A review of security assessment methodologies in industrial control systems

Qais Saif Qassim
College of Computer Science and Information Technology, Universiti Tenaga Nasional, Selangor, Malaysia

Norziana Jamil
Institute of Informatics and Computing in Energy, Universiti Tenaga Nasional, Selangor, Malaysia and College of Computer Science and Information Technology, Universiti Tenaga Nasional, Selangor, Malaysia

Maslina Daud
CyberSecurity Malaysia, Seri Kembangan, Selangor, Malaysia

Ahmed Patel
Department of Computer Science, Universidade Estadual do Ceara, Fortaleza, Brazil, and

Norhamadi Ja'affar
CyberSecurity Malaysia, Seri Kembangan, Selangor, Malaysia

Received 19 April 2018
Revised 11 June 2018
Accepted 30 June 2018

Abstract

Purpose – The common implementation practices of modern industrial control systems (ICS) has left a window wide open to various security vulnerabilities. As the cyber-threat landscape continues to evolve, the ICS and their underlying architecture must be protected to withstand cyber-attacks. This study aims to review several ICS security assessment methodologies to identify an appropriate vulnerability assessment method for the ICS systems that examine both critical physical and cyber systems so as to protect the national critical infrastructure.

Design/methodology/approach – This paper reviews several ICS security assessment methodologies and explores whether the existing methodologies are indeed sufficient to meet the cyber security assessment exercise required to validate the security of electrical power control systems.

Findings – The study showed that most of the examined methodologies seem to concentrate on vulnerability identification and prioritisation techniques, whilst other security techniques received noticeably less attention. The study also showed that the least attention is devoted to patch management process due to the critical nature of the SCADA system. Additionally, this review portrayed that only two security assessment methodologies exhibited absolute fulfilment of all NERC-CIP security requirements, whilst the others only partially fulfilled the essential requirements.

Originality/value – This paper presents a review and a comparative analysis of several standard SCADA security assessment methodologies and guidelines published by internationally recognised bodies. In

This research study is supported by the Ministry of Science, Technology and Innovation Malaysia (MOSTI) through DSTIN project and Tenaga Nasional Berhad through TNB Seed Fund 2016.

Information & Computer Security
Vol. 27 No. 1, 2019
pp. 47-61
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-04-2018-0048

addition, it explores the adequacy of the existing methodologies in meeting cyber security assessment practices required for electrical power networks.

Keywords Cyber attacks, Vulnerability analysis, Power systems, SCADA systems, Security assessment, Vulnerability analysis

Paper type Research paper

1. Introduction

The progress in telecommunication technologies and the need for enhanced functionality and efficacy that is cost-effective in modern industrial control systems (ICS), for instance, the supervisory control and data acquisition (SCADA) networks appear to have undergone evolvement towards adapting the Internet-of-Things and cloud computing technologies (Sadeghi *et al.*, 2015). However, the present implementation practices of ICS/SCADA systems have introduced a wide range of security vulnerabilities (Sajid *et al.*, 2016). Cyber-attacks on ICS/SCADA systems can be performed from the internet or devices connected to the business or enterprise networks, which have access to the field-level devices (Sahu *et al.*, 2016). As a result, ICS turn into obvious targets for cyber-attacks. The impact of these cyber-attacks can range from disrupting or damaging critical infrastructural operations to causing major economic losses or even more dangerously, claim human lives.

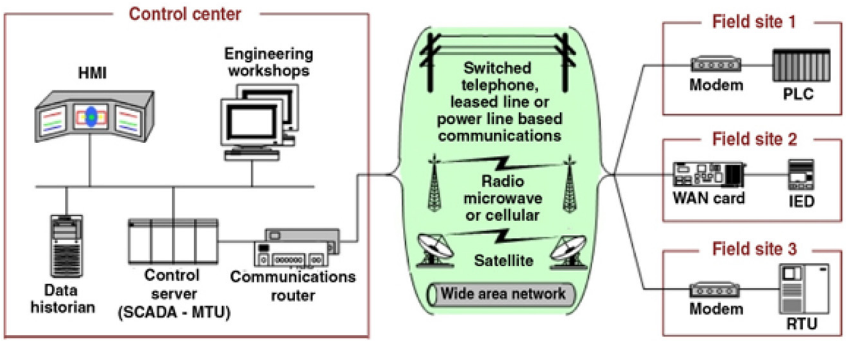
Cyber-attacks exploit SCADA security vulnerabilities to take control or to disrupt the normal functions of the system. Hence, it is critical to identify and to analyse the security vulnerabilities and the weaknesses of these systems to develop security solutions and protection mechanisms. Furthermore, as technology evolves, so does cyber-attack threats, thus demanding effective detection and protection measures for timely reporting and initial detection of attacks. Generally, three countermeasures are available to secure the SCADA systems (Drias *et al.*, 2015), which are: to identify known security incidents at the perimeter of the system by using several security tools, such as firewalls and systems that detect intrusions and malicious activates; to analyse the normal flow of data in systems and to look into benign control function in SCADA network in the attempt to identify threats due to alteration or damaging attempts; and lastly, which is an integral approach, to eliminate the vulnerabilities in the control system designs and implementations by performing technical auditing tests, for instance, penetration tests.

This paper presents a review and a comparative analysis of several standard SCADA security assessment methodologies and guidelines published by internationally recognised bodies. In addition, it explores the adequacy of the existing methodologies in meeting cyber security assessment practices required for electrical power networks. The rest of the paper is organised as given in the following: Section 2 explains the general overview concerning SCADA networks, their essential components and the communication protocols applied for data transmission in the system. Next, Section 3 reviews the existing security assessment methods, whilst Section 4 depicts the primary contribution of this paper, where the comparative analysis is presented. Section 5 discusses the challenges of existing security assessment methods and the complexity imposed by the cyber-physical systems onto the security assessment methods. Section 6 presents the future works. Lastly, this paper is concluded in Section 7.

2. Overview of SCADA systems

A typical SCADA system is comprised of control centre(s), along with several distributed devices of remote field, for example, remote terminal unit (RTU), programmable logic controllers (PLCs) and intelligent electronic device (IED), which are linked with a certain medium of communication (Singh *et al.*, 2015). Commonly, sensor reading information in analogue format is received by the RTU fed from field devices, which is later converted into digital format to be sent to the corresponding control centre(s). Additionally, the RTU, apart from receiving commands in digital format from control centre(s), also generates alarms (Cherdantseva *et al.*, 2016). Similar to the RTU, the PLC is a digital computer system with specific functionalities that monitors the sensors of field devices and decides by adhering to pre-programmed commands to regulate solenoids, actuators and valves. On the other hand, the control centre, which includes the SCADA server, receives data from and gives commands to RTUs, apart from processing and storing information to be presented to the human operators in supporting the decisions made. In fact, the system is observed and controlled by human operators by using a human–machine interface (HMI) at the control centre (Cherdantseva *et al.*, 2016). Moreover, varied computer software applications are integrated with the SCADA server, which are inclusive of billing and inventory management applications, to manage corporate and business functions (Larkin *et al.*, 2014). Typically, data exchange amongst these software applications is performed by adhering to software interface standards (e.g. OPC), database interaction (e.g. ODBC) or through an API (Dayal *et al.*, 2015). A variety of data protection and recovery mechanisms are used in the SCADA systems, such as intrusion detection and real-time data backup, mainly to hinder interception or loss of critical telemetry data.

These SCADA systems, generally, observe and regulate the industrial processes embedded within the physical control system. Hence, the control processes of the SCADA network range from lowering and raising the temperature of the devices to controlling energy-generating and distribution networks, including nuclear, traffic systems and rail networks (McLaughlin *et al.*, 2016). Therefore, the impacts of cyber-attacks upon these systems are disastrous and a successful attack is an attractive goal for both individual hackers and state-sponsored organisations. Thus, the security of SCADA system is extremely important, as well as of national concern (Coletta and Armando, 2016; Shukla, 2016). In fact, the recent cyber-attacks on SCADA systems (Li *et al.*, 2015; Gao *et al.*, 2013) have drawn attention to the significance of vulnerability assessments and penetration testing exercises in SCADA systems, especially to detect potential vulnerabilities, security loopholes and threat agents. Figure 1 illustrates the SCADA network architecture and several components.



Source: Stouffer *et al*. (2008)

Figure 1. SCADA network architecture

3. Review of security assessment methodologies

A security assessment is a commonly used practice that estimates the present cyber security posture of an information system. It identifies security weaknesses and loopholes that may be utilised by an attacker to execute cyber-attacks against the target system (Cherdantseva *et al.*, 2016). Generally, the security assessment offers recommendations and guidelines to enhance its security and protection mechanisms to mitigate risks and avoid potential security threats.

Generally, most internet-facing systems, as well as interconnected systems and applications, introduce various security threats and potential risks. Security professionals address these security risks through risk assessment, vulnerability assessment and penetration test processes. Risk assessment involves identifying potential hazards and analysing what could happen if a hazard occurs (Moore, 2013). Meanwhile, vulnerability assessment exercise involves a variety of manual testing methods and automated vulnerability tests to reveal the efficacy of security mechanism in the tested system (Anwar *et al.*, 2008). On the other hand, penetration testing encompasses exploiting the identified drawbacks of the system to evaluate the security of its IT infrastructure. The penetration tester carefully simulates potential activities of a malicious attacker by exploiting the detected vulnerabilities in assessing the efficacy of implemented security countermeasures, as well as protection mechanisms in the target system.

The literature depicts several assessment methodologies as proposed by the industrial and research institutes, each with its own specific scope, procedure and assessment technique (McLaughlin *et al.*, 2016; Wu *et al.*, 2016). Nevertheless, they share a common course: plan, execute and communicate results. Planning for assessment includes discovering all hardware and software assets within the facility, as well as identifying legal and business requirements, policies, procedures and controls. The second phase is about assessment execution that involves identifying security weaknesses and software pitfalls. Lastly, documentation and coordination of the identified shortcomings are carried out.

The analysis is comprised of three phases. First, the analysed security assessment standards are selected based on several criteria. At the second phase, an in-depth study of each selected methodology is carried out to extract information regarding security assessment methods, processes and coverage. Finally, each SCADA cyber security standard and guideline is evaluated by complying with the security requirements outlined by North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP).

The literature review on cyber security assessment for critical infrastructure systems reveals a handful number of security standards and recommendations for ICS and SCADA security analyses. Hence, to identify the most related standards, a careful and thorough search for documents produced by standardisation bodies and governmental agencies had been performed. Besides, a set of criteria was used to determine whether a standard could be considered for review:

- The standard/guideline is freely available and is written in English language.
- The standard/guideline is published by a standard body or governmental agency.
- The standard/guideline must be implemented for/or applied in the context of ICS/SCADA systems.
- The standard/guideline presents a detailed description of the proposed security assessment methodology.

As a result, 11 standards and guidelines had been selected based on the defined requirements. The identified publications were examined in detail to identify the most suitable vulnerability assessment methodology that could efficiently handle the vulnerability assessment process, aside from ascertaining compliance with the NERC standards. The rest of this section presents a brief overview of each examined methodology.

The Office of Critical Infrastructure Protection (OCIP) under the US Department of Energy reported on its vulnerability assessment methodology (US Department of Energy, 2001). The proposed method comes in three primary stages, which are: pre-assessment, assessment and post-assessment. Every stage has some tasks devised to ascertain the aspects of confidentiality and inclusiveness for the assessment outcomes. Hence, the learnt lessons have improvised and expanded the methods applied. These tasks, which are related to every assessment, can be adjusted in achieving the objectives of the assessment.

In 2002, the NIST (Stoneburner *et al.*, 2002) has issued a special publication that reflects the guideline for organisational risk management process and its first revision in 2012 (Blank and Gallagher, 2012). In this guideline risk management processes, the following have been incorporated: framing, assessing, responding and monitoring risks. The initial element shows how are security researchers being framing or establishing a risk context to devise a plan to manage risks so as to further assess, respond and observe risks. Next, risk is assessed based on the frame of risk, to detect both external and internal vulnerabilities, as well as threats towards the examined system, in hindering potential harm. Meanwhile, responding to risks exemplifies how security researchers should react upon identifying a risk from assessment. Finally, monitoring risks refers to how organisations monitor risk over time, especially to verify the efficacy of responses towards risks, apart from determining shifts that take place due to risks in the operating systems.

Furthermore, the US Department of Justice (Hart, 2002) has developed a method for vulnerability assessment by collaborating with the Sandia National Laboratories, particularly its Energy Department. This conceptualised method is intended to assess the security of chemical facilities by detecting and assessing possible risks and threats, apart from enhancing the chemical facility security system. Moreover, this proposed method exhibits compliancy with the NERC-CIP requirements, except for personnel security assessment and awareness, which are not considered.

The National Petrochemical and Refiners Association (NPRA) and the American Petroleum Institute (API) have proposed an assessment for security loopholes within the petroleum industry (American Petroleum Institute, 2003). The guidelines describe an approach for assessing security vulnerabilities, which can be applied for many facilities within the industry. In fact, the suggested assessment for security embeds stances from the general view, as well as from particular asset view. The general view reflects the wholesome effects of losses, the architectures and the interdependency at the level of facility, whilst analysis of outer perimeter incorporates physical protection and control of access.

In mid-2005, Permann and Rohde (Permann and Rohde, 2005) proposed a method of assessing cyber threats for a SCADA network following the security assessment for multiple SCADA networks, which was performed in conjunction with National SCADA Test Bed (NSTB) event initiated by the Idaho National Laboratory and US Energy Department. In November 2007, Sandia National Laboratories (Parks, 2007) released a document describing a customised assessment to evaluate cyber threats with compliancy of standards outlined in CIP, which NERC had adopted. The guideline blankets the planning, execution and reporting of the assessment upon the electronic security perimeter (ESP) and critical utility assets. The guide emphasises dual varying, but associated cyber threat assessments, as demanded by CIP-005 (ESP) and CIP-007 (cyber properties that are critical).

In 2011, NIST released a special publication that offers guidance to establish SCADA systems (Stouffer *et al.*, 2011), and in May 2015, the guidelines were revised to cover practices for ICS, which incorporated distributed control systems (DCS), SCADA networks and several other control networks, for instance, PLC, apart from evaluating reliability, safety requirements, as well as performances exerted. Hahn and Govindarasu (2011) developed a modified version of NIST 800-115 vulnerability assessment methodology. The authors determined the needs for the threat evaluation based on smart grids and electrical power grid environments, particularly for substation automation networks. Hahn *et al.* have presented a comprehensive method that determined the steps required for the vulnerability assessment process, besides differentiating this approach from other conventional IT environments. Additionally, integral issues were addressed, such as the negative effects upon the system due to the assessments carried out.

A guide was also published by the Centre for the Protection of National Infrastructure (Centre for the Protection of National Infrastructure (CPNI), 2011), which provides an overview of the assessment process to help security personnel comprehend the execution of cyber security assessment for SCADA. The guideline covers the planning stage for the assessment, for example, selecting areas to be tested. This planning identifies the details of assets accurately, and it is flexible for all skills within the evaluation team. Besides, information from the real evaluation familiarises the property owner about the steps and the reason for the evaluation.

The Idaho National Laboratory (Idaho National Laboratory, 2011) conducted cyber security assessments for the US Energy Department for its NSTB program. Its aim was to aid both the government and the industry to enhance ICS security installed for energy infrastructure in the USA. One integral aspect of this goal is the ICS evaluation to detect threats that may compromise its infrastructure.

Another publication by NIST is concerning the implementation of patch-and-vulnerability management program. The initial guidelines were published in 2005, whilst the last edition was published in 2013 (Souppaya and Scarfone, 2013). These publications are designed to help establishments with the implementation of patch-and-vulnerability approach. This develops a process for the organisation and examines its efficiency, aside from informing available solutions to address probable threats. Its main aim is to guide the security patch-and-vulnerability program, apart from determining its efficiency.

4. Comparative analysis of vulnerability assessment methodology

This section presents the findings of the comparative analysis performed to compare varied SCADA cyber security standards and guidelines. The methodologies were evaluated based on the supported security assessment methods, including vulnerability assessment, penetration testing, vulnerability prioritisation, risk assessment and patch management.

4.1 Analysis criteria

The examined methods differ by domains and goals, as they were generated for varied purposes, such as for petroleum industry, chemical plants and power grid. Hence, they cover various methods of security assessments, which range from vulnerability assessment and penetration testing to patch management. Table I depicts the criteria to analyse each publication by its assessment method. The literature shows that the security assessment methods in SCADA and IT systems are rather similar, as they rely on vulnerability analysis and risk management approaches to detect and fix loopholes within the system. The vulnerability analysis may consist of one or more of the following activities: vulnerability assessment, penetration testing and vulnerability prioritisation. Meanwhile, risk management may encompass risk assessment and patch management. Thus, this work reviewed the existing SCADA security assessment methodologies based on these approaches and methods.

Security analysis in general, and vulnerability assessment in specific, may be carried out by using passive or active evaluation approaches. The passive technique only observes and accumulates data without implying traffic to the examined system, thus suitable for assessing the security posture in test and actual ICS environments. Meanwhile, the active techniques inject traffic into the system to identify threats and to evaluate responses; thus, active vulnerability assessment should be executed with extra precautions in production functional systems. Nevertheless, the active approach could interrupt the network, hence losing control and visibility on its functional, as well as power outages. Such interruption could be generated due to atypical traffic caused by the instruments applied for the evaluation. For instance, vulnerability scanning may cause reboot or hang in system, cause exhaustion on resources of network or even cause system saturation. Thus, detecting threats in a SCADA demands various approaches, when compared to an IT setting.

Network vulnerabilities scanning tools make discovery of all hosts in a system more rapid, including the service run and threats detected. Nonetheless, the methods of service fingerprinting, frequent host-probing to detect threats and port scanning have an adverse effect on SCADA systems. Besides, active threat scanning can interrupt the function of system due to bandwidth consumption, stalled response time and unforeseen impacts. Moreover, one main concern refers to DoS glitch upon the system and devices, as well as the scanners that frequently probe and simulate attacks. Thus, to protect the SCADA system, the NERC developed critical infrastructure protection (CIP) set of standards for industrial control systems, as depicted in Table II. The primary aim of the CIP standard is to offer a framework of cyber security to detect and to protect cyber properties so as to retain viable function in the electric network. One essential goal of the assessment of security is meeting the required compliances. As SCADA networks that support power system need to comply with NERC-CIP, its assessment method should look into every requirement. The NERC-CIP standard determines the needs of security measures that should be addressed in the methods of assessing SCADA.

4.2 Analysis results

The selected standards were analysed in-depth to extract data about security assessment methods, processes, coverages, methodologies and their compliance with NERC-CIP requirements. As such, this section presents the outcomes of the review. First, the security assessment activities from each methodology are displayed. Next, the methodologies are

Technique	Criteria
Vulnerability assessment	The publication described a substantial methodology for the vulnerability assessment process or sub-activities that contribute to its consummation
Penetration test	The publication considered the attempt to exploit the identified vulnerabilities to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application
Vulnerability prioritisation	The publication considered a vulnerability scoring system or clearly describes a qualitative method of assessing security risks to estimate the severity of vulnerabilities
Risk assessment	The publication clearly defines a substantial risk management or assessment process
Patch management	The publication describes implementing a vulnerability management programme, including patch and remediation management

Table I. Analysis criteria

categorised into active or passive assessment mode. Lastly, the methods that complied with NERC-CIP requirements are listed. A comprehensive study on the selected documents revealed five primary activities linked to security assessment process, as shown in Table III, based on each method. In the table, cell with χ mark reflects that the method has not considered the denoted activity, whilst the ✓ mark indicates the opposite.

Table III displays that most of the examined methodologies concentrated on vulnerability identification and prioritisation techniques, whilst other security techniques received noticeably less attention. These two techniques are considered as the essential steps towards implementing a secure system. The review exhibited that the least attention is devoted to patch management process mainly due to the critical nature of the SCADA system. Besides, only the documents published by Hahn and Govindarasu (2011) and CPNI (2011) were designed to cover all cyber security assessment approaches. The methodology included numerous elements in cyber-security evaluation, such as planning, executing and reporting stages, to aid procurement or facilitation of ICS security assessment.

Table II.
NERC-CIP security requirements

Requirement	Description
CIP-002	The publication described a substantial methodology for the vulnerability assessment process or sub-activities that contribute to its consummation
CIP-003	Documentation and implementation of cyber security policy reflecting commitment and ability to secure critical cyber assets
CIP-004	Maintenance and documentation of security awareness programmes to ensure personnel knowledge on proven security practices
CIP-005	Identification and protection of electronic security perimeters and their access points surrounding critical cyber assets
CIP-006	Creation and maintenance of physical security controls
CIP-007	Definition and maintenance of methods, procedures and processes to secure cyber assets within the electronic security perimeter
CIP-008	Development and maintenance of cyber security incident response plan that addresses classification, response actions and reporting
CIP-009	Creation and review of recovery plans for critical cyber assets

Table III.
Activities of the security assessment process addressed by the methods

Study	Vulnerability assessment	Penetration test	Vulnerability prioritisation	Risk assessment	Patch management
US Department of Energy (2001)	✓	✓	✓	✓	×
Stoneburner *et al.* (2002)	✓	×	✓	✓	×
Hart (2002)	✓	×	✓	✓	×
API (2003)	✓	×	✓	✓	×
Permann and Rohde (2005)	✓	×	×	×	×
Parks (2007)	✓	×	×	×	×
Stouffer *et al.* (2011)	✓	×	✓	✓	×
Hahn and Govindarasu (2011)	✓	✓	✓	×	✓
CPNI (2011)	✓	✓	✓	✓	✓
Idaho National Laboratory (2011)	✓	✓	×	×	×
Souppaya and Scarfone (2013)	✓	✓	✓	✓	×

The review of the existing methods showed that the vulnerability analysis is comprised of two stages, which are:

(1) vulnerability assessment that encompasses the discovery of system vulnerabilities; and

(2) penetration testing that consists of some tests performed to evaluate the detected vulnerabilities.

Hence, both penetration testing and vulnerability assessment are the two kinds of testing for vulnerability that are frequently combined, as they have varied strengths. Upon combination, a more wholesome evaluation is attained, for they provide more detailed information regarding the assessment aspects, thus enabling enhanced security for the networks.

Basically, these vulnerability evaluation methods are used by software programs, for instance, OpenVas and Nessus, for scanning of IP addresses to detect threats, whereby a report with detected threats, severity of the threats and essential remediation procedures is provided. Such tool that manages vulnerability aids the team that monitors security to be alert of arising issues within the networks. Moreover, latest threat identification methods are integrated with prioritisation algorithms to better address glitches that demand instant solution so as to hinder breach in its security system. Recently, the vulnerability assessment for SCADA has turned into an essential requirement in NERC cyber security standards for electric power systems.

The study reveals that evaluation for security can be carried out by using either passive or active testing approaches. Table IV portrays the classification of studies that investigated passive and active testing methods. However, the active approach may interrupt the network, which could be due to atypical traffic caused by the instruments applied for the evaluation of security.

The primary aim of the NERC-CIP standard is to offer a framework of cyber security to detect and to protect cyber properties so as to retain viable function in the bulk electric network. One essential goal of the assessment of security is meeting the required compliances. Table V displays the requirements of CIP based on each security assessment technique. As indicated in the table, cells with empty circle show that the CIP requirement has not been addressed by the method, whilst cells with a filled circle indicate that the particular phase has been addressed in detailed, and a half circle exhibits that some requirements have been addressed (addressed not in detail, absence of actions in detail, no suggestion on how to meet the requirements). This review exemplifies that only two of the

Reaction	Study
Active	Vulnerability Analysis of Energy Delivery Control Systems
	Cyber Assessment Methods for SCADA Security
	Vulnerability Assessment for Substation Automation Systems
	Guide for Conducting Risk Assessments
	Creating a Patch and Vulnerability Management Program
Passive	Vulnerability Assessment of U.S. Chemical Facilities
	Cyber Security Assessments of Industrial Control Systems
	Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries
	A Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment
	A Guide to Industrial Control Systems (ICS) Security
	Vulnerability and Risk Analysis Program

Table IV. Classification of the methods based on their assessment mode

examined security assessment methods appear to have absolute fulfilment of all NERC-CIP security requirements, whilst others only partially fulfilled the necessary requirements. The review also displayed that most of the examined methodologies did address NERC's requirements of CIP-002 and CIP-005 related to identifying and documenting critical cyber properties, as well as detecting and securing ESPs, including the surrounding points of access, respectively. On the other hand, the requirement of security for CIP-004, which involves security personnel training and awareness, has received less attention.

5. Discussion

Managing the security of today's critical infrastructure and ICS poses many challenges. In addition to the new vulnerabilities that are discovered every day in these systems, there are some issues related to: their operational requirements, the utilisation of legacy systems and blurred boundaries between the cyber and physical networks (Alcaraz and Zeadally, 2015; McLaughlin *et al.*, 2016; Ozturk and Aubin, 2011). The lack of resources and proper assessment tools become the biggest obstacles to maintaining a reliable and an up-to-date security measures. Historically, these systems were physically isolated from other computing resources (such as business and enterprise networks) and have used proprietary hardware components, software and communication protocols (Sheng *et al.*, 2011). Nevertheless, the current trends in ICS implementations are embracing the new IT technologies for cost reduction, minimal maintenance efforts and easier accessibility, in addition to improved efficiency (McLaughlin *et al.*, 2016). Therefore, these challenges must be handled to minimise the attack surface on the system and reduce the impact risk that may be caused by potential cyber-attacks.

The security assessment is the key process in any information security program. However, assessing the security of critical infrastructure and ICS is more complicated and challenging than general standard IT systems (Alcaraz and Zeadally, 2015). This is due to the fact that infrastructure control systems' processes and equipment are more fragile and more easily susceptible to harm. For example, using standard enumeration and scanning techniques on ICS can result in failures with grave consequences in the physical environment. Therefore, assessing the security of industrial control and critical infrastructure systems requires careful planning and execution. This section briefly presents security assessment challenges in industrial systems to be considered during the planning phase for more comprehensive security assessment.

Perhaps the most challenging problem of ICS security assessment is due to its complexity, large-scale and heterogeneity. Being a cyber-physical system, the scale and

Table V.
Method compliancy to the NERC-CIP requirements

Study	CIP 002	CIP 003	CIP 004	CIP 005	CIP 006	CIP 007	CIP 008	CIP 009
US Department of Energy (2001)	●	●	○	●	●	●	●	●
Stoneburner *et al.* (2002)	●	○	○	●	◐	●	◐	○
Hart (2002)	●	●	◐	●	●	●	●	●
API (2003)	●	◐	○	●	○	●	●	◐
Permann and Rohde (2005)	◐	◐	○	●	◐	○	◐	○
Parks (2007)	◐	●	○	●	●	●	○	○
Stouffer *et al.* (2011)	◐	●	●	●	○	●	●	◐
Hahn and Govindarasu (2011)	●	●	◐	●	●	●	●	●
CPNI (2011)	●	●	●	●	●	●	●	●
Idaho National Laboratory (2011)	○	○	●	◐	○	◐	●	◐
Souppaya and Scarfone (2013)	●	●	○	●	○	●	●	◐

complexity of ICS and the communication technologies that they are associated with, making planning, executing and reviewing cyber and physical security assessments become a substantially challenging problem. Therefore, a domain-specific conceptual model is required to establish a generic framework for cyber security analysis to examine and investigate security threats on cyber-physical systems.

Another major challenges of security assessment in ICS is associated with the lifetime of the industrial devices (Alcaraz and Zeadally, 2015); where in today's SCADA, critical national infrastructure and ICS, there are many legacy systems that may be vulnerable to cyber-attack because cyber security was not considered at the time of initial design and installation, as they were physically separated from other networks(Cherdantseva *et al.*, 2016).

The third major security assessment challenge is due to the enormous number of known vulnerabilities (McLaughlin *et al.*, 2016), where the overwhelming volume of vulnerabilities identified and reported by security agencies and professional bodies can lead organizations and security enforcement authorities to focus on high severity vulnerabilities only. It is a common practice that, from an organizations' point of view, handling high severity vulnerabilities is a number one priority. However, in ICS, such exercise is not applicable for two reasons:

(1) lack of proper ICS-specific vulnerability prioritisation mechanism; and

(2) challenges in the remediation process itself.

The security vulnerabilities in general IT systems are being prioritised based on the CVSS score and perform some level of asset importance classification within the process. However, for industrial control and critical infrastructure systems, the priority of security standards is not the same because their business and mission goals differ (Coffey *et al.*, 2018). The major difference is in how each prioritises the canonical security objectives of confidentiality, integrity and availability. In standard IT systems, confidentiality is the highest priority, followed closely by integrity; availability is rarely deemed equally important. In contrast, in control systems, availability is most important, far outstripping confidentiality and even integrity, which in turn means it is very difficult and costly to interrupt these systems for security updates and similar activities (Goel and Hong, 2015). For example, few minutes of downtime in critical infrastructure operator's terminal loses the view of the physical process which may lead to catastrophic consequence. This challenge also explains the defiance in the remediation process, where applying security patches to running systems without interrupting the process or causing downtime is a challenge (Cherdantseva *et al.*, 2016). For this reason, organisations that support critical infrastructure cannot risk downtime by allowing automatic security updates for ICS that could cause systems to restart or shut down. Shutdown or isolate a system to apply security patches and updates is also not an affordable option. Therefore, planning efforts needed to be implemented for prioritisation of the tasks necessary to enhance ICS security.

Another security assessment challenge in ICS is the arise of data privacy and protection efforts, especially after the European Union (EU) General Data Protection Regulation (GDPR) comes into force (Urquhart and McAuley, 2018). Today, security assessment and assurance programmes have become as much about people and process as it is about technology. For example, the vulnerability assessment operation requires collecting and processing a significant amount of confidential data related to the assessed system, systems' operators and intermediary processes by eligible parties, usually the security assessment team (Ferrag *et al.*, 2018). The collected data are compiled, analysed and made available to entitles personnel. Besides, as many risk assessment outcomes demonstrated that human factors are the greatest causes of risks (Ali and Awad, 2018), most of vulnerability assessment methods considered people as one of the significant information assets. Therefore, their personal details and background were collected for assessment. This introduces data privacy and protection challenges and creates a new risk for the industrial control and critical infrastructure systems, where the collected data should be protected and kept private to prevent unauthorised disclosure of information that is not open to the public and individuals.

On the other hand, specific security provision in Article 32 of GDPR deals with the requirements for controllers and processors to implement a level of security appropriate to the risk. Therefore, identifying the vulnerabilities and securing information assets, and their surrounding eco-system, that handle and process data is an important step in any security programme. Tenable Network Security ("Tenable Network Security", 2019) have published a guideline for essential steps to follow to meet the security challenges of the GDPR obligation (Giordano and Gary, 2016).Tenable researchers have suggested that a security assessment team should utilise and appreciate information security framework designed specifically for industrial control and critical infrastructure systems to maintain the best practices accumulated by security professionals across industries over time. With reference to the GDPR, Tenable security researchers have recommended a data discovery approach which involves using both active system scanning and passive network monitoring to locate unencrypted sensitive data in an enterprise information ecosystem. Moreover, they have also suggested to use active and passive scanners, as well as manual inspection to carefully identify all unknown assets and shadow IT and other ICS components. Where, in ICS, there are many components that can pose a security risk and are often not seen or understood well enough by IT. Additionally, in reference with GDPR, Article 35 requires that organisations should perform data protection impact assessment (or DPIA). The DPIA help organisations to identify, assess and mitigate or minimise privacy risks with data processing activities (Alnemr *et al.*, 2016). The DPIA is required and particularly relevant when a new data process, system or technology is being introduced. This introduces and new mandatory activities to be addressed by the security assessment methods.

6. Implications for further research

This study was being of an exploratory and comparative in nature, raises a number of challenges found in existing security assessment practices and identifies a number of opportunities for future research, both in terms of method development, enhancement and concept validation. Additionally, the reported findings in this work present potentially useful information to practitioners engaged with compliance with the NERC-CIP standard. More research will, in fact, be necessary to refine and further elaborate the findings of this work.

The previous section has identified several challenges in performing security assessment in industrial systems, challenges associated with the existing security assessment methods, vulnerability handling and management, remediation process and data privacy and protection. Therefore, planning for more comprehensive security assessment is required. Future direction should address these challenges.

To address the complexity of ICS, for instance, a domain-specific conceptual model is required to establish a generic framework for cyber security analysis to examine and investigate security threats on cyber-physical systems. The conceptual model is meant to be an architectural template representing all services, protocols and assets in different domains and operational levels. It aims at offering a support for cyber security analysis of the ICS with an architectural approach allowing for a representation of interdependencies amongst different operational layers and subsystems. It should offer the full support for both the current implementation of the critical national infrastructure and future applications of the smart grid, IoT and SCADA systems. More studies are required to address the prioritisation, management and handling of vulnerabilities in ICS considering the security requirements and objectives of these systems. Moreover, further studies are required to address challenges of the remediation process, as there is no technology that can easily and economically solve the problem without interrupting the normal operation of industrial control system. Lastly, future studies should address data privacy and protection. Where for years, there was no specific binding legislation devoted to data protection in ICS and critical infrastructure systems such as in smart grid and smart meter applications.

7. Conclusion

The escalating interconnectivity of ICS networks is exposed to a wide range of vulnerabilities and security threats. Thus, ICS have become a target of cyber-attacks, hence posing significant risks to the nation's critical operations. Besides, lack of viable ICS security measures and inadequate security mechanisms could eventually lead to severe disruption of the normal ICS operations, upon being attacked. These may result in catastrophic consequences on the physical world. As such, security analysis and countermeasure planning are deemed as mandatory. The ICS security analysis aids in detecting vulnerabilities, threats and possible attacks that may target the ICS and their underlying components. These tasks are essential to protect and to secure the system against cyber-attacks. Nevertheless, due to the scale and the intricacy of ICS, as well as the communication technologies linked with planning, executing and reviewing cyber and physical vulnerability assessments, are rather difficult. Therefore, several standards and guidelines have been proposed in the literature. With that, this work has reviewed several ICS security assessment methodologies and carried out detailed analysis of the examined methodologies so as to explore the sufficiency of these existing methodologies in meeting the needs and requirements of cyber security evaluations meant for power networks. Furthermore, the literature showed that the security assessment techniques in ICS and IT systems are quite similar, as both rely on performing vulnerability analysis and risk management techniques to identify and to fix loopholes within the system. From the findings, most of the examined methodologies seem to concentrate on vulnerability identification and prioritisation techniques, whilst other security techniques received noticeably less attention. This is because these two techniques have been considered as the essential steps towards implementing a secure system. The review also displayed that the least attention is devoted to patch management process due to the critical nature of the ICS. Additionally, this review portrayed that only two security assessment methodologies exhibited absolute fulfilment of all NERC-CIP security requirements, whilst the others only partially fulfilled the essential requirements.

References

Alcaraz, C. and Zeadally, S. (2015), "Critical infrastructure protection: requirements and challenges for the 21st century", *International Journal of Critical Infrastructure Protection*, Vol. 8, pp. 53-66.

Ali, B. and Awad, A. (2018), "Cyber and physical security vulnerability assessment for IoT-based smart homes", *Sensors*, Vol. 18 No. 3, p. 817.

Alnemr, R., Cayirci, E., Corte, L.D., Garaga, A., Leenes, R., Mhungu, R., Pearson, S., Reed, C., de Oliveira, A.S., Stefanatou, D., Tetrimida, K. and Vranaki, A. (2016), "A data protection impact assessment methodology for cloud", Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 60-92.

American Petroleum Institute (2003), *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, American Petroleum Institute, Washington, DC, available at: www.nrc.gov/docs/ML0502/ML050260624.pdf

Anwar, Z., Shankesi, R. and Campbell, R.H. (2008), "Automatic security assessment of critical cyber-infrastructures", *Proceedings of the International Conference on Dependable Systems and Networks*, pp. 366-375.

Blank, R.M. and Gallagher, P.D. (2012), *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, MD, available at: https://doi.org/10.6028/NIST.SP.800-30r1

Centre for the Protection of National Infrastructure (CPNI) (2011), "Cyber security assessments of industrial control systems: a good practice guide", available at: www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016), "A review of cyber security risk assessment methods for SCADA systems", *Computers and Security*, Vol. 56, pp. 1-27.

Coffey, K., Smith, R., Maglaras, L. and Janicke, H. (2018), "Vulnerability analysis of network scanning on SCADA systems", *Security and Communication Networks*, Vol. 2018, pp. 1-21.

Coletta, A. and Armando, A. (2016), "Security monitoring for industrial control systems", *Lecture Notes in Computer Science*, 9588th ed., Springer, Cham, pp. 48-62.

Dayal, A., Deng, Y., Tbaileh, A. and Shukla, S. (2015), "VSCADA: a reconfigurable virtual SCADA test-bed for simulating power utility control center operations", *2015 IEEE Power and Energy Society General Meeting, IEEE, Denver, CO*, pp. 1-5.

Drias, Z., Serhrouchni, A. and Vogel, O. (2015), "Analysis of cyber security for industrial control systems", *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1-8.

Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J. and Shu, L. (2018), "A systematic review of data protection and privacy preservation schemes for smart grid communications", *Sustainable Cities and Society*, Vol. 38 No. 1, pp. 806-835.

Gao, H., Peng, Y., Jia, K., Dai, Z. and Wang, T. (2013), "The design of ICS testbed based on emulation, physical, and simulation (EPS-ICS testbed)", *Proceedings – 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, pp. 420-423.

Giordano, S. and Gary, T. (2016), "Thirteen essential steps to meeting the security challenges of the new EU general data protection regulation", available at: www.wickhill.com/uploads/knowledge_library/GDPR/Tenable_Thirteen_Essential_Steps_to_Meeting_GDPR_Security_Challenges.pdf

Goel, S. and Hong, Y. (2015), "Security challenges in smart grid implementation", *Smart Grid Security*, Springer, London, pp. 1-39.

Hahn, A. and Govindarasu, M. (2011), "Vulnerability assessment for substation automation systems", World Scientific Review Volume, pp. 1-16.

Hart, S.V. (2002), "A method to assess the vulnerability of US chemical facilities (Report no. NCJ 195171)", US Department of Justice, Washington, DC, available at: www.ncjrs.gov/pdffiles1/nij/195171.pdf

Idaho National Laboratory (2011), "Vulnerability analysis of energy delivery control systems (Report no. INL/EXT-10-18381)", ID Falls, ID, available at: https://energy.gov/sites/prod/files/VulnerabilityAnalysisofEnergyDeliveryControlSystems2011.pdf

Larkin, R.D., Lopez, J., Butts, J.W. and Grimaila, M.R. (2014), "Evaluation of security solutions in the SCADA environment", *ACM SIGMIS Database*, Vol. 45 No. 1, pp. 38-53.

Li, W., Xie, L., Liu, D. and Wang, Z. (2015), "False logic attacks on SCADA control system", *Proceedings – 2014 Asia-Pacific Services Computing Conference, APSCC 2014*, pp. 136-140.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A., Maniatakos, M. and Karri, R. (2016), "The cybersecurity landscape in industrial control systems", *Proceedings of the IEEE*, Vol. 104 No. 5, pp. 1039-1057.

Moore, D.A. (2013), "Security risk assessment methodology for the petroleum and petrochemical industries", *Journal of Loss Prevention in the Process Industries*, Vol. 26 No. 6, pp. 1685-1689.

Ozturk, M. and Aubin, P. (2011), "SCADA security: challenges and solutions", Schneider Electric, No. June, p. 10.

Parks, R.C. (2007), "Guide to critical infrastructure protection cyber vulnerability assessment (Report no. SAND2007-7328)", Sandia National Laboratories, Albuquerque, NM, available at: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/26-CIP_CyberAssessmentGuide.pdf

Permann, M.R. and Rohde, K. (2005), "Cyber assessment methods for SCADA security", *15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*, p. 12.

Sadeghi, A.R., Wachsmann, C. and Waidner, M. (2015), "Security and privacy challenges in industrial internet of things", *Proceedings of the 52nd Annual Design Automation Conference on – DAC '15, ACM Press, New York, NY*, pp. 1-6.

Sahu, S.K., Anand, A., Sharma, A. and Nautiyal, N. (2016), "A review: outrageous cyber warfare", *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), IEEE, Noida*, pp. 70-74.

Sajid, A., Abbas, H. and Saleem, K. (2016), "Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges", *IEEE Access*, Vol. 4, pp. 1375-1384.

Sheng, S., Yingkun, W., Yuyi, L., Yong, L. and Yu, J. (2011), "Cyber attack impact on power system blackout", *IET Conference on Reliability of Transmission and Distribution Networks (RTDN 2011)*, p. 3B3.

Shukla, S.K. (2016), "Cyber security of cyber physical systems: cyber threats and defense of critical infrastructures", *2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID)*, pp. 30-31.

Singh, P., Garg, S., Kumar, V. and Saquib, Z. (2015), "A testbed for SCADA cyber security and intrusion detection", *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), IEEE*, pp. 1-6.

Souppaya, M. and Scarfone, K. (2013), *Guide to Enterprise Patch Management Technologies, National Institute of Standards and Technology (NIST) – Special Publication 800-40*, National Institute of Standards and Technology, Gaithersburg, MD, available at: https://doi.org/10.6028/NIST.SP.800-40r3

Stoneburner, G. Goguen, A. and Feringa, A. (2002), "Risk management guide for information technology systems", Gaithersburg, MD, available at: https://doi.org/10.6028/NIST.SP.800-30

Stouffer, K. Falco, J. and Kent, K. (2008), "Guide to industrial control systems (ICS) security recommendations of the national institute of standards and technology", Nist Special Publication, Vol. 800 No. 82.

Stouffer, K. Falco, J. and Scarfone, K. (2011), "Guide to industrial control systems (ICS) security, recommendations of the national institute of standards and technology", Gaithersburg, MD, available at: https://doi.org/10.6028/NIST.SP.800-82

Tenable Network Security (2019), available at: www.tenable.com

US Department of Energy (2001), "Vulnerability and risk analysis program: overview of assessment methodology".

Urquhart, L. and McAuley, D. (2018), "Avoiding the internet of insecure industrial things", *Computer Law and Security Review*, Vol. 34 No. 3, pp. 450-466.

Wu, G., Sun, J. and Chen, J. (2016), "A survey on the security of cyber-physical systems", *Control Theory and Technology*, Vol. 14 No. 1, pp. 2-10.

Corresponding author
Qais Saif Qassim can be contacted at: qaisjanabi@gmail.com