment of an attack, evaluate the defence effectiveness, simulate various attacks and defence scenarios, verify the system vulnerability, and provide security solutions. However, these tools need to support more equipment and protocols. Moreover, the cost of deployment and maintenance needs to be reduced.

5.2. Intrusion Detection and Prevention Technologies

IDS. With recent advancements in ICSs and cybersecurity issues [1, 2, 3, 4, 5], more research on IDS has been conducted in the past few years. Existing studies [18, 65, 66, 67, 69] have focused on signatures and rule-based IDSs and the anomaly-based IDSs. The signature-based IDSs are easy to deploy and understand if we have to detect known cybersecurity issues. Basically, a key advantage of using signature-based IDSs in ICS infrastructures is high accuracy of detecting the well-known attacks. Since the signature-based IDSs can only detect known attacks, novel attacks can easily bypass the detection. However, in regards to cybersecurity in ICSs, many attacks could be zero-day attacks; therefore, signature-based IDS solutions are less effective in detecting such attacks. In contrast, an anomaly-based IDS specifies the accepted network behaviour and uses them as a baseline for detecting malicious behaviour. Therefore, such as anomaly detection approach can be used to detect a new attack. But, since different vendors have introduced different protocols, it is very hard to define generic normal traffic patterns for all protocols. Therefore, some studies [65, 66] in the past focus on specific ICS solutions. Moreover, a high false rate is another major concern for not using the anomaly detection solution in ICSs.

ICS Standard Protocols. Currently, ICS standard protocols collect and measure the system status, and use control-layer protocols to configure the automation controller, and send new logic and update the code. However, the control-layer protocols are most of the time vendor-specific protocols, so one challenge here is how to design a control-layer that is more general but at the same time secure.

Secure Smart Devices. The main issue is if an attack compromises one smart device, then the infected device disrupts the normal operation of several other industrial equipment. Therefore, how to secure those smart devices remains a challenging yet important topic for future research.

5.3. Risk Assessment and Metrics

A security risk assessment covers the risk of equipment failure, personal safety risk, and potential cyber attacks. Depending on the security requirements of each company, the security department will design the appropriate procedures to analyse and evaluate the risk associated with their business. The risk assessment can help the company to decide on prioritising those

risks based on the internal and external constraints. When researchers consider the risk management and assessment in ICSs, they also discuss safety. Unfortunately, an unsafe environment can cause death, injury, and loss of equipment or property. Knowles *et al.* [74] mention that safety is the main consideration when we design an ICS system with a good security practice. Moreover, Knowles *et al.* also discuss the availability of services provided by the ICS. As a core critical part of the infrastructure, an ICS solution has to provide continuous and reliable operations. Therefore, the risk assessment has to evaluate the potential effects of disrupting an ICS operation and develop an incident recovery plan based on Knowles *et al.*'s assumptions. Furthermore, most recently attacks target physical devices such as Stuxnet [5] or cyber attacks on the Ukraine power grid [6].

5.4. Future Research Directions

Further research and investigations are still required for enhancing cybersecurity in ICSs, especially in the following areas:

IDS. We suggest considering several criteria when designing an IDS for an ICS environment. These criteria include adaptability, relevance, and operability. *Adaptability* indicates the solution can be adapted into an ICS without a high update/upgrade cost. *Relevance* refers to the solution that is designed for preventing all the well-known attacks. *Operability* requires that all features should be easily enabled or disabled and meet the real-time detection requirements. To this end, we recommend the use of a hybrid approach, where we can combine the advantages of both signature-based and anomaly-based solutions. The signature-based IDSs contain malicious patterns for current attacks. We can use different rule sets to train the anomaly-based IDSs for understanding the difference between normal traffic and anomalous traffic. Furthermore, leveraging sophisticated machine learning methods in IDS will be a new research direction. As we know, both attacks and protections are always improving. It is impossible to build IDSs for the ICS to solve all unknown security issues. With a self-learning ability, the IDS for ICSs can automatically adjust the detection rules in real-time according to the change in the detection environment. Consequently, this solution can enhance the performance and accuracy of IDSs in an ICS environment. Last but not least, the SDN solution has been introduced for the ICS protection in recent works such as [60, 62, 64], where researchers use SDN networks to isolate the malicious traffic. To this end, we can leverage SDN solutions

by using an SDN to split traffic into a particular IDS system based on the protocol so that each IDS can process specific traffic. As a result, it will improve the processing speed and reduce the packet drop rate [105].

Risk Assessment and Metrics. Based on the findings in this survey, we make some suggestions about how to evaluate the potential physical damages from a cyber incident. For instance, how an incident could manipulate the operation of sensors and actuators to impact the physical environment; redundant controls that exist in the ICS to prevent an impact; and how a physical incident could arise based on these conditions. After analysing the detailed risk assessment, the next step is to design an appropriate ICS security program, which is based on analysing security requirements and ICS technologies as well as deployment environments. In order to choose the right ICS security solution, we recommend that system administrators identify the hardware or software used in the target ICS system. For instance, SCADA [106] and DCS [22] represent the logical controller while PLCs and sensors represent the physical controller. Managers can remotely access a supervisory computer or HMIs. Second, we select ICS security controls [102], mainly based on the security categorisation of the ICS and the security requirement (such as the size of the organisation, the operation complexity, and the business requirements) for the ICS information program. After defining the security guidelines, we need to ensure that the security control is configured correctly, operating as intended, and the security requirements are met. To accomplish this, some researchers propose metrics, defined in standards such as ISO/IEC17799, NIST800-55 [45, 44], which help in assessing security control. The organisations can use or even modify these metrics based on their requirements for their ICS environments.

In short, in this section, we summarised the lesson that learned from this survey, highlighted the remaining security issues in three ICS security research categories, and proposed feasible solutions for resolving those issues for further study.

6. Concluding Remarks

Over the years, cyber attacks on ICS systems have been on the rise. Not surprisingly, ICS systems are becoming more vulnerable to security threats that compromise confidentiality, integrity, and availability of these systems. In this survey, we provide an overview of existing ICS cybersecurity approaches and we classify them into three categories based on their charac-

teristics, objectives, and solutions. First, we reviewed some existing studies that propose some security assessments, guideline and metrics that could help network administrators to predict the potential risk, guide them to find the best solution for protecting the ICS system from attacks or deliberate assaults. Then, the security metrics are used to assess the effectiveness of the solution to determine if it has achieved the desired effect. Although these solutions provide best practices to improve the security quality and an effective way to measure security strategies, they also reveal some issues, such as many risk assessment metrologies or metrics are tied with a specified security control mechanism, and no single method can be applied to any environment. Further, we analysed security solutions and we found that most of the security solutions were designed for a specific industrial control environment, where they address only one specific security issue. Moreover, several IDS solutions have low accuracy for detecting new malicious activities. Last but not least, the simulation tools or environments allow system administrators to assess systems' vulnerabilities before the deployment. The high costs and inconsistent evaluation models are major challenges in ICS simulation tools that still need to be addressed in the future.

Acknowledgements

We thank the anonymous reviewers for their valuable comments and suggestions, which helped us in improving the quality of our work.

7. Appendix

Table 3: Abbreviations and their descriptions.

Abbreviation	Description
AVD	Attack-Vulnerability-Damage
ABAC	Attribute-Based Access Control
AGC	Automatic Generation Control
AI	Artificial Intelligence
AICS	Autonomic Intelligent Cyber Sensor
AVD	Attack Vulnerability Damage
BPMN	Business Process Management Notation
BCIT	British Columbia Institute of Technology
Continued on next page	

Table 3 – continued from previous page

Abbreviation	Description
CIA	Confidentiality, Integrity, and Availability
COBIT	Control Objectives for Information and Related Technologies
CPN	Coloured Petri Net
CPPS	Cyber-Physical Production System
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
DCS	Distributed Control System
DE	Digital Ecosystem
DLL	Dynamic-Link Library
DNP3	Distributed Network Protocol version 3
DMZ	Demilitarised Zone
DoS	Denial-of-Service
FPBN	Fuzzy Probability Bayesian Network
GUI	Graphical User Interface
HHM	Hierarchical Holographic Model
HIL	Hardware In Loop
HMI	Human Machine Interface
HMM	Hidden Markov Model
ICSs	Industrial Control Systems
ICT	Information and Communications Technology
IDSs	Intrusion Detection Systems
IIM	Interoperability Input-output Model
IoT	Internet-of-Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPS	Intrusion Prevention System
ISSRR	Information Security System Rating and Ranking
IT	Information Technology
MANET	Mobile and Ad Hoc Networks
MitM	Man-in-the-Middle
ML	Machine Learning
MTTC	Mean Time To Compromise
MTU	Master Terminal Unit
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OPC	Open Platform Communications

Continued on next page

Table 3 – continued from previous page

Abbreviation	Description
PASIV	Proximity, Accessibility, Safety, Impact, and Value
PC	Personal Computer
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMBOK	Project Management Body of Knowledge
PRA	Probabilistic Risk Assessment
RBAC	Role-Based Access Control
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDLC	System Development Life Cycle
SDN	Software-Defined Networking
SoC	System-on-Chip
SysML	Systems Modelling Language
TABOR	Time Automata and Bayesian netwORk
TAIGA	Trustworthy Autonomic Interface Guardian Architecture
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WSN	Wireless Sensor Network

References

[1] U. P. D. Ani, H. He, A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective, Journal of Cyber Security Technology 1 (1) (2017) 32–74.

[2] E. Byres, J. Lowe, The myths and facts behind cyber security risks for industrial control systems, in: Proceedings of the VDE Kongress, Vol. 116, 2004, pp. 213–218.

[3] M. Cheminod, I. Bertolotti, L. Durante, P. Maggi, D. Pozza, R. Sisto, A. Valenzano, Detecting chains of vulnerabilities in industrial networks, Industrial Informatics, IEEE Transactions on 5 (2) (2009) 181–193.

[4] J. Leyden, Polish teen derails tram after hacking train network, The Register 11 (2008).

[5] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, Security Privacy, IEEE 9 (3) (2011) 49–51.

[6] D. U. Case, Analysis of the cyber attack on the ukrainian power grid, Electricity Information Sharing and Analysis Center (EISAC) (2016).

[7] R. Walters, Cyber attacks on us companies in 2014, The Heritage Foundation 4289 (2014) 1–5.

[8] L. Bonner, Cyber risk: How the 2011 sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches, Wash. UJL & Pol'y 40 (2012) 257.

[9] J. Jansen, R. Leukfeldt, Phishing and malware attacks on online banking customers in the netherlands: A qualitative analysis of factors leading to victimization, International Journal of Cyber Criminology 10 (1) (2016) 79.

[10] M. Fabro, T. Nelson, Control systems cyber security: Defense-in-depth strategies (2007).

[11] J. Falco, K. Stouffer, A. Wavering, F. Proctor, IT security for industrial control systems (2002).

[12] I. C. Bertolotti, L. Durante, T. Hu, A. Valenzano, A model for the analysis of security policies in industrial networks, in: Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013, ICS-CSR 2013, BCS, UK, 2013, pp. 66–77.

[13] M. Cheminod, L. Durante, L. Seno, A. Valenzano, On the description of access control policies in networked industrial systems, in: Factory Communication Systems (WFCS), 2014 10th IEEE Workshop on, 2014, pp. 1–10.

[14] R. Chakravarthy, C. Hauser, D. E. Bakken, Long-lived authentication protocols for process control systems, International Journal of Critical Infrastructure Protection 3 (3–4) (2010) 174 – 181.

[15] J. Stamp, J. Dillinger, W. Young, J. DePoy, Common vulnerabilities in critical infrastructure control systems, SAND2003-1772C. Sandia National Laboratories (2003).

[16] E. Yalcinkaya, A. Maffei, M. Onori, Application of attribute based access control model for industrial control systems, International Journal of Computer Network and Information Security 9 (2) (2017) 12.

[17] Y. Xu, Y. Yang, T. Li, J. Ju, Q. Wang, Review on cyber vulnerabilities of communication protocols in industrial control systems, in: Energy Internet and Energy System Integration (EI2), 2017 IEEE Conference on, IEEE, 2017, pp. 1–6.

[18] A. Dolgikh, T. Nykodym, V. Skormin, J. Antonakos, M. Baimukhamedov, Colored petri nets as the enabling technology in intrusion detection systems, in: MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011, 2011, pp. 1297–1301.

[19] R. A. Kisner, W. W. Manges, L. P. MacIntyre, J. J. Nutaro, J. Munro, P. D. Ewing, M. Howlader, P. T. Kuruganti, R. M. Wallace, M. M. Olama, Cybersecurity through real-time distributed control systems, Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30 (2010).

[20] L. Lemaire, J. Lapon, B. De Decker, V. Naessens, A SysML extension for security analysis of industrial control systems, in: Proceedings of the 2Nd International Symposium on ICS & SCADA Cyber Security Research 2014, ICS-CSR 2014, BCS, UK, 2014, pp. 1–9.

[21] T. Vollmer, M. Manic, Cyber-physical system security with deceptive virtual hosts for industrial control networks, Industrial Informatics, IEEE Transactions on 10 (2) (2014) 1337–1347.

[22] K. Stouffer, J. Falco, K. Scarfone, Guide to industrial control systems (ICS) security, NIST special publication 800 (82) (2011) 16–16.

[23] V. M. Igure, S. A. Laughter, R. D. Williams, Security issues in scada networks, computers & security 25 (7) (2006) 498–506.

[24] F.-L. Lian, J. Moyne, D. Tilbury, Network design consideration for distributed control systems, IEEE Transactions on Control Systems Technology 10 (2) (2002) 297–307.

[25] C. Alcaraz, S. Zeadally, Critical control system protection in the 21st century, Computer 46 (10) (2013) 74–83.

[26] W. Schwab, M. Poujol, The state of industrial cybersecuity 2018, Trend Study Kaspersky Reports (2018) 33.

[27] J. Leyden, Water treatment plant hacked, chemical mix changed for tap supplies, last accessed: Aug 18, 2019 (2016).
URL https://www.theregister.co.uk/2016/03/24/water_utility_hacked/

[28] A. A. Cárdenas, S. Amin, S. Sastry, Research Challenges for the Security of Control Systems, Usenix, 2008.

[29] NERC, North american electric reliability corporation (nerc) standards, last accessed: May 2, 2019 (2019).
URL https://www.nerc.com/pa/Stand/Pages/default.aspx

[30] NIST, Nist publishes final guidelines for protecting sensitive government information held by contractors, last accessed: May 2, 2019 (2015).
URL https://www.nist.gov/news-events/news/2015/06/nist-publishes-final-guidelines-protecting-sensitive-government-information

[31] J. Slay, M. Miller, Lessons learned from the maroochy water breach, in: International Conference on Critical Infrastructure Protection, Springer, 2007, pp. 73–82.

[32] M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks, Industrial Informatics, IEEE Transactions on 9 (1) (2013) 277–293.

[33] Y. Y. Haimes, Hierarchical holographic modeling, IEEE Transactions on Systems, Man, and Cybernetics 11 (9) (1981) 606–617.

[34] D. J. Leversage, E. J. Byres, Estimating a system's mean time-to-compromise, IEEE Security & Privacy 6 (1) (2008) 52–60.

[35] K. G. Crowther, Y. Y. Haimes, Application of the Inoperability Input—output Model (IIM) for systemic risk assessment and management of interdependent infrastructures, Systems Engineering 8 (4) (2005) 323–341.

[36] R. Setola, S. De Porcellinis, M. Sforna, Critical infrastructure dependency assessment using the input–output inoperability model, International Journal of Critical Infrastructure Protection 2 (4) (2009) 170–178.

[37] E. J. Henley, H. Kumamoto, Probabilistic risk assessment and management for engineers and scientists, IEEE Press (2nd Edition) (1996).

[38] M. Stamatelatos, H. Dezfuli, G. Apostolakis, C. Everline, S. Guarro, D. Mathias, A. Mosleh, T. Paulos, D. Riha, C. Smith, et al., Probabilistic risk assessment procedures guide for NASA managers and practitioners, NASA Technical Reports Server (2011).

[39] D. Syed, T.-H. Chang, D. Svetinovic, T. Rahwan, Z. Aung, Security for complex cyber-physical and industrial control systems: Current trends, limitations, and challenges, Pacific Asia Conference on Information Systems (2017).

[40] H. Deng, A. Mukherjee, D. P. Agrawal, Threshold and identity-based key management and authentication for wireless ad hoc networks, in: Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, Vol. 1, IEEE, 2004, pp. 107–111.

[41] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial Internet of Things, in: Proceedings of the 52nd annual design automation conference, ACM, 2015, p. 54.

[42] K. Poulsen, Slammer worm crashed Ohio nuke plant network, last accessed: May 2, 2019 (2003).
URL `https://www.securityfocus.com/news/6767`

[43] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, K. Jones, A survey of cyber security management in industrial control systems, International Journal of Critical Infrastructure Protection 9 (2015) 52 – 80.

[44] E. Chew, M. M. Swanson, K. M. Stine, N. Bartol, A. Brown, W. Robinson, Performance measurement guide for information security, National Institute of Standards and Technology Special Publications (2008).

[45] M. Stoddard, D. Bodeau, R. Carlson, C. Glantz, Y. Haimes, C. Lian, J. Santos, J. Shaw, Process control system security metrics–state of practice, I3P Institute for Information Infrastructure Protection Research Report 1 (2005).

[46] M. Krotofil, D. Gollmann, Industrial control systems security: What is happening?, in: Industrial Informatics (INDIN), 2013 11th IEEE International Conference on, 2013, pp. 670–675.

[47] R. Leszczyna, Approaching secure industrial control systems, Information Security, IET 9 (1) (2015) 81–89.

[48] A. Zimba, Z. Wang, H. Chen, Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express (2018).

[49] P. Auerswald, L. Branscomb, S. Shirk, M. Kleeman, T. Porte, R. Ellis, Critical infrastructure and control systems security curriculum, Department of Homeland Security, version 1 (73) (2008) 0–73.

[50] F. Salvadori, M. de Campos, P. Sausen, R. de Camargo, C. Gehrke, C. Rech, M. Spohn, A. Oliveira, Monitoring in industrial systems using wireless sensor network with dynamic power management, Instrumentation and Measurement, IEEE Transactions on 58 (9) (2009) 3104–3111.

[51] H. L. Gawand, A. Bhattacharjee, K. Roy, Online monitoring of a cyber physical system against control aware cyber attacks, Procedia Computer Science 70 (2015) 238–244.

[52] T. Cruz, J. Barrigas, J. Proenca, A. Graziano, S. Panzieri, L. Lev, P. Simoes, Improving network security monitoring for industrial control systems, in: Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, 2015, pp. 878–881.

[53] S. Sridhar, M. Govindarasu, Model-based attack detection and mitigation for automatic generation control, IEEE Transactions on Smart Grid 5 (2) (2014) 580–591.

[54] Z. Drias, A. Serhrouchni, O. Vogel, Taxonomy of attacks on industrial control protocols, in: Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on, 2015, pp. 1–6.

[55] T. H. Morris, W. Gao, Industrial control system cyber attacks, in: Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013, ICS-CSR 2013, BCS, UK, 2013, pp. 22–29.

[56] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, S. Sastry, Understanding the physical and economic consequences of attacks on control systems, International Journal of Critical Infrastructure Protection 2 (3) (2009) 73 – 83.

[57] T. Fleury, H. Khurana, V. Welch, Towards a taxonomy of attacks against energy control systems, in: Critical Infrastructure Protection, Springer, 2008, pp. 71–85.

[58] U. Tupakula, V. Varadharajan, Techniques for detecting attacks on critical infrastructure, in: Computing, Networking and Communications (ICNC), 2014 International Conference on, 2014, pp. 48–52.

[59] E. N. Yılmaz, S. Gönen, Attack detection/prevention system against cyber attack in industrial control systems, Computers & Security 77 (2018) 94–105.

[60] K. Fenrich, Securing your control system, in: 50th Annual ISA. POWID Symposium/17th ISA POWID/EPRI Controls & Instrumentation Conference, 2007, p. 11.

[61] O. A. Harshe, Preemptive detection of cyber attacks on industrial control systems, Ph.D. thesis, Virginia Tech (2015).

[62] M. Sainz, M. Iturbe, I. Garitano, U. Zurutuza, Software defined networking opportunities for intelligent security enhancement of industrial

control systems, in: International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain, September 6–8, 2017, Proceeding, Springer, 2017, pp. 577–586.

[63] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, S. J. Rueda, Leveraging software-defined networking for incident response in industrial control systems, IEEE Software 35 (1) (2018) 44–50.

[64] S. Manson, D. Anderson, Practical cybersecurity for protection and control system communications networks, in: Petroleum and Chemical Industry Technical Conference (PCIC), 2017, IEEE, 2017, pp. 195–204.

[65] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, X. Li, Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation, Systems, Man, and Cybernetics: Systems, IEEE Transactions on 45 (10) (2015) 1345–1360.

[66] C.-T. Lin, S.-L. Wu, M.-L. Lee, Cyber attack and defense on industry control systems, in: Dependable and Secure Computing, 2017 IEEE Conference on, IEEE, 2017, pp. 524–526.

[67] Q. Lin, S. Adepu, S. Verwer, A. Mathur, TABOR: A graphical model-based approach for anomaly detection in industrial control systems, Asia Conference on Computer and Communications Security (2018).

[68] D. Robinson, C. Kim, A cyber-defensive industrial control system with redundancy and intrusion detection, in: Power Symposium (NAPS), 2017 North American, IEEE, 2017, pp. 1–6.

[69] R. Nair, C. Nayak, L. Watkins, K. D. Fairbanks, K. Memon, P. Wang, W. H. Robinson, The resource usage viewpoint of industrial control system security: An inference-based intrusion detection system, in: Cybersecurity for Industry 4.0, Springer, 2017, pp. 195–223.

[70] B. Green, D. Prince, U. Roedig, J. Busby, D. Hutchison, Socio-technical security analysis of Industrial Control Systems (ICS), in: Proceedings of the 2Nd International Symposium on ICS & SCADA Cyber Security Research 2014, ICS-CSR 2014, BCS, UK, 2014, pp. 10–14.

[71] B. Green, D. Prince, J. Busby, D. Hutchison, The impact of social engineering on industrial control system security, in: Proceedings of

the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, ACM, New York, NY, USA, 2015, pp. 23–29.

[72] M. A. McQueen, W. F. Boyer, M. A. Flynn, G. A. Beitel, Time-to-compromise model for cyber risk reduction estimation, in: Quality of Protection, Springer, 2006, pp. 49–64.

[73] T. Vollmer, M. Manic, O. Linda, Autonomic intelligent cyber-sensor to support industrial control network awareness, Industrial Informatics, IEEE Transactions on 10 (2) (2014) 1647–1658.

[74] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, A. Rashid, Assurance techniques for Industrial Control Systems (ICS), in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, ACM, New York, NY, USA, 2015, pp. 101–112.

[75] B. Green, D. D. C. Prince, J. S. Busby, D. Hutchison, How long is a piece of string: Defining key phases and observed challenges within ICS risk assessment, Workshop on Cyber-Physical Systems Security and Privacy (2017).

[76] Q. Zhang, C. Zhou, Y.-C. Tian, N. Xiong, Y. Qin, B. Hu, A fuzzy probability bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems, IEEE Transactions on Industrial Informatics 14 (6) (2018) 2497–2506.

[77] W. Boyer, M. McQueen, Critical information infrastructures security: Second international workshop, critis 2007, málaga, spain, october 3-5, 2007. revised papers, in: J. Lopez, B. M. Hämmerli (Eds.), Critical Information Infrastructures Security: Second International Workshop, CRITIS 2007, Málaga, Spain, October 3-5, 2007. Revised Papers, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, Ch. Ideal Based Cyber Security Technical Metrics for Control Systems, pp. 246–260.

[78] F. Bustamante, W. Fuertes, P. Díaz, T. Toulkeridis, Integration of it frameworks for the management of information security within industrial control systems providing metrics and indicators, in: 2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON), IEEE, 2017, pp. 1–4.

[79] S. COBIT, A business framework for the governance and management of enterprise IT, Rolling Meadows (2012).

[80] K. H. Rose, A guide to the Project Management Body of Knowledge (PMBOK® guide) - fifth edition, Project management journal 44 (3) (2013) e1–e1.

[81] A. Cohen, Cyber (in) security: Decision-making dynamics when moving out of your comfort zone, The Cyber Defense Review 2 (1) (2017) 45–60.

[82] C. Gonzalez, N. Ben-Asher, D. Morrison, Dynamics of decision making in cyber defense: Using multi-agent cognitive modeling to understand cyberwar, in: Theory and Models for Cyber Situation Awareness, Springer, 2017, pp. 113–127.

[83] C. Zhong, H. Liu, A. Alnusair, Leveraging decision making in cyber security analysis through data cleaning, Southwestern Business Administration Journal 16 (1) (2017) 1.

[84] H. J. Wall, L. K. Kaye, Online decision making: Online influence and implications for cyber security, in: Psychological and Behavioral Examinations in Cyber Security, IGI Global, 2018, pp. 1–25.

[85] Y. Qin, Q. Zhang, C. Zhou, N. Xiong, A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems, IEEE Transactions on Systems, Man, and Cybernetics: Systems 99 (2018) 1–8.

[86] Z. Franklin, C. Patterson, L. Lerner, R. Prado, Isolating trust in an industrial control system-on-chip architecture, in: Resilient Control Systems (ISRCS), 2014 7th International Symposium on, 2014, pp. 1–6.

[87] C. Schuett, J. Butts, S. Dunlap, An evaluation of modification attacks on programmable logic controllers, International Journal of Critical Infrastructure Protection 7 (1) (2014) 61–68.

[88] M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, DNPSec: Distributed Network Protocol version 3 (DNP3) security framework, in:

Advances in Computer, Information, and Systems Sciences, and Engineering, Springer, 2007, pp. 227–234.

[89] I. Modbus, Modbus messaging on TCP, IP Implementation Guide v1.0a, North Grafton, Massachusetts (2004).
URL www.modbus.org/specs.php

[90] B. Genge, F. Graur, P. Haller, Experimental assessment of network design approaches for protecting industrial control systems, International Journal of Critical Infrastructure Protection 11 (2015) 24 – 38.

[91] B. Genge, C. Siaterlis, I. N. Fovino, M. Masera, A cyber-physical experimentation environment for the security analysis of networked industrial control systems, Computers & Electrical Engineering 38 (5) (2012) 1146 – 1161, special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing.

[92] C.-K. Q. Nguyen, Industrial control systems (ICS) & Supervisory Control & Data Acquisition (SCADA) cybersecurity of power grid systems: Simulation/modeling/cyber defense using open source and virtualization (2014).

[93] B. Reaves, T. Morris, An open virtual testbed for industrial control system security research, International Journal of Information Security 11 (4) (2012) 215–229.

[94] Q. Tao, M. Jiang, X. Wang, B. Deng, A cloud-based experimental platform for networked industrial control systems, International Journal of Modeling, Simulation, and Scientific Computing (2017) 1850024.

[95] B. Green, S. A. F. Frey, A. Rashid, D. Hutchison, Testbed diversity as a fundamental principle for effective ICS security research, SERECIN (2016).

[96] R. B. Vaughn Jr, T. Morris, Addressing critical industrial control system cyber security concerns via high fidelity simulation, in: Proceedings of the 11th Annual Cyber and Information Security Research Conference, ACM, 2016, p. 12.

[97] E.-M. Kalogeraki, N. Polemi, S. Papastergiou, T. Panayiotopoulos, Modeling SCADA attacks, in: Smart Trends in Systems, Security and Sustainability, Springer, 2018, pp. 47–55.

[98] B. Green, A. T. Le, R. Antrobus, U. Roedig, D. Hutchison, A. Rashid, Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research, 17th Workshop on Cyber Security Experimentation and Test (2017).

[99] D. Walker, Utility IT executives expect breach of critical SCADA systems, Pipeline & gas journal 233 (2) (2006) 24–27.

[100] M. Brandle, M. Naedele, Security for process control systems: An overview, IEEE Security & Privacy 6 (6) (2008) 24–29.

[101] T. O. Foundation, What is opc?, last accessed: May 2, 2019 (2019). URL `https://opcfoundation.org/about/what-is-opc`

[102] T. Macaulay, B. L. Singer, Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2016.

[103] G. Kabasele Ndonda, R. Sadre, A two-level intrusion detection system for industrial control system networks using P4, in: ICS-CSR 2018, 2018, p. 11.

[104] A. F. M. Piedrahita, V. Gaur, J. Giraldo, A. A. Cardenas, S. J. Rueda, Leveraging software-defined networking for incident response in industrial control systems, IEEE Software 35 (1) (2018) 44–50.

[105] Q. Hu, M. R. Asghar, N. Brownlee, Evaluating network intrusion detection systems for high-speed networks, in: Telecommunication Networks and Applications Conference (ITNAC), 2017 27th International, IEEE, 2017, pp. 1–6.

[106] C. Alcaraz, S. Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, International journal of critical infrastructure protection 8 (2015) 53–66.