Computers & Security 89 (2020) 101666

Contents lists available at ScienceDirect

Computers & Security

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

SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations

Darshana Upadhyay, Srinivas Sampalli[*]

Faculty of Computer Science, Dalhousie University, Halifax, Nova Scotia B3H 1W5, Canada

ARTICLE INFO

Article history:
Received 4 May 2019
Revised 31 August 2019
Accepted 12 November 2019
Available online 13 November 2019

Keywords:
SCADA vulnerability
Firewalls
Critical infrastructure
Security mitigations
SCADA incidents

ABSTRACT

Growing dependency and remote accessibility of automated industrial automation systems have transformed SCADA (Supervisory Control and Data Acquisition) networks from strictly isolated to highly interconnected networks. This increase in interconnectivity between systems raises operational efficiency due to the ease of controlling and monitoring of processes, however, this inevitable transformation also exposes the control system to the outside world. As a result, effective security strategies are required as any vulnerability of the SCADA system could generate severe financial and/or safety implications. The primary task when identifying holes in the system is to have proper awareness of the SCADA vulnerabilities and threats. This approach will help to identify potential breaches or aspects in the system where a breach may occur. This paper describes various types of potential SCADA vulnerabilities by taking real incidents reported in standard vulnerability databases. A comprehensive review of each type of vulnerability has been discussed along with recommendations for the improvement of SCADA security systems.

1. Introduction

Automation plays a vital role in industrial systems. To accelerate industrial processes, almost all industries perform operations remotely through Supervisory Control and Data Acquisition (SCADA) systems. Some examples of industry where SCADA systems are employed include: controlling the flow of gas and oil through pipes in the oil industry, water flow management in water & sewage systems, management of the electrical output of power plants to the power grid, process control in chemical plants, management of transmission and distribution of products in manufacturing units, and the signaling network employed by railway and other transportation infrastructure.

A SCADA network typically includes a control server placed at the control center, communication links and one or more topographically dispersed field sites containing field devices. The SCADA sensors and actuators at field sites monitor the different attributes of electromechanical equipment continuously and send signals to field control devices like Programmable Logic Controller (PLC), Remote Terminal Unit (RTU) or Intelligent Electronic Device (IED). Via communication links, the transfer of information transpires back and forth between field control devices and the control center. The field control devices will supply digital status information to the control center, where software will process the status information and determine acceptable parameter ranges. This information will then be transmitted to the field device(s) where action may be taken in order to avoid various hazards or optimize the performance of the system. The control center will store the status information in data historian and display it on a HMI (Human Machine Interface) which provides centralized monitoring of digital status information and system control.

SCADA protocols typically implemented in large geographical areas include Ethernet/IP, Modbus, DNP3, Profinet, DCOM etc. These protocols will communicate in a Wide Area Network (WAN) through satellite, radio or microwaves, cellular networks, switched telephone or leased line communication media (Forner and Meixel 2013). Large SCADA networks will require hundreds of field devices and dedicated sub-control servers to manage communication exchange to ease the burden on the primary server. Fig. 1. Large SCADA communication architecture (SINGLE FITTING IMAGE) represents a large SCADA network map of the general architecture of component and configuration.

Originally, the goal of a SCADA system was to focus on accurate and efficient process execution in a single location, such as a manufacturing plant, rather than having an emphasis on securing network information. Due to the increase in interconnectivity of networks and the remote accessibility of systems on a SCADA network, there exists danger from various vulnerabilities and cyber-attacks. It has become necessary to incorporate adequate safety measures to strengthen the security of SCADA networks. General safeguards include restricted perimeters, patch manage-

[*] Corresponding author.
E-mail addresses: dr629110@dal.ca (D. Upadhyay), srini@cs.dal.ca (S. Sampalli).

https://doi.org/10.1016/j.cose.2019.101666

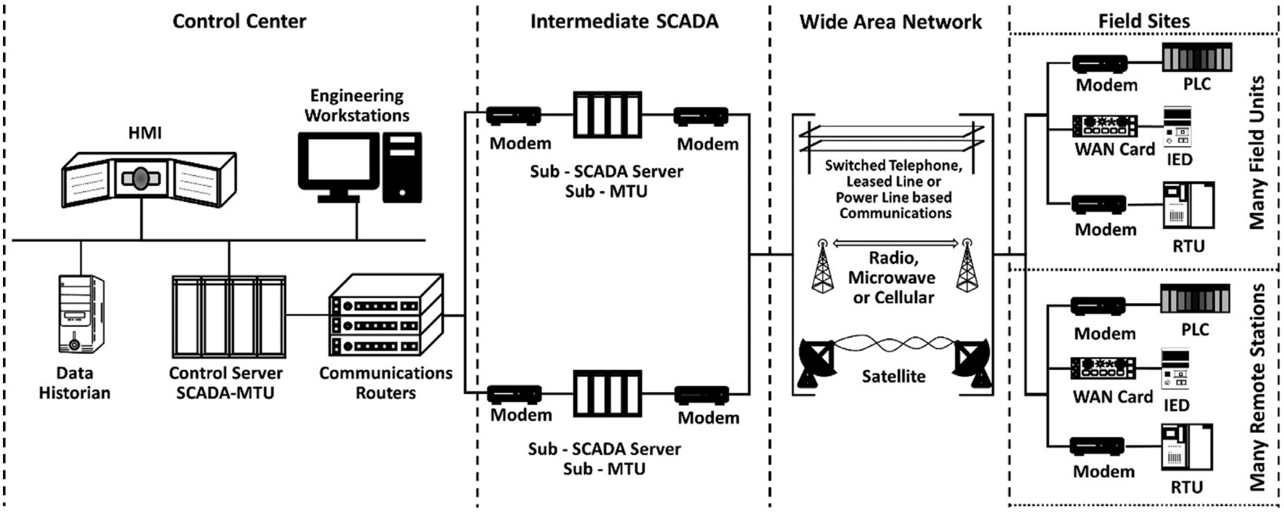

Fig. 1. Large SCADA communication architecture (SINGLE FITTING IMAGE).

ment, strong cryptography and most importantly, separation of the control network and corporate network through the defense in depth mechanism. Nevertheless, these security guards are difficult to apply owing to legacy-inherited security weaknesses and the significance of possible exploitation during real-time communication (Nazir et al. 2017).

This paper mainly focuses on recent SCADA vulnerabilities and recommendations to strengthen the security of industrial infrastructure on four major components of SCADA systems, citing detailed examples of vulnerabilities in critical infrastructure that were reported through various organizations. These four components are (1) SCADA products, (2) SCADA configuration, (3) SCADA network, and (4) SCADA communication protocols. This paper will provide a well-organized literature review to help owners, vendors, and researchers to leverage the security of a SCADA system. The discussion herein highlights recent vulnerabilities according to real incident reports which can aid in understanding various techniques of cyber-attack and will aid in the successful reinforcement of SCADA cyber security. The aim of our contribution is to cover the SCADA landscape with respect to various security weaknesses to help in the secure implementation and deployment of SCADA systems in automated industries.

This review paper is organized into the following sections: Section 2 lists several points with regards to complexity in securing SCADA network versus IT network, Section 3 emphasis on the involvement of several organizations in the direction of SCADA vulnerabilities assessment, Section 4 focuses on various SCADA security vulnerabilities and related mitigation techniques that help the researchers for farther enhancement of SCADA security, Section 5 lists the best practices and standards recommended by several professional bodies involved in the improvisation of SCADA security, and finally, Section 6 where concluding remarks are presented.

2. A difference in approach – IT Security versus SCADA Security

Securing a SCADA network is more critical than securing an IT network. The design and operation of most IT security solutions are based on typical security assumptions. These assumptions begin with the basic security mechanism of the network and extend up to every facet of product operation including performance specifications, reliability requirements, the software and hardware architecture of the product, risk management policies and many more. However, these assumptions are often invalid for SCADA systems. SCADA differs from IT networks due to legacy-inherited cyber security vulnerabilities and the consequence of their potential exploitation. The below issues show the complexity of approaching SCADA network security compared to IT network security and stay SCADA security engineers/programmers on their toes. Table 1 represents the difference between an IT network and SCADA network requirements (Stouffer et al. 2006).

2.1. Security mechanisms

In IT network, the critical asset that is protected is information, such as bank account data, credit card records, customer records, etc. The security of any IT system is primarily focused on confidentiality of the data at all costs, which may even require shutting down the network for a few hours. In contrast, the critical asset in SCADA networks is the high availability of the plant or infrastructure process. For example, a plant must run continuously and shutting down the network even for a few minutes is just not an option in most SCADA networks. Availability of a network is the topmost priority of a SCADA network (Mackenzie 2012). Traditional security approach works effectively for securing enterprise networks but typically cannot support the high-level availability requirement for SCADA networks. SCADA security solutions that could be installed, configured, tested, and even upgraded without affecting communications in the plant network is challenging in nature.

2.2. Vulnerabilities management

In many organizations, the field devices are vulnerable to malware attacks owing to weak structural design. Most of the SCADA Controllers and field devices were manufactured in an era when cyber-attacks were not a major concern (Ranathunga et al. 2016). Therefore, field elements can be easily disrupted by high network traffic or may be exposed to malware attacks. Hence, it is essential to execute security updates on a routine basis. Daily maintenance of security updates is one of the crucial factors in securing process/data in the organization. In IT networks, vulnerabilities are typically managed by using automated tools to scan all the devices to identify the requirements of a security upgrade. According to scan reports, upgrades are then installed on the network devices. However, we cannot apply the same approach to a SCADA network. PLC's (Programmable Logic Control) and RTU's (Remote Terminal Unit) network interface is so fragile in nature that the act of scanning the device may shut the whole SCADA system down

Table 1
Comparison of IT system and SCADA system requirements.

	Requirement	IT Network	SCADA Network
1	Ambient Temperature Range	0 to 40-degree C	−40 to +70-degree C
2	Environmental Conditions	Moderate (office)	Severe (e.g. Dust, moisture, chemicals, water)
3	EMI/RFI Conditions	Moderate (office)	Severe
4	Power Supply	110 Volts AC (wall plug)	9-60 Volts DC
5	Life Cycle	3-5 years	25+ years
6	High Jitter and Delay	Maybe acceptable	Serious Concern
7	Response and Interaction	Consistent response, less critical emergency interaction	Response to human and other time-critical interaction is crucial
8	Fault Tolerance	Less important	Essential
9	Security Mechanism	High Integrity	High Availability
10	Risk Management	Focuses on message integrity and data confidentiality	Focuses on human safety and protection of process
11	Access to Components	Usually Locally found with easy access	Majorly Remotely Located, needed extensive physical effort to access
12	Managed Support	Diversify support from different vendors	Generally Single vendor support system
13	Communication	Standard communication protocols	Proprietary and standard communication protocols
14	Patch management	Easy to install, Remote and automated at the enterprise level	OEM vendor specific, long time to install
15	Testing and audit policy	Use robust and modern methodology	Tune testing methodology, susceptible to failure of equipment while testing
16	Incident response	Easy to develop and deploy	Depends on System renewal
17	Compliance	Eventual governing methodology	Specific governing guidelines

(Mackenzie 2012). For example, in the Hatch nuclear power plant, On March 2008, software engineers applied software updates on a single computer, shutting down the entire plant (Kesler 2011). In addition, the controllers used in SCADA systems are based on a proprietary operating system, and as a result, patches are only available to OEM vendors. Therefore, security upgrades can only be patched by vendors and many security updates cannot upgrade in plants. Daily maintenance of security upgrades according to security alerts in a SCADA system is more problematic.

2.3. Operational requirements

Most IT devices are deployed in well-controlled environments, such as corporate sectors or server rooms. In contrast, most of the sections of the SCADA system exist on the plant floor. Electrical and environmental conditions in the plant are much more severe. This condition might cause degradation or failure of the system. Therefore, devices deployed in the system must be designed accurately according to the requirements. Also, the lifecycle of the components in the IT system is designed for shorter-term usage, compared to SCADA components (Stouffer et al. 2006). Therefore, the design choice of the components in a SCADA network should be taken into consideration so as to ensure a long-lasting product. As a result, a control engineer needs ultra-reliable hardware and sound knowledge of SCADA security implementation before configuring components into a SCADA network. Listed below is a comparative table of IT and SCADA system requirements:

3. Contribution towards SCADA vulnerability assessment

Whilst several professional bodies and businesses are involved in the assessment of SCADA vulnerabilities, in several cases, it is a determination of government that plays a vital role. The U.S. Department of Homeland Security- National Cyber Security Division's Control System Security Program (DHS -CSSP) and Industrial Control System Computer Emergency Readiness Team sponsored by DHS have performed a cyber security assessment for Industrial Control System along with United States Computer Emergency Readiness Team (NCCIC 2016). In this case, the vulnerability assessments have been performed using field knowledge gained by real incident responses. Accordingly, remarkable findings have been published in a series of reports and advisory databases. These security controls are defined by considering similarity in a framework of SCADA, PCS (Process Control System) and DCS (Distributed Control System). In addition, the UK national infrastructure department is currently working on the understanding and mitigation of electronic risks to industrial automation by taking help from the Centre for the Protection of National Infrastructure (CPNI). The CPNI funded program focuses on vulnerabilities and protection research on industrial infrastructure awareness by sharing information in forums on SCADA threats, incidents, and mitigation through SCADA and Control System Information Exchange (SCSIE). Moreover, Electronically - SCADA and Control System Information Exchange (E-SCSIE) is working on protection policies and control of SCADA systems of European governments and industries along with other security programs developing in the USA, Canada, Australia, New Zealand, and Europe. So far, CPNI has recommended nine best practice guidance documents for process control and SCADA security assessments as part of a SCADA vulnerabilities awareness program (CPNI 2011). The U.S. Federal Energy Regulatory Commission (FERC) and government authority of Canada motivate NERC (North American Electric Reliability Corporation) to implement these to enhance security and reliability of the power system in North America. For this to be successful, NERC implements and applies security standards to a bulk power system, and monitors and assesses the power system for future adequacy (Leszczyna 2018). Furthermore, NERC audits operators, owners, and users for security measures and accordingly trains industry workers for security concerns. NERC is also working on cybersecurity standards of bulk electric systems. These standards include measures of audits and non-compliance levels that can be subject to a penalty(NERC). More specific to SCADA vulnerabilities, NERC sponsored a one-day workshop on how the global community is responding to emerging threats and vulnerabilities of SCADA networks on March 3, 2011 (NERC 2011). This workshop majorly focused on tools and techniques of ethical vulnerability research disclosure and various mitigation strategies. Furthermore, in September 2014, NERC and FERC began an initiative to assess plant entities for restoration and recovery of bulk power and released a report in January 2016 (NERC 2016). Based on the provided recommendations, they initiated another study in January 2017 on “Grid Restoration, Recovery Plans Absent SCADA or EMS (PRASE)” to estimate the impact of the loss of Inter-control Center Communications Protocol (ICCP) functionality during the restoration of the system (FERC-NERC 2017).

Table 2
Vulnerability assessment reports by various organizations.

Organization	Source of Report
Air Force Institute of Technology (AFIT)	Distinguishing Internet-facing ICS Devices using PLC Programming Information (2014)
Centre for the Protection of National Infrastructure (CPNI)	Cyber security assessments of industrial control systems a good practice guide (2011)
Department of Homeland Security (DHS)	Malware Trends (2016) Common Cybersecurity Vulnerabilities in ICS (2011) Common Cybersecurity Vulnerabilities Observed in ICS (2009) Common Control System Vulnerabilities (2005)
DigitalBond	Leveraging Ethernet Card Vulnerabilities in Field Devices(2011)
Department of Energy (DOE)	Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program (2008)
Electric Power Research Institute (EPRI)	ICCP: Threats to Data Security and Potential Solutions (2001)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Industrial Control Systems Assessments 2014 - Overview and Analysis Incident Response Summary Report - 2009-2011
Idaho National Laboratory (INL)	Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector (2017) Vulnerability Analysis of Energy Delivery Control Systems (2011) NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses (2010) Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program (2008) Safety vs Security (2006) Cyber Incidents Involving Control Systems (2005)
National Cybersecurity and Communications Integration Center (NCCIC)	ICS-CERT Annual Vulnerability Coordination Report Industrial Control Systems Cyber Emergency Response Team 2016 NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report
North American Electric Reliability Corporation (NERC)	Top 10 Vulnerabilities of Control Systems and their Mitigations (2007)
Positive Tech	SCADA Safety in Numbers (2012)
Toolswatch	Top 10 Most Dangerous ICS Software Weaknesses (2015)
Wind River	Caution: Malware Ahead - An analysis of emerging risks in automotive system security (2011)

A non-profit center, Electric Power Research Institute (EPRI), gathers leading organizations, engineers, scientists, and several industry experts to jointly focus on the key success of the electric power control system challenges. The collaboration work of NERC Control Systems Security Working Group (CSSWG) and the U.S. Department of Energy National SCADA Test Bed (DOE -NSTB) summarised potential risk of electricity sectors, described mitigation policies and provided a list of most common vulnerabilities to the control system. Table 2 represents a list of vulnerability assessment reports presented by various organizations for the control system. National SCADA Test Be(NSTB), Idaho National Laboratory (INL), Pacific Northwest National Laboratory (PNNL), Sandia National Laboratories (SNL), Lawrence Berkeley Laboratory (LBL), Los Alamos Laboratory (LAL), Oak Ridge Laboratory (ORL) and the National Institute of Standards and Technology (NIST) along with Department of Energy (DOE) working on various initiatives towards cybersecurity challenges of energy system as part of Cybersecurity for Energy Delivery Systems (CEDS) program (Office of Electricity 2003). Their major functions include verification and validation of security algorithms, techniques, vulnerabilities, and threat assessments of various SCADA systems for automated industries and testing of various products. Refer Table 3 that indicates the list of SCADA projects under development in various laboratories.

4. SCADA vulnerabilities and recommendations

Every industry aims to achieve a substantial increase in their productivity by reducing operational cost and fault tolerance. One of the online research articles, “Global SCADA Market 2017-2021” has forecasted the vendor strategies and future market trend for SCADA (TechNavio 2017). The report summarized the most prominent vendor’s strategies in the global SCADA market. These vendors include ABB, Schneider Electric, Honeywell, General Electric, Rockwell Automation, Mitsubishi Motors, among others. Commenting on the report, the future market demands cloud-based SCADA system. This can be achieved by adopting efficient and secure SCADA strategies in the organization by owners and vendors. However, as per the market survey, one of the greatest challenges for the vendors is the lack of knowledge regarding the implementation of cyber security standards in the product (TechNavio 2017). These weaknesses in the product then translate into an increased risk level for the vendors. These risks include damage of brand name, financial implication, reduction in share value, and most importantly, loss of life (Nicholson et al. 2012). Table 4 reveals the statistics of SCADA vulnerabilities in top vendor products (SCADA Vulnerabilities and Exposures Database).

Vulnerability assessment is typically a highly subjective process; it requires powerful analytical strategy and computational methodology. For a thorough review of SCADA weaknesses and recommendations, we have followed multiple advisory databases, named – NVD (National Vulnerability Database), CVE (Common Vulnerabilities Exposures Database), CWE (Common Weakness Enumeration Database), and SVE (SCADA Vulnerabilities and Exposures Database). According to incidents reports on these databases, since 2007 around 886 SCADA vulnerability incidents have been reported. Substantially, more than 250 SCADA vulnerability incidents have reported in 2015, followed by 125 in 2016, 148 in 2017 and 56 CVE entries have been noted so far in 2018. The above summary represents a current assessment to the best of our available knowledge; however, it is not every company is interested in disclosing their vulnerabilities publicly. Also, by referring to real incidents in vulnerability databases, we have classified vulnerabilities taxonomy in a broader way. Each sub-section of this section will typically illustrate a specific category of vulnerabilities in a SCADA system. Moreover, each sub-section will conclude with common vulnerabilities and corresponding recommendations summary table. These vulnerabilities are derived according to the findings of the faulty systems and most of them were updated by best practices. Note that all the recommended security practices in this section are just examples. Furthermore, each point is derived according to the survey incidents reported. We try to cover focal points in the summary-table

Table 3
Various laboratories and vulnerability assessment projects of SCADA.

Laboratory / Project Name	Organization Name	Period	Country	Source URL
DETER project	DETER Lab	Since 2003	U.S.	http://deter-project.org/
CRUTIAL (Critical Utility Infrastructural resilience) project	CESI RICERCA	Since 2006	Italy	http://crutial.rse-web.it/
Cyber Security for Distributed Energy Resources Systems	EPRI	Since 2013	Canada	http://eprijournal.com/securing-the-grids-edge/
ENEA Test ENEA's Critical Infrastructures Protection Program: SCADA Cybersecurity	Safeguard EU-Project	Since 2009	Italy	http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_download&gid=316&Itemid=58
European Network for Cyber Security (ENCS)	Alliander	2012-2013	Netherlands	https://encs.eu/activities/
European Reference Network for Critical Infrastructure Protection	European Commission (ERNCIP)	Since 2011	Italy	https://erncip-project.jrc.ec.europa.eu/
Security Program for Hydropower Projects Revision	FERC	Since 2009	U.S.	https://www.ferc.gov/industries/hydropower/safety/guidelines/security/security.pdf
Idaho National Laboratory	INL	Since 1979	U.S.	https://www.inl.gov/research-program/critical-infrastructure-protection/
Illinois Center for the smarter electric grid (ICSEG)	University of Illinois		U.S.	http://icseg.iti.illinois.edu/
Industrial Instrumentation Process Lab	British Columbia Institute of Technology		Canada	https://www.bcit.ca/appliedresearch/centres/industrial.shtml
Japan Center security System Control (CSSC)	Advanced Institute of Science and Technology	Since 2012	Japan	http://www.css-center.or.jp/en/index.html
KEMA Test Centre	DNV KEMA	Since 2012	Netherlands	https://www.dnvgl.com/services/?QueryString=SCADA
SCADA Security Laboratory and Power and Energy Research laboratory	Mississippi State University	2011	U.S.	http://www.ece.msstate.edu/
National SCADA Test Bed (NSTB)	NSTB Multi-Laboratory Team	Since 2003	U.S.	http://energy.gov/oe/national-scada-test-bed
Pipelines 101	Interstate Natural Gas Association of America (INGAA)	Since 2011	U.S. and Canada	https://www.ingaa.org/Security.aspx
SFP 983805 - SCADA Testbed Simulator	Faculty of electrical engineering and computing, University of Zagreb	Since 2012	Hrvatska	http://www.fer.unizg.hr/NATO_SNG/
The Virtual Power System Testbed (VPST) and Inter-Testbed Integration	University of Illinois	Since 2009	U.S.	https://www.usenix.org/legacy/event/cset09/tech/slides/bergman.pdf
TRUST-SCADA Experimental Testbed	Team for Research in Ubiquitous Secure Technology	2008-2013	U.S.	http://www.truststc.org/
Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project	University of Illinois	Since 2010	U.S.	http://tcipg.org
Virtual Control System Environment (VCSE)	Sandia National Laboratories	Since 2009	U.S.	http://www.sandia.gov/ccd/projects.html

Table 4
Statistics of SCADA top vendor's vulnerability disclosure (Year 2013-2018).

Top Vendors	CMS	HMI	NETWORK	OPC	OTHER	PLC	RTU	SOFTWARE	Vulnerability (Count)
ABB		1		1	3			1	6
Advantech		1			8	1			10
Allen-Bradley		1		1	2	2			6
General Motors					1				1
Honeywell					1			1	2
Mitsubishi					1				1
Moxa	1		2	2	17		1		23
MySCADA					1				1
Rockwell Automation					14	2		1	17
Schneider Electric		3			29	7	1	2	42
Siemens		2	1	1	50	3		4	61
SpiderControl					3				3
VTScada		1							1
Windows		18		12	2	1			33
Yokogawa					1	1			2
Total	**1**	**27**	**3**	**17**	**133**	**17**	**2**	**9**	**209**

released by the various government and standard organizations as part of SCADA security awareness and enhancement program.

4.1. SCADA product/software security vulnerabilities

Secure design and development of SCADA products is the primary step towards securing a SCADA system. Mostly, SCADA application suffers due to inappropriate validation practice, poor scriptwriting, and/or improper exceptional handling technique by the programmer. One of the real-time examples of bad programming vulnerability introduced in the product is Stuxnet warm along with hardcoded username and password running in the WinCC database, PCS SCADA software (Nicholson et al. 2012).

4.1.1. Improper input validation

A technique of input validation is used to ensure that the input applied to a system does not allow an intruder to gain access to unintended functionality or privilege escalation (Chaffin and Nelson 2011). However, buffer overflow, lack of bounds checking, command injection, cross-site scripting, and directory path traversal are the common loopholes of SCADA software implementation. These threats lie under the category of improper input validation and they are capable enough to alter the control flow of the program. Compared to other vulnerabilities, buffer overflow is the most frequent entry point for SCADA exploitation (Nicholson et al. 2012). As per the previous 8 years (2011 to 2018) of CVE statistics, around 49% of improper input validation SCADA vulnerabilities were reported owing to overflow in buffer size, 30% owing to command injection, 15% due to cross-site scripting and 6% due to directory path traversal and lack of index validation (Common Vulnerabilities Exposures Database).

4.1.1.1. Buffer overflow: A buffer overflow occurs when malicious code tries to overwrite adjacent memory by providing more data into a buffer than assigned memory. If, a function code does not write and validate by the control engineers properly, allowing attackers to modify the program execution in PLCs/RTUs (INL 2010). Many exploits found in buffer overflow vulnerabilities point out poor code development by vendor or by individual programmer (Nicholson et al. 2012). Table 5 represents an example of buffer overflow vulnerabilities discovered in SCADA products (Common Vulnerabilities Exposures Database; National Vulnerability Database; SecureAuth Labs). Inadequate function implementation of SCADA protocols is also vulnerable by malicious packets. These packets interpret and alter network traffic. Moreover, SCADA services define protocol traffic. Defective services are the possible entry point on the SCADA network. Hence, service and function validation should be the main target of laboratory assessment before launching a product to the market.

Similarly, lake of bounds checking occurs due to unvalidated input or negative index value of an array. Altering index values to a negative number generates out of range indexes that cause DOS (Denial of Service) and sometimes crash SCADA system communication or proprietary fault tolerance network equipment protocols (Chaffin and Nelson 2011). Even though inputs have not been entered directly by users, SCADA traffic may be intercepted during transmission. Hence, integrity checks play a vital role during validation and testing of the module.

4.1.1.2. Command injection and Cross-site scripting: SQL Slammer worm is one of the real threat examples of SQL injection which infected in a Davis-Besse nuclear power plant in Oak Harbour as a threat of denial of service (DOS) attack (Holloway 2015). This worm can directly attempt DOS attack due to vulnerabilities in SCADA software, it is not mandatory that DOS be applicable to generic network communication (Nicholson et al. 2012). Moreover, SCADA Command injection includes two major types of vulnerabilities: (1) OS command injection, and (2) SQL injection (INL 2010). These vulnerabilities have been constructed from external input without proper sanitization (DHS-NCCIC 2015). To avoid such vulnerabilities, control engineers should use library calls instead of external processes. They should focus more on store procedure and prepared statements while programming. Likewise, cross-site scripting is a part of fake website scripting injected in the client machine to get the privilege of a web server. For that, phishing attack is used to access the login credentials of the client machine. For better protection of SCADA application, the organizations should use tested and confirmed third-party web servers to host their SCADA application remotely.

4.1.2. Poor code quality

Poor code quality results in a lack of security features in the product. This does not necessarily refer to the vulnerabilities in the product but rather causes the product to act like an insecure product. A program which is more complex and difficult to maintain has a higher probability of vulnerabilities that are easily suppressed in the code (Homeland Security 2015). These products are more likely vulnerable when compared to secure products. Various SCADA code reviews specify that software design and implementation of SCADA system does not follow secure software development lifecycle in general. The unsafe function calls in a proprietary application and especially in OPC dynamic-link libraries (DLLs) easily make SCADA system vulnerable (Homeland Security 2015). Therefore, vendors or asset owners should arrange special training sessions for SCADA developers to train them on secure coding practices.

4.1.3. Improper control of a resource

Misconfiguration or poor maintenance of the product along with hardware and the operating system also contribute to SCADA vulnerabilities. Multiple assessment reports found old and unpatched versions of SCADA software and firmware systems with some applications just being patched with security fixes(DHS and CSSP 2008). However, these applications remain open to other cyber attacks. Weak database versions, vulnerable web server versions, and feeble SSL libraries are examples of unpatched SCADA products. Generally, patches are release after the vulnerabilities are discovered, however, there could be a possibility of a time gap between a new patch release causing vulnerability (Nazir et al. 2017). Furthermore, sometimes patches will introduce unknown vulnerabilities due to real-time deployment without proper testing (Carlson et al. 2005). Two major issues are identified with regards to poor patch management: (1) lack of patches, and (2) failure rate of patches. In 2011, ICS-CERT identified that 60% of vulnerabilities in control system resulted owing to failure rate of patches, and less than 50% of vulnerability patches were available at that time. Hence, it is important for policymaker and technology specialist to make sure proper patch management and certification of the products during software upgradation and maintenance. After a thorough review of incidents reported into SCADA advisory databases, we have summarized SCADA software vulnerabilities and correlated recommendations in Table 6. The reader can review a detailed description of each element by referring to the citations mentioned in the table. For greater details on configuration management program, readers can also review Section 6.2.4 of special publication of “Guide to ICS security” published by NIST (Stouffer et al. 2015).

4.2. SCADA system configuration vulnerabilities

SCADA vulnerabilities are not only inherited by insecure products but also depend on the installation and maintenance of the system. Although the design specification of a SCADA product may limit the embed security features, the organizational risk can be

Table 5
Examples of SCADA buffer Overflow vulnerabilities (Year: 2011 to 2018).

Targeted components	A strategy of attacks & Damages	Number of CVEs found CVE Database References (163 total entries found)
Stack-based buffer overflows (61 CVE entries found (37%)):		
OPC client, SCADA hosts, OLE for OPC server, A historian of SCADA, PLC application, SCADA micro -browser, Server interface	Attackers remotely executed the code on SCADA hosts; Abnormal program termination due to runtime error; Allows intruder to obtained and modified sensitive information or cause a denial of service through crafted POST request or via traffic on various TCP ports (e.g. 5000,4013); Allow local attackers to gain access rights through malformed DLL file; Random code execution on software to gain access to SCADA software.	CVE-2018: 7499, 17911, 18999, 20410 CVE-2017: 12707 CVE-2016: 0868,2292,3962,4512,4519 CVE-2015: 1000,7909,7937, CVE-2014: 0753,0764,0765,0766,0767, 0768,0770,0774,0782,0783,0784,0787, 0985,0986,0987,0988, 0989,0990, 0991, 0992,3888, 8388,9190,9204,9205, 9206 CVE-2013: 0657,0680,2687 CVE-2012: 0238,0254,1800,1830,3007,3008,4353,4708 CVE-2011: 0488,0517,1918,2089,2959,3142,3492,4052, 4519,4875,5007
Multiple buffer overflow (11 CVE entries found (7%))		
OPC-Automation server, Object ActiveX control components, VAMPSET, DLL components, Web server, SCADA server, PLC application.	Allow Internal intruder to gained access privileges through malware attack to record data in the CFG/DAT file; Allow external attackers to caused DOS through long arguments or malformed request through HTTP or FTP server; Allow external attackers for arbitrary code execution via long string/crafted data packets/ crafted HTML documents/long filename or long separators.	CVE-2014: 8390,0789 CVE-2013: 3075,2785 CVE-2012: 4700,0929, CVE-2011: 4870,4537,4529,0342,0340
Multiple Heap-based buffer overflows (2 CVE entries investigated (1%)):		
HMI application, Web server.	Attackers remotely performed arbitrary code execution on a web server; Attack via crafted packets.	CVE-2016-0857, 1564
Heap-based buffer overflows (20 CVE entries reported (12%)):		
OPC server, Web interface, ActiveX components, SCADA node, Information server, Application server, HMI, Runtime loader.	Attackers remotely executed code on hosts via crafted packets/long filename/crafted HTML request/ long string/unspecified vectors; Cause denial of service via crafted web pages/malformed HTML documents.	CVE-2018-8845, CVE-2016: 4509,2290,0869 CVE-2015: 7939,0979 CVE-2014: 0781 CVE-2013: 0658 CVE-2012: 2427,1831,0258,0257 CVE-2011: 4536,4520,3498,3491,3321,2961,2960,0406
Multiple stack-based overflows (19 CVE entries examined (12%)):		
Packet-parsing application, Modbus serial driver, Web-based SCADA, HMI based products, Web server, DLL files, VAMPSET,	Allow remote attackers to gain sensitive information through weblink; Arbitrary code execution with user privilege through PLC;	CVE-2018-1090, CVE-2016:3988,0856, CVE-2015:1001,0986, CVE-2014:9208,9202,5407,2364 CVE-2013:0662, CVE-2012:2515,1801,0245, CVE-2011:3493,3490,2962,1919,1567,1563
Buffer overflows (46 CVE entries found (28%)):		
Modbus/OPC - RPC Server, Modbus/TCP - OPC Server, ActiveX Control, Network interface, Historian database, HART device type library, ActiveX control, Gateways along with firmware, Ethernet module	Allows internal SCADA users to cause a DOS via malicious packets/ DLL/ unspecified vectors/ crafted RPC request/ long parameter/ invalid field name/ malformed URL/ crafted HTML document; Allow remote attackers to gain access to the network; Allow local users to gain privileges through DLL file/ inserting a long string	CVE-2018-1789 CVE-2016:4528,2280,0860 CVE-2015:3977,1449,0982 CVE-2014:9203,9188,8514, 8513, 8512,8511, 8385 CVE-2013:2688,0675, 0674, 0656 CVE-2012:6438,6436,4715,4711, 4696, 3815, 3035, 2598, 1817,1805, 1802, 0243,0227, CVE-2011:5163, 5089,4535,4526,4524,4055,4050, 4045,4037,4034,4033,3330,3141,2530,1914
Integer based overflows (6 entries found (4%)):		
Human-Machine Interface (HMI), Web server	Gain administration access; Allow unauthorized disclosure of information;	CVE-2018-17897 CVE-2016-0859 CVE-2012:4706,3793 CVE-2011:5008,4043

controlled by securely configuring the SCADA system in the network (INL 2010). The common vulnerabilities related to SCADA system configuration include poor system access control along with open network shares on SCADA hosts, cryptographic issues, feeble authentication, weak credential management, inefficient planning, and poor policies and procedures. Also, exploitation of vulnerable SCADA services is more dangerous in nature. That allows attackers to gain the privilege of any account holder with full accessibility. Those accounts may be an account of manager or database administrator or root level access on SCADA hosts. This means owing to flaws in software configuration, external or local attackers can potentially gain access to a SCADA network. However, Owners could increase the assurance of secure configuration by applying detailed security instructions and automated security configuration packages (Chaffin and Nelson 2011). During the procurement of a product, an administrator should have a detailed instruction set that

Table 6
SCADA product/software vulnerabilities and recommendations.

Vulnerability	Recommendation
Improper Input Validation (INFOSEC; Department of Energy 2008; Chaffin and Nelson 2011; Homeland Security 2015)	
Buffer overflow	1. Coding practice should incorporate length validation according to inputs; 2. Size of a buffer should not be identified by user inputs; 3. Sanity and integrity checks need to be implemented to avoid fuzzy attempts to crash the network or server by DOS.
Lack of index validation	1. Programmers should be trained to implement secure code by adopting index validation in practice; 2. To avoid network traffic intercept index value check needs to be implemented.
OS & SQL injections	1. Create static function calls for external commands; 2. Use library calls implementation technique in programming; 3. Use strict validation rules to accept input strings; 4. Use prepared statement, parameterized or stored function to process SQL queries.
Cross-Site Scripting	1. A web server should be tested and validated thoroughly for malformed inputs; 2. Developers can add an extra layer of protection using open source libraries which automatically detect the encoding of the data which must be filtered to prevent the system from XSS attacks; 3. Implement alerts and intrusion detection system for web browser and email security.
Directory path traversal	1. Specify strict acceptable inputs in a list; 2. Input string should be transformed into acceptable input before being validated.
Poor Code Quality (Quinn et al. 2009; Pauna and Moulinos 2013)	
Invalid function calls	1. The custom application should be implemented using security features; 2. Code review should perform during each iteration of testing; 3. SCADA protocols should integrate integrity check and authentication.
Improper resource shutdown of release	1. Product deployed into SCADA environment should also be passed through security check; 2. During the procurement process, asset owners should explicitly understand the security features of a product.
Null pointer dereferences	1. Null pointer dereferences can be prevented using a sanity check method before all pointers are modified.
Improper Control of Resource (NERC 2005; DHS and CSSP 2008; Pauna and Moulinos 2013)	
Poor patch management and security configuration	1. Management policies should include below mentioned elements in patch management program: 1.1 Configuration & patch management Plan 1.2 Incident responses plan 1.3 Vulnerabilities notification plan 1.4 Risk assessment plan 1.5 Backup/Archive plan 1.6 Disaster recovery plan 1.7 Complete and unified control system asset inventory plan 2. Consider below key points to maintain documentation of patch related alerts: 2.1 Keep all the records of relevant patch alerts 2.2 Define proper cataloging of patch related alerts 2.3 Maintain test results of the specific alert 2.4 List out possible solutions for each alert 2.5 Label best practices for patch management/configuration 3. Vendors should support in patch testing; 4. Vendors should provide the service for patch upgrades based on findings; 5. Vendors should always follow the latest version of the third-party software and update the current version by add-ins before delivering the product.

includes a list of necessary applications and services along with permissions and privileges, details of allocated ports and components (Quinn et al. 2009).

4.2.1. Feeble access control mechanism

The foremost task of securing SCADA networks is to ensure that unauthorized users do not gain access to the network. Therefore, it is crucial to define strong access control mechanism policies. However, defining proper rules of access control policies on the SCADA network is a very difficult task (Igure et al. 2006). In 1997-1998, one survey presents, owing to economics of staffing, 50 water utilities control 60% of their system using a dial-up connection (Hildick-Smith 2005). This indicates, over 20 years ago, remote accessibility of control systems was in demand. Generally, a SCADA network is connected to the outside world via Gateway links. Unfortunately, these gateway links are not the only connection with the internet. There may be other vulnerable connections to gain access to an entire network such as telephonic lines, modem dial-up links, fax lines, etc. This terminology is known to enter into the SCADA network through multiple pathways. Also, some devices never have shown their appearance in the network. For example, laptops that are carried in and out from the plants, as well as USB keys, move from one computer to another computer for data transfer. These devices can easily spread viruses or malware in the network (Mackenzie 2012). As a technical solution perspective, dedicated VPN gateways must be implemented in the control sites to ensure the security mechanism, such as user authentication, recipient confidentiality, and message integrity. Also, these features must be flexible to various SCADA protocols (Igure et al. 2006).

4.2.2. Poor authentication

Proper authentication is the primary step towards achieving strong access control. Only authorized users can gain access to a SCADA network using their login credentials. However, owing to an insecure password policy mechanism or by social engineering attacks unauthorized entities may succeed in cracking the login information. Many solutions have suggested potential way to deal with this issue. For example, one of the solutions is to select smart card-based authentication (Sauter and Schwaiger 2002). Smart card security stores the user's passwords and helps to improve the key-management policies. Fingerprint or retina scan can also be used for authentication. These techniques support adding one more layer of security (Grother and Salamon 2013). While defining authorization policies, assignment of permissions and privileges according to the role of the users is very important. Also, User should assign permission based on the principle of least privilege. As a result, vendors are expected to define proper product policies for specific account types. In addition, asset owners should follow proper permission and privilege assignment for each user type. However, proposed solutions do not eliminate all the typical authentication problems of the SCADA network, but it will help to strengthen the security of a SCADA network.

4.2.3. Cryptographic Issues

Mostly, SCADA networks use proprietary protocols and remote access services that usually support unencrypted plain text network communication. Some features of the control system use RPC (Remote Procedure Call) which follows open link communication and a root cause of the Blaster worm. Many network sniffing tools are freely available to view such network traffic. However, encryption is not always a feasible solution for cryptography in SCADA networks. Real-time communication is always time critical and should be accurate for a reply-response mechanism for control systems. Therefore, timing concerns may make encryption unfeasible (Baily and Cooke 2005). As well, Aircraft-NG is a freely available tool, which can easily sniff and decrypt wireless communication packets (Nazir et al. 2017). According to a survey, many weak hashing algorithms and pseudo-random number generator routines make SCADA systems more vulnerable (Chaffin and Nelson 2011). Consequently, proper research and awareness of recent SCADA vulnerabilities are one of the key points for control engineers and developers.

4.2.4. Poor credential management and maintenance practices

The disturbing fact is that industrial infrastructures are not only vulnerable to cyber attacks by terrorists or external attackers but also exposed by disgruntled internal employees or by script kiddies. As noted in a presentation by Internet Security Systems, many credential management systems of SCADA use a common username like "admin" or "console" instead of real usernames (Blau 2004). This creates an ambiguity to trace internal intruders. Credential information stored in configuration files which are openly shared and few hashes are not properly protected. Also, many default login credentials of product databases are available online in SCADA default Password Database (SDP Database). This becomes a critical issue as, most of the time, while configuring SCADA software, default username and password remain unchanged by the installer. Moreover, the automatic termination of the session setup was not incorporated during configuration. These may lead attackers to gain the privilege of the network or database server to crack the system. LM (LAN Manager) password hashes are one of the feeble password protection techniques, which supports 14 characters longer password only. Another example is administrator passwords displayed on a web page using database server configuration (Giannopoulos 2018). Therefore, it is important for vendors and owners to get acquainted with proper password protection policies.

4.2.5. Inadequate policies and procedures

The first step towards implementing cyber security can be achieved by compiling security rules with the steps of implementing a procedure for the unique requirements of the organization. This includes rules for risk assessment and management according to loopholes in the system. If the organization has a failure in planning and implementing policies for cyber security, then that will incur vulnerabilities in the system. Rapid SCADA, software version 5.5.0 was affected owing to weak access control restriction policies. This specific vulnerability exists in an access control mechanism that is established and altered during product installation. An attacker could influence the vulnerability by overwriting original files to elevate administrator rights as the installation folder has full access privilege for any user in the system. This means any insider in the system could execute this attack. Perhaps more alarming, according to an advisory report, at that moment the vendor refused to focus on the vulnerability informed to them (Oliveira 2018). Ultimately, in February 2018, CVE was assigned to the vulnerability due to flaws in software configuration (CVE-2018-5313). In such cases, apart from the technical solution, it is important to define clear security policies in the organization to protect a network from insiders. These security management policies must be ensured by all the employees of the company by adopting in their daily practices. To generate and maintain centralized security documentation in a timely manner is the foremost task of compliance team. Also, reviewing, updating, and implementing security plans during security audits will strengthen the security of SCADA system. Table 7 illustrate vulnerabilities owing to poor configuration methodology and consequent improvisation techniques.

4.3. SCADA network security vulnerabilities

The network architecture of the SCADA system must be securely constructed and deployed in order to allow remote users access for monitoring and processing of data according to business needs. During implementation, one of the crucial points is to make sure that the control network must be always segregated from incoming and outgoing traffic. For that, the deployment of security zones with well-defined access control rules is one of the key factors (Knapp 2011). That will reduce intentional and unintentional risk owing to attacks. The exploitation of the control network can be formed using allowed IP addresses, port numbers or a set of protocols and rules. Consequently, building security features in assigned services and protocols are equally important. Also, a proper understanding of the limitations of security products provided by vendors is essential for secure network design and implementation. A well-known strategy "defense-in-depth" layers security mechanism can minimize the impact of failure which might occur due to product and configuration vulnerabilities (Fabro et al. 2016). This strategy is originally formed from military security strategy to provide the barriers to obstruct the attackers in their periphery (Fabro et al. 2016). This is a holistic approach to protect all the components of the SCADA network by considering all interconnects and dependencies.

4.3.1. Network design fragility

The security perimeter is used to distinguish corporate network devices and SCADA network devices logically as well as physically by referring documented access points. But defining a single security perimeter clearly is not enough. To ensure the proper configuration and deployment of SCADA security controls, plants should be formally broken down into the level of segmentation called zones and traffic between those areas should be controlled by conduits. Conduits define allowable traffic among zones. ANSI/ISA99 and IEC 62443.02.01 series of standards define concepts of zones and conduits to ensure the protection of SCADA network for the region of North America and European countries (ANSI/ISA 2007; Alves and Morris 2018). It was identified that 80% of routers are vulnerable to cyber attacks owing to the inefficient security configuration and that may make network connections open for backdoors and holes (Eckstein 2014). Improper definition of security perimeters along with minimal security interfaces (zones) allow vulnerabilities enabling exploitation of the system (Rao et al. 2017). This can lead to unauthorized access of control related traffic from corporate LAN and misuse of control network services. Advantech Web Access is providing solutions for IOTs, cloud computing, and SCADA & HMI software. The products are deployed in East Asia, the United States and Europe in various sectors such as manufacturing, energy, wastewater units. All SCADA Node versions prior to 8.3.1 of Advantech WebAccess is not only vulnerable to external and local attackers due to external control file name or path but also have other multiple vulnerabilities like security bypass, privilege-escalation, denial of service, multiple arbitrary code execution. These weaknesses may allow attackers to delete or modify the network configuration file (SecurityFocus 2018). Mat Powell and Steven Seely working with Zero Day Initiative, have reported

Table 7
SCADA configuration weaknesses and recommendations.

Vulnerability	Recommendation
Feeble permission and privilege for access control (Igure et al. 2006; Oliveira 2018)	
Improper authentication and access control	1. All installations should not start at root users (privilege mode); 2. Assign role-based authentication for component communication used in SCADA; 3. SCADA services and protocols should restrict access control of the system from another host machine without proper authentication.
Improper privilege management	1. Dedicated VPN Gateways must be implemented in SCADA network; 2. Vendors and asset owners should ensure to use a concept of least privileges assignment policy according to user role; 3. Generate multiple accounts for multiple functions with default configurations to each account type.
Poor Authentication (Grother and Salamon 2013; Nazir et al. 2017)	
Weak authentication controls	1. Organizations should define scope, role, purpose, responsibilities, coordination, compliance etc. to facilitate proper authentication policies and control; 2. NIST SP 800-63-3 specify guidelines of digital identity, NIST SP 800-63A,63B,63C signifies remote electronics guidelines; 3. A system should identify and authenticate users by their functions, User functions should differentiate as role-based, group-based and devices based; 4. Before establishing a connection, identification and authentication of the system from specific safeguard is mandatory; 5. Proper physical security controls should confine local emergency actions.
Cryptographic Issues (AGA 2006; Grassi et al. 2017)	
Broken encryption techniques for sensitive information	1. SCADA control engineers and developers should properly research before incorporating encryption solution in the product; 2. Security experts should update the team regularly on published vulnerabilities to keep patches up to date.
Poor Credential Management (Chaffin and Nelson 2011; Nicholson et al. 2012)	
Use of hardcoded credentials	1. SCADA vendors should replace all the hard-coded credential with secure functions stored in a configuration file; 2. SCADA integrators should have a facility to use secure protocols for configuration, they should have the privilege to disable the services of a hard-coded password.
Unprotected password transmission in the network	1. SCADA vendors should remove an unsecured layer of the protocol by replacing common IT services like FTP (File Transfer Protocol), telnet, rlogin and HTTP with Secure Shell – SSH and HTTPS; 2. Avoid use of LM (LAN Manager) password hash technique due to easy decoding (decoding can easily perform by Rainbow Tables, John the Ripper, etc.), instead use strong NTLM (NT LAN Manager) hash technique; 3. Control engineers should use key management and encryption technique for protecting login credential.
Inadequate Planning, Policy & Procedure (CPNI 2011; Eckstein 2014)	
Insufficient and poor security documentation	1. Design formal documented security policies, examples are as under: 1.1 List of cybersecurity threats 1.2 List of cybersecurity controls 1.3 Internal and external fragile components 1.4 Funding opportunities for cyber security 1.5 Operational risk assessment policies 2. Maintain and update security policies documents periodically according to loopholes in the system
An improper security assessment process	1. Periodic assessment should perform to validate security controls of the system by factory/site acceptance testing; 2. Outcomes of assessment should rigorously followed-up by management; 3. Security enhancement suggestions should be incorporated into the system.

these vulnerabilities to NCCIC in May 2018. Particularly, considering these vulnerabilities, Advantech released a patch within 3 months-August 2018. To protect the network from such vulnerabilities, it would be recommended to separate control system networks and remote devices through a DMZ configured industrial firewall by proper conduits ruleset to narrow down the focus. Remote access could only be permitted through secure and updated VPNs in allowed zones only (NERC 2017).

4.3.2. Feeble firewall rules

As an administrator point of view, the data processed in the SCADA system is highly time critical, as it always operates real-time. One of the safety system examples is a nuclear power plant (Cai et al. 2008). However, security safeguards such as firewalls and antivirus software drop the speed of entire process or might drop the packets by filtering mechanism, causing decreased efficiency of the SCADA system process. Surprisingly, sometimes in such situation, where process delay is intolerable, operators of SCADA system bypass or turn-off the security mechanism (Nicholson et al. 2012). This makes SCADA systems open to cyber-attacks. Also, the configuration of a firewall needs expertise in the field of network configuration which involves training in component specific configuration languages owing to the complex structure and lack of automation tools (Ranathunga et al. 2016).

SCADA system devices should not have a direct connection with the outside world. SCADA networks must be completely isolated from the corporate network using a firewall- DMZ or firewall-VPN technique. Placement of traffic analyzer at multiple levels in the network is the best way to minimize network exposure for companies to protect from cyber-attack. Most of the key points specific to firewall fragility have been included in summary Table 8 has been referenced from the “Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide” (Byres et al. 2005).The American National Standard Institute-International Society for Automation describes the security policy specifications to mitigate vulnerabilities in control systems (ISA 2007). Also, National Infrastructure Security Co-ordinator Center specifically summarized some of the key points of firewall configuration, weaknesses and best practices for SCADA architecture (NISCC and CPNI 2005).

Proper placement of a security system in the network makes a huge impact on increasing security. For example, SCADA system components such as field devices, and control system interconnects should be placed behind a firewall, however this setup is not suitable for IoT enabled interconnects which are sitting in the middle of the supposedly super secured Operational Technology (OT) environment. In such scenario, attackers can intercept the communication link. Hence it is crucial to implement the additional security measures; for example, all the sensitive data travels

Table 8
SCADA network security weaknesses and recommendations.

Vulnerability	Recommendation
Network Design Fragility (Eckstein 2014; Fabro et al. 2016)	
Lack of network segments and functional DMZs	1. SCADA security perimeter should be physically separate from the corporate network by defining proper zones and logically separate by defining proper conduits. 2. Create multi-layers (defense in depth) architecture through zones to break down plant network; 3. Define separate functionalities and separate access privileges via conduits according to the importance of accessibility (interface between DMZ and IT, interface between DMZ and Control network, interface between DMZ and remaining network like Data Server, Data Historian); 4. Use VPNs or DMZs to interconnect IT and SCADA networks for secure communication; 5. The firewall should configure via DMZ to filter specific traffic communication amongst Data Server/Data Historian, corporate IT and control network;
Firewall Rules (Byres et al. 2005; Stouffer et al. 2015; Ranathunga et al. 2016)	
Bypassed firewall	1. All connection of the SCADA network should be routed through a firewall; 2. Avoid configuration of backdoor network access in the organization; 3. Avoid hardwire connections directly with LAN by circumventing firewall; 4. Each SCADA host should be evaluated periodically if sidestepping with a firewall; 5. Never use third network card on a server which can bypass the firewall; 6. A monitoring system should be implemented for any new unknown connection alerts.
Improper configuration of the firewall	1. Configure firewall by IP address, port number, direction and content of both inbound and outbound packets; this will stop sending return connection from the victim PC to the attackers; 2. Implement a stateful inspection firewall for UDP/TCP traffics to filter legitimate packets and session expires; 3. Implement application proxy gateway firewall for specific services like FTP, HTTP, RLogin to prevent a network from unauthorized remote access or file transfer depending on the tolerance of delay in a process; 4. Configure host-based or small stand-alone firewall in front of running individual control devices for backup, support, and maintenance as this could increase significance management overhead; 5. Provide access restrictions of a control system according to the nature of traffic through firewall and DMZ; 6. The structure located into DMZ should turn as antagonistic; Keep very few exceptions between DMZ and control system; exceptional between corporate and control system should be eliminated.
Inappropriate access restriction rules	1. Set of filtering rules which are not only based on a port number but also based on considering used & unused IP addresses to restrict the traffic flow to prevent an attack path by unused addresses; 2. The network components access control list should be well defined and organized; 3. Proper network and subnet mask should be defined for inside and outside interfaces; 4. Password or predefined control list should protect network services accessibility; 5. Email clients should not have any access privilege to corporate LAN.
Poor customize rules for SCADA traffic	1. To create effective firewall and IDS rules, an owner should have documentation from the vendor which will describe how SCADA system components are utilized in the network; 2. In case of unavailability of network requirements and protocol specifications, the network administrator should monitor network traffic to classify normal system behavior and validate control system traffic as and when required; 3. In the case of ever-changing security threats, firewall rules should support acceptable protection; 4. Firewall rules for control system should be identified and implemented carefully by considering few exceptions excluding most of the traffic, incoming traffic of corporate IT must be inhibited into a control network and access-privilege of the control network devices should be assigned via DMZ; Outbound packets of control network should be controlled according to communication requirements and restricted by services and port addresses.
Audit and accountabilities (Chaffin and Nelson 2011; Department of Energy 2011; Stouffer et al. 2015; Mattioli and Levy-Bencheton 2014)	
Lack in management for periodic audit	1. The administrator should use modern audit reporting tools to generate security assessment reports; 2. Unused firewall rules should be removed from the list during a periodic audit; 3. Auditors should identify active services, patch level, and vulnerabilities during an audit; 4. Management should take corrective action according to audit reports; 5. The network administrator should retest the systems to ensure corrective action plan; The network administrator should scan non-productive environments actively to identify potential weaknesses of the system. 6. Management should conduct routine self-assessments and disaster recovery plans.
Poor Logging practices	1. The network administrator should review logging files regularly to identify security incidents; 2. Audit records should contain a timestamp, type, user identity and, the outcome of the event; 3. The proper methodology should be implemented to trace all console related activities; 4. Proper policies should be implemented for log storage, protection, and review.
Week enforcement of remote login policy	1. The network administrator should have an accurate network diagram along with active connections, DMZs, protected subnets, and external networks; 2. All entry points of the SCADA network should be well-defined in security policy; 3. An organization should define media restricted access policy and should verify during periodic audits; 4. During the audit, intrusion detection rulesets of each domain should be monitored.

through the IoT systems, should be encrypted to prevent interception. IoT devices firmware code should use light-weight ciphers for robust handshaking and key-exchange mechanism. Also, these devices should be certified at the time of manufacturing for proper identification and authentication services. Section 6 provides a description of the vulnerabilities and recommendations for IoT systems.

4.3.3. Audit and accountabilities

Technical audit plays a vital role in maintaining ongoing security effectiveness of a SCADA network. A sign of a mature organization is one that establishes a comprehensive security audit and accountabilities of the systems/networks regularly. With established policies and procedures, an organization can ensure compliance by reviewing and assessing adequate network controls, and recommend necessary updates in security controls, policies and procedures through the audit process. The proper establishment of security controls provides a safety measure to respond to problems such as consequential assessment failure or audit log fault tolerance. Sometimes, the network administrator is unaware of the fact that the existing network diagram should be compatible with the present state of the SCADA network (Chaffin and Nelson 2011). Also, many of the process control devices integrated with SCADA system do not have the ability to deliver effective audit results. Hence, more modern tools for audit systems are in demand to review the network activities in critical infrastructure (Stouffer et al. 2015). Audit tools do not only help in eliminating “path of least resistance” that an attacker could exploit but are also useful for analysis of the significance of vulnerabilities to take appropriate corrective action for actual elimination of weaknesses in the network (Department of Energy 2011). Sometimes regulatory compliance adds complexity to authentication management. In this case, diligent usage of log management tools can make available valued assistance from installation through the system life cycle in the SCADA network. For greater details with regards to log management accountability, the reader can refer “log management including audit logs” published by NIST SP 800-92 (Stouffer et al. 2006). We have summarized SCADA network security issues and associated mitigations in Table 8 by referring various network vulnerability reports.

4.4. Flaws in SCADA protocols

Improvement in SCADA protocol security features will automatically strengthen the overall security of a SCADA system (Byres and Lowe 2004). A common vulnerability like IP spoofing and man-in-the-middle attacks are presented in TCP/IP protocols can also reveal a SCADA system as many open standard SCADA protocols are communicating over TCP/IP without incorporating additional protection strategies (Cherdantseva et al. 2016). Deep understanding and analysis of existing protocols and their vulnerabilities will help to incorporate new security mechanisms in protocol specifications. However, incorporating changes can be time-consuming as current SCADA protocol standards are well-defined by international specifications governed by expert bodies. A proper understanding of loopholes will take a few revisions to make changes and create new protocol standards (Igure et al. 2006). During the analysis phase, it is important to differentiate SCADA protocol vulnerabilities in two major categories – vulnerabilities due to inheritance and vulnerabilities due to improper implementation. Typically, protocol vulnerabilities resulting from improper implementation are easier to fix (Matthew 2004). Recently ICS-CERT has provided an update for the incident reported by Adam Crain and Chris Sistrunk for DNP3 stack vulnerabilities using test tool AEGIS in power industry equipment (Advisory (ICSA-13-291-01B) 2018). Vulnerabilities which were present in SCADA MTU server station rather than just in SCADA slave devices was the most alarming part about this disclosure. There are chances to knock the station down in case of an attack on slave devices, however, to knock the entire system offline due to an attack is impractical (Byres 2013). As per researchers, this vulnerability was present due to improper input invalidation during the implementation of third-party components in software products. These vulnerabilities exposed the network remotely as well as locally over an IP-based or serial-based implementation. This will bring greater awareness to developers and consumers of third-party components for extenuation resolution (Fabro et al. 2016).

Also, it is equally important to define precise rules for SCADA communication protocols. However, the rules and requirements are varied significantly according to business needs and the network architecture of the organization. Moreover, the configuration of a firewall according to business needs is the primary focus of any organization - "allow the traffic which is absolutely required for business". In such cases, many organizations consider allowing SQL traffic as required in data historian servers. Unfortunately, many SCADA communication protocols such as HTTP, OPC/DCOM, FTP, TFTP, MODBUS/TCP are vulnerable to Slammer worm which is a vector of SQL data (Stouffer et al. 2015). To strengthen the network in certain scenarios, while installing a firewall with or without DMZ for shared server, detailed attention requires to be considered. At a minimum, while installing a firewall without DMZ, the configuration rules should be defined specifically to IP addresses and port numbers. The address part of the rules is used to confine inbound packets to the data historian of the control network. In addition, configured ports should be clearly differentiated and restrict the unencrypted protocols to cross the firewall as packet sniffing and modifications are always the soft attack techniques. On the other hand, while installing a firewall with DMZ, with very few exceptions, all traffic from either the corporate side or control side should terminate at DMZ. This is a more flexible approach for inherently insecure protocols. For example, MODBUS is used to establish communication between PLC and data historian, while HTTP is used to established communication between data historian server and enterprise hosts although neither of these can cross the defined range of networks. Extension to this approach is the concept of "disjoints" protocols where certain protocols are allowed in DMZ and corporate network are explicitly restricted in DMZ and control network. This approach greatly reduced the possibility of malware attacks. For example, Slammer worm makes its own way into a control network by using two different activities over two different protocols. One of the focal points while configuring the firewall for control network is outgoing traffic should be limited to essential communication only. This will reduce the significance of unmanaged risk; as an example, Trojan horse software can exploit poorly defined outgoing traffic by HTTP tunneling. The Industrial Automation Open Networking Association (IAONA) offers an analysis of commonly found protocols in an industrial environment by considering the various factors like security risk, functionality, and impact of vulnerabilities. Readers are highly recommended to refer to the analysis report offered by IAONA while deploying rules of specific protocol (Tangermann 2006). Here, in Table 9 we have summarised some of the key issues and suggested practices for commonly used protocols in SCADA communication; Most of the key-points are taken from the two reports. One is “NIST Special Publication 800-82 Revision 2” (Stouffer et al. 2015) and another is “SCADA: issues, vulnerabilities, and future directions” (Yardley 2008). Please see Table 9 for key points from various standards and publications.

5. Standardization efforts

Worldwide, many standards bodies and government organizations have been continuously focusing on improvisation of SCADA security to ensure a robust and secure infrastructure of various industries. They have been developing several standards and best practices which deal with exploitation issues of the SCADA system. In this section, we have listed the contributions of several bodies towards SCADA security recommendations by aggregating widely accepted and most popular guidelines, standards, and best practices. To help owners, vendors, network administrators and researchers in choosing the appropriate standards which are applicable to their area, we have also classified these standards into two major categories as some of these standards address organizational aspects and/or contractual aspects which help in minimizing the damage caused by vulnerabilities, while some address technical aspects to enhance the security of SCADA system.

International Electrotechnical Commission (IEC) TC57 WG15 is designed to accomplish the development of cyber security standards for power system communication. The development includes the design of secure communication protocols standard defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870- 6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series (Cleveland 2012). Furthermore, the formation carried out

Table 9
SCADA communication protocol's vulnerabilities and recommendations (Yardley 2008; Stouffer et al. 2015).

Function	Vulnerability/Attack	Recommendation
OPC/DCOM (Dynamic TCP/UDP Port Allocation) (Byres et al. 2005; ENISA 2011; CIPC 2013)		
Uses RPC - remote procedure call for OPC.	Runtime open a wide range of ports which cannot be filtered by general firewall rules; Exploited through Blaster warm attack and other malware like Havex.	1. A protocol should only be allowed in DMZ and control network; 2. A user should restrict the port ranges using the registry modification technique on devices(Byres et al. 2005); 3. Derive content inspection technology according to the approved client request and valid packet type.
MODBUS / TCP (Port 502) (Homeland Security 2010; Chen et al. 2015; Alves et al. 2018; Li et al. 2019)		
MODBUS over TCP establish a request-response mechanism amongst Master-HMI, slave-PLC/RTU, and field devices.	Issue harmful commands to MODBUS devices identified by packet sniffer in the network; SCADA MODBUS slave replied to the illegal functions generated by remote attackers through crafted packets;	1. An extended version of MODBUS security is recommended; 2. Sanity checks should be implanted to block traffics that is not confirming with MODBUS standard(Homeland Security 2010); 3. Control engineers should explicitly define a set of allowed MODBUS commands, register values, and binary coils; 4. Generate an alert system to block and report for unspecified rules.
PROFINET (Port 135) (Samtani et al. 2016; Siemens ProductCERT 2018)		
Siemens' Ethernet communication protocol uses to exchange information between control devices and field devices.	Improper parsing of packets in Profinet - DCP (Discover & Configuration Protocol) could cause DOS; Crafted packets are used to modify device configuration through feeble device engineering mechanism.	1. Use the latest release of software controller according to the version of the processor (e.g. SIMATIC S7-1500, SIMATIC S7-400 V8.1) (Siemens ProductCERT 2018). 2. Configure network environment according to vendor-specific guidelines and product manual; 3. Apply cell protection concept using VPN between two cells;
DNP3 (Byres 2013; Darwish et al. 2015, 2016)		
The open standard protocol allows communication between the control center and field devices through TCP, UDP, HTTP etc.	Remotely expose network through TCP crafted packets due to weak IP based implementation; Locally exploit network through serial-based implementation using social engineering to put a system in an infinite loop for a forceful restart to reset the conditions.	1. Developers should rigorously test the module during quality control of the product; 2. Block the DNP3 based traffic from corporate into control networks through IPS, firewall or DMZ with DNP3 specific rules (Advisory (ICSA-13-291-01B) 2018); 3. Owners should take additional defensive actions by adopting secure methods and virtual private connections to prevent the control network from remote attackers (Byres 2013).
Ethernet/IP (TCP port - 44818 or UDP port - 2222) (Byres and Lowe 2004)		
Rockwell's Ethernet/IP Protocol is used to upload and download an application to PLC; Reading and writing register values in PLCs/ RTUs.	Allow a remote attacker to cause DOS through CIP message for modification of network and configuration parameters; Allow the number of unauthenticated commands to proceed into PLC ; Allow man-in-middle attackers to target HTTP traffic.	1. The functional code of exploitation of vulnerability owing to weakness in Ethernet/IP is available in a Metasploit framework, therefore administrators are advised to contact the vendors regarding the latest updates and releases(Konstantinos and Adrian 2013); 2. Deploy unified threat management that supports CIP packets filtering(NERC 2017); 3. Network administrators are advised to monitor the systems which belong to Ethernet/IP communication.
HTTP & HTTPS (ports 80 (HTTP) and port 443 (HTTPS)) (Matthew 2004)		
Providing service in web browsers, plant floors as well in all-purpose query tools.	HTTP packets can be sniffed; HTTP can become transmission media for many attacks and automated worms; Feeble authentication in HTTPS server due to untrusted X.509 certificate distribution.	1. Configure HTTP proxies in a firewall to filter all incoming packets and other applications from corporate to control networks if required; 2. Implement authorization service at application layer instead of network layer; 3. Log all attempts of service utility; 4. Use HTTPS web-based service for specifically authorized devices.
FTP & TFTP (port 20, 21 (FTP) and 69 (TFTP)) (Samtani et al. 2016)		
Use to transfer files amongst SCADA devices; PLCs and RTUs use FTP owing to minimum processing power.	Feeble FTP configuration carrying buffer overflows vulnerabilities; Theft of login credential; Insecure communication may cause unwanted access control of a network.	1. FTP communication should be established using token-based two-way authentications and an encrypted tunnel; 2. Whenever possible, SCP (Secure Copy protocols) should be deployed in communication link instead of TFTP communication.
TELNET (port 23) (Samtani et al. 2016)		
Remote login and text-based communication between client and SCADA host with limited resources and limited need for security.	Theft during transmission of data and login credential to gain illegal access.	1. Use SSH2 instead of TELNET for remote communication; 2. Outgoing sessions are only allowed over a secure tunnel to specific devices; 3. Inbound sessions to the control network should be prohibited in most of the cases; 4. If required establish token-based three-way handshaking.

technical reports on end-to-end security framework for the power system infrastructure. North American Electric Reliability Council (NERC) has released CIP (Critical Infrastructural Protection) guidelines which elaborate organizational risks, assessment techniques and best practices to support electricity sub-sector organizations in North America (NERC 2012). Moreover, NERC provides suggestions for effective patch management strategies for control systems by defining well-executed patch-management programs for asset owners and vendors which will help in alleviating many of the challenges from malicious intrusion to maintain product level reliability (NERC 2005). The vulnerability assessment details and recommendations about patch management are described in Section 4.1.3 in this paper were interpreted by taking few key-points from NERC guidelines of patch management. The Department of Energy (DOE) along with The President's Critical Infrastructure Protection Board, has outlined the steps of SCADA security improvement for industrial infrastructure. These steps don't provide all-inclusive SCADA security solutions, however, address necessary key-points to improve the protection of SCADA system. The key-points are categorized into two major categories – implementation improvements and underlying management policies and procedures (Department of Energy 2011). Section 4.3.3 refers key-points of the DOE guidelines to illustrate recommendations for audits & accountability of secure control network. The American Gas Association (AGA) has released consecutive four standards based on "Cryptographic Protection of SCADA Communications". The goal of these documents is to provide guidelines on effective implementation of cryptographic functions to strengthen SCADA components and communication channels (AGA 2006). Section 4.2.3 follows AGA standards to represents effective strategies for a cryptographic function. Furthermore, the American Petroleum Institute (API) has developed industry-specific standard – 1164, "Pipeline SCADA Security" which provides security guidelines to pipeline operators on resource-constrained environment (API 2009). Critical Infrastructure Security Working Group (CISSWG) has briefly summarized control system security standards for energy sectors in the National SCADA Test Bed (NSTB). The report documented the state of the information with regards to contribution of various standards towards cyber security enhancement by measuring the structural effectiveness in terms of security policy, vulnerability and risk assessment, business continuity management, cryptographic system test plan, compliance, etc. in the energy sector (Carlson et al. 2005).

The National Institute of Standard and Technology (NIST) published a report on System Protection Profile in 2004 which not only covers the objective of risk assessment but also provides an extension to existing ISO standard (Evans et al. 2004). Also, a special publication SP 800-82 Guide by NIST, focuses on SCADA vulnerability analysis and assessment which comprises various techniques from the primary port scanning to those includes vulnerability exploitation through the actual attack. In its entirety, NIST covers all the technical, management and organizational aspects of security controls through various guidelines and standards (Kent and Souppaya 2006; Stouffer et al. 2006; Grassi James L Fenton Privacy Authors et al. 2017). We have followed mostly all the reports of NIST guidelines to incorporate vulnerability recommendations cited in Section 4. Furthermore, technical aspects (implementation/configuration flaws) of SCADA systems were evaluated and assessment techniques were incorporated using guidelines of the US Department of Homeland Security (DHS) in Section 4. DHS published various guidelines on the security assessment of control network which are based on analysis of securing controls by determining the correctness of the implementation, operating envisioned, and producing desired outcome by fulfilling the security requirements (DHS 2009). Furthermore, the seven best practices were presented which help the security practitioner in the implementation of countermeasures for common exploitable weaknesses in control systems. This includes the following: 1. Application Whitelisting (AWL) – use to detect and prevent attempted execution of malware adversaries on HMI and control servers; 2. Device configurations and patch management; 3. Reduction of attack surface area by proper isolation techniques; 4. Segmentation and defendable network environment; 5. Manage authentication; 6. Implementation of secure remote access; 7. Monitoring and executing prepared response for adversarial penetration (DHS-NCCIC 2015). In the UK, the Centre for the Protection of National Infrastructure (CPNI) is known as a hub of best practice guidance which ensures the security of SCADA system. The CPNI provides nine best practice guideline documents for the SCADA system which cover a wide range of issues from configuring proper deployment of firewall to manage third party risk (CPNI 2011). The guidelines emphasize high level of management aspects rather than focusing more on technical details. We have followed CPNI best practices to enhance Section 4.2.5 – Inadequate policies & procedures. Furthermore, The European Union Agency for Network and Information Security (ENISA) has released standard reports on protection of Industrial Control System (ICS) for the Europe and member states, which reveals critical security issues and testing recommendations through common testbed practices. For greater details on each organizational standards, readers can also review special publication "Standards on cyber security assessment of smart grid" (Leszczyna 2018). This special edition presents a systematic analysis of security issues identified by standards and their corresponding security assessment guidance. Please see Table 10 for references to each of the standardization efforts.

6. Internet of Things (IoT) security considerations for SCADA networks

We are currently witnessing a surge in the deployment of Internet of Things (IoT) in critical industrial infrastructures and hence it becomes important to consider the impact of security on SCADA environments. In this section, we highlight the key research challenges and some of the proposed solutions and recommendations for securing IoT-based SCADA systems.

IoT refers to a collection of autonomous, smart, connected, and uniquely identifiable objects with embedded processors that have sensing, computing and communicating capabilities. Such smart objects are equipped with microcontrollers for processing, transceivers for digital communication, and a full protocol stack for inter-object and user-object communication (Lin et al. 2017; Qiu et al. 2018). The Industrial Internet Consortium (IIC 2019) and the Reference Architectural Model for Industry 4.0 (RAMI 4.0) have recognized IoT as an integral part of critical industry infrastructure and their seamless integration with SCADA devices.

The importance of security in Internet of Things for industrial applications has been highlighted in the research work by Lin et al. (2017), Choo et al. (2018), Shaikh et al. (2018). This design challenge stems from a number of factors. Firstly, a characteristic of IoT devices is their severe resource constraint, since they mainly consist of small sensors with limited computational power and bandwidth. This makes the deployment of sophisticated encryption and reliability algorithms infeasible. Secondly, IoT devices have limited intrusion detection capability, making them highly susceptible to being used as bots. The recent Denial of Service attack on IoT devices with the Mirai malware highlighted the vulnerability of the technology and the urgent need to mitigate such attacks (Kolias et al. 2017). Thirdly, although IoT does include wired counterparts, it is largely characterized by heterogeneous mobile objects integrating wireless technologies such as radio frequency identification, mobile cloud computing, wireless sensor, Bluetooth, WiFi

Table 10
Organizations involved in SCADA security improvisation.

Organization	Standardization efforts	Type	Classification of Standards
Electric Power			
International Electrotechnical Commission (IEC)	IEC 62351, IEC TC57 WG15: "Data and Communication Security, Security Standards for the Power System Information Infrastructure" (Cleveland 2012)	Standard	Technical aspects
North American Electric Reliability Council (NERC)	"Security Management in the North American Electricity Sub-Sector A Guideline" (NERC 2016)	Guideline	Organizational aspects
	"Security Guideline for the Electricity Sub-sector: Physical Security Response" (NERC 2012)	Guideline	Organizational aspects
	"Security Guidelines for the Electricity Sector: Patch Management for Control Systems (NERC 2005)	Guideline	Contractual (vendor specific), Technical aspects
	"NERC 1300 - Cyber Security, "CIP standards CIP-001 through CIP-014" (NERC 2017)	Standard	Technical aspects
Department of Energy (DOE)	"21 Steps to Improve Cyber Security of SCADA Networks" (Department of Energy 2011)	Best Practice	Organizational/Management aspects
Critical Infrastructure Security Working Group (CISSWG)	"National SCADA Test Bed - "A Summary of Control System Security Standards Activities in the Energy Sector" (Carlson et al. 2005)	Guideline	Organization aspects
Oil and Gas			
American Petroleum Institute (API)	"API Std 1164 - Pipeline SCADA Security, Second Edition" (API 2009)	Standard	Organizational aspects
	"Security Guidelines for the Petroleum Industry" (API 2005)	Guideline	Organizational aspects
	"Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries" (API 2003)	Guidelines	Organizational aspects
American Gas Association (AGA)	"AGA Report No. 12 Part 1 – "Cryptographic Protection of SCADA Communications Background, Policies & Test Plan"(AGA 2006)	Guideline	Organizational aspects (compliance and policy management)
	"AGA Report No. 12 Part 2 – "Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications" (Hadley and Huston 2006)	Guideline	Technical aspects (communication channel security enhancement)
	"AGA Report No. 12 Part 3 – "Cryptographic Protection of SCADA Communications: Protection of Networked Systems"	Guideline	Technical aspects (network security)
	"AGA Report No. 12 Part 4 – "Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components"	Guideline	Technical aspects (device level security)
Cross-Cut Organizations			
Centre for the Protection of National Infrastructure (CPNI)	Good Practice Guides(CPNI 2011) "Process control and SCADA security -General Guidance" "guide 1 - Understand the Business Risk" "guide 2 - Implement Secure Architecture" "guide 3 - Establish Response Capabilities" "guide 4 - Improve Awareness and Skills" "guide 5 - Manage Third Party Risk" "guide 6 - Engage Projects" "guide 7 - Establish Ongoing Governance" "Firewall Deployment for SCADA and process control networks good practice guide"(NISCC and CPNI 2005)	Best Practices	Organizational, Contractual aspects (Management & Risk assessment)
Department of Homeland Security (DHS)	"Primer Control Systems Cyber Security Framework and Technical Metrics"(Homeland Security 2009)	Guideline	Technical aspects
	"Department of Homeland Security: Cyber Security Procurement Language for Control Systems"(DHS 2009)	Guideline	Technical aspects
	"Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" (Fabro et al. 2016)	Best Practice	Technical aspects (network level)
	"Configuring and Managing Remote Access for Industrial Control Systems"(Homeland Security 2010)	Guideline	Organizational, Technical aspects
	"Seven Steps to Effectively Defend Industrial Control Systems"(DHS-NCCIC 2015)	Best Practice	Technical aspects
	"Recommended Practice for Patch Management of Control Systems"(DHS and CSSP 2008)	Best Practice	Organizational, Contractual (vendor specific) aspects
National Institute of Standards and Technology (NIST)	"Security Capabilities Profile for Industrial Control Systems" (Stouffer et al. 2004) "System Protection Profile for Industrial Control Systems (SPP-ICS)" (Evans et al. 2004) "Guide to SCADA and Industrial Control Systems Security"(Stouffer et al. 2006) "NIST Special Publication 800-70, Revision 4, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers" (Quinn et al. 2009) "SP800-82 Guide for SCADA and ICS Security"(Stouffer et al. 2015) "A cyber security Testbed for Industrial Control System" (Candell et al. 2014)	Guidelines	Organizational, Technical, Contractual aspects

(*continued on next page*)

Table 10 (*continued*)

Organization	Standardization efforts	Type	Classification of Standards
American National Standards Institute (ANSI)	"ISA99.00.01 – Part 1: Terminology, Concepts and Models" (ISA 2007) "ISA99.00.02 – Part 2: Establishing an Industrial Automation and Control System Security Program" (ISA 2007) "ISA99.00.03 – Part 3: Operating an Industrial Automation and Control System Security Program" (ANSI/ISA 2007)	Standards	Organizational aspects
European Union Agency for Network and Information Security (ENISA)	ERNCIP - "European Reference Network for Critical Infrastructure Protection Handbook 2018 edition"(Giannopoulos 2018) "Good Practices for an EU ICS Testing Coordination Capability" (Konstantinos and Adrian 2013) "Methodologies for the identification of Critical Information Infrastructure assets and services"(Mattioli and Levy-Bencheton 2014) "Protecting Industrial Control Systems Annex I to Annex VI" (ENISA 2011) "Window of exposure - a real problem for SCADA systems? Recommendations for Europe on SCADA patching" (Pauna and Moulinos 2013)	Guidelines	Organizational, Technical, Contractual aspects

and cellular, each with its own set of security constraints and vulnerabilities.

The Internet Engineering Task Force (Kumar and Sethi Ericsson 2019) has recently released its RFC 8576 that identifies the vulnerabilities of IoT. In particular, the RFC identifies vulnerable software, privacy breaches, object cloning, malicious substitution, eavesdropping, man-in-the-middle, routing attacks, denial of service and firmware attacks as the main threats for IoT based systems.

In terms of solutions for securing IoT based SCADA systems, (Sajid et al. 2016) provide an excellent review of the security challenges for cloud-assisted IoT-based SCADA systems. They make the following ten recommendations and best practices for securing such systems: Network segregation, Log analysis, Network traffic analysis, Malicious activity detection, Vulnerability testing, Continuous monitoring and analysis, File integrity monitoring, Memory dump analysis, Continuous updating and patching, and Proxy solutions (Sajid et al. 2016). The Industrial Internet Consortium has proposed a data driven security monitoring and analysis model (IIC 2019). Roukounaki et al. (2019) propose a Secure IoT architecture that can be integrated with SCADA systems. It is based on a "Monitor-Analyze-Act" cycle and consists of five layers, namely, IoT systems, data collection and actuation, security intelligence, security services and security use cases.

7. Conclusion

The safeguarding of a Nation's critical infrastructures is one of critical importance when ensuring public confidence and for affluence, security, and welfare of any Nation. However, as the vulnerability landscape of SCADA systems continuously grows the probability of attack, and the severity of consequences may lead to major disasters such as critical system failure. By taking precautionary steps, an organization can standardize and implement secure control systems and their underlying architecture. To drive the automation and processes securely in the organization, periodic audits of both risk and vulnerability assessments are required. We have addressed various vulnerabilities and threats, to bring awareness to asset-owners and vendors regarding potential weaknesses and the targeted areas of a SCADA system. We have also outlined high-level discoveries and mitigation recommendations within this paper. However, the all-inclusive focus of an assessment is dependent on the overall framework, design, and scope of the organization. We have summarized several standards and best practices by standard-bodies and government organizations to strengthen the SCADA system architecture. Nevertheless, upcoming standards still require advanced recommendations, administrative policies, and procedures for a security mechanism that addresses the shortcomings of a current SCADA system used in grid and IoT based architectures. Also, the release of incidents related information in various vulnerability databases is frequently observed as a security risk. With this in mind, it is important that automated industries perceive from SCADA security catastrophes in order to assure that industrial infrastructure is robust against international cyber attacks.

Declaration of Competing Interest

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

Acknowledgment

The authors thank the anonymous reviewers and the Editor for their valuable comments and suggestions that have improved the quality of the paper. The authors gratefully acknowledge the support in part by the Natural Sciences and Engineering Research Council (NSERC) and industry partners Cistel Technology Inc. and Technologies Sanstream, through a Collaborative Research Grant.

References

Advisory (ICSA-13-291-01B), 2018. DNP3 Implementation Vulnerability (Update B) | ICS-CERT. Adv. Database. [cited 2018 Nov 21]. Available from: https://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B .

AGA, 2006. AGA Report Number 12, Cryptographic Protection of SCADA Communications Part 1:"Background, Policies and Test Plan". Am. Gas. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Cryptographic+Protection+of+SCADA+Communications+Part+1#1.

Alves, T, Das, R, Morris, T, 2018. Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. IEEE Embedded Syst. Lett. 10 (3), 99–102.

Alves, T, Morris, T., 2018. OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research. Comput. Secur. 78, 364–379. Available from: https://doi.org/10.1016/j.cose.2018.07.007.

ANSI/ISA T 00. 0. S. Security Technology for Manufacturing and Control Systems United States of America; 2007.

API, 2003. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries WashingtonAvailable from: https://www.nrc.gov/docs/ML0502/ML050260624.pdf.

API, 2005. Security Guidelines for the Petroleum Industry Available from: www.dhs.gov.

API, 2009. API Std 1164 Pipeline SCADA Security [cited 2018 Nov 9]. Available from http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/API-1164-PipelineSCADASecurity2nded.pdf.

Baily, M, Cooke, E., 2005. The Blaster Worm: Then and Now. IEEE Secur. Privacy 26–31. Available from: http://nsrg.ece.illinois.edu/publications/IEEE_Security_Privacy_Blaster_Final.pdf.

Blau, J., 2004. The Battle Against Cyberterror | Network World [cited 2018 Oct 8]. https://www.networkworld.com/article/2327822/lan-wan/the-battle-against-cyberterror.html.

Byres, E., 2013. DNP3 Vulnerabilities Part 1 of 2 - NERC's Electronic Security Perimeter is Swiss Cheese | Tofino Industrial Security Solution [cited 2018 Nov 17]. Available from: https://www.tofinosecurity.com/blog/dnp3-vulnerabilities-part-1-2-nercs-electronic-security-perimeter-swiss-cheese.

Byres, E, Karsch, J, Carter, J, 2005. Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide. Centre for the Protection of National Infrastructure (CPNI).

Byres, E, Lowe, J., 2004. The myths and facts behind cyber security risks for industrial control systems. In: Proceedings of the VDE Kongress.

Cai, N, Wang, J, Yu, X, 2008. SCADA system security: Complexity, history and new developments. In: Proceedings of the 6th IEEE International Conference on Industrial Informatics. IEEE, pp. 569–574.

Candell R, Anand DM, Stouffer K. A Cybersecurity Testbed for Industrial Control Systems. In: ISA, editor. Texas; 2014 [cited 2018 Sep 11]. Available from: http://www.isa.org

Carlson RE, Dagle JE, Shamsuddin SA, Evans. RP. A Summary of Control System Security Standards Activities in the Energy Sector Enhancing control systems security in the energy sector NSTB. U.S.; 2005. Available from: https://www.energy.gov/sites/prod/files/SummaryofCSStandardsActivitiesintheEnergySector.pdf

Chaffin, M, Nelson, T., 2011. Common Cybersecurity Vulnerabilities in Industrial Control Systems. DHS.

Chen, B, Pattanaik, N, Goulart, A, Butler-Purry, KL, Kundur, D, 2015. Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. In: Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability, pp. 1–6.

Cherdantseva, Y, Burnap, P, Blyth, A, Eden, P, Jones, K, Soulsby, H, et al., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27. Available from: http://www.sciencedirect.com/science/article/pii/S0167404815001388.

Choo, K-KR, Gritzalis, S, Park, JH, 2018. Cryptographic solutions for industrial Internet-of-Things: research challenges and opportunities. IEEE Trans. Ind. Informat. 14 (8), 3567–3569.

CIPC. Security Guideline for the Electricity Sub-sector: Physical Security Response. 2013. Available from: http://www.esisac.com/.

Cleveland F. IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure. 2012. Available from: http://iectc57.ucaiug.org/wg15public/PublicDocuments/WhitePaperonSecurityStandardsinIECTC57.pdf.

Common Vulnerabilities Exposures Database. CVE - Home. Web Database. [cited 2018 Oct 2]. Available from: https://cve.mitre.org/cve/.

Common Weakness Enumeration Database. CWE - Common Weakness Enumeration. Web Database. [cited 2018 Aug 30]. Available from: https://cwe.mitre.org/index.html.

CPNI. Centre for the protection of national infrastructure. 2011. Available from: https://web.archive.org/web/20130620125607/http://www.cpni.gov.uk/advice/cyber/scada/#.

Darwish, I, Igbe, O, Celebi, O, Saadawi, T, Soryal, J, 2016. Smart Grid DNP3 Vulnerability Analysis and Experimentation. In: Proceedings of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015, pp. 141–147.

Darwish, I, Igbe, O, Saadawi, T, 2015. Experimental and theoretical modeling of DNP3 attacks in smart grids. In: Proceedings of the 36th IEEE Sarnoff Symposium, pp. 155–160.

Department of Energy, 2008. Enhancing control systems security in the energy sector NSTB National SCADA Test Bed Common Cyber Security Vulnerabilities Observed in Control System Assessments. INL NSTB Program. U.S. Available from: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/31-INL_Common_Vulnerabilities_Report.pdf.

Department of Energy. 21 steps to improve cyber security of SCADA Networks. 2011.

DHS-NCCIC. Seven steps to effectively defend industrial control systems. 2015;1–7. Available from: https://ics-cert.us-cert.gov/sites/default/files/documents/SevenStepstoEffectivelyDefendIndustrialControlSystems_S508C.pdf.

DHS. Department of homeland security: cyber security procurement language for control systems. U.S.; 2009.

DHS, CSSP. Recommended practice for patch management of control systems recommended practice for patch management of control systems DHS national cyber security division control systems security program acknowledgement. 2008. Available from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf.

Eckstein C. Validating security configurations and detecting backdoors in new network devices. 2014. Available from: https://www.sans.org/reading-room/whitepapers/networkdevs/validating-security-configurations-detecting-backdoors-network-devices-35472.

ENISA. Protecting industrial control systems. 2011. Available from: https://www.enisa.europa.eu/publications/annex-ii/at_download/fullReport.

Evans DL, Bond PJ, Bement AL. System protection profile-industrial control systems version 1.0. 2004. Available from: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=822602.

Fabro M, Gorski E, Spiers N. Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies industrial control systems cyber emergency response team. 2016. Available from: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

FERC-NERC. FERC, NERC issue report on grid restoration, recovery plans absent SCADA, EMS. 2017 [cited 2019 Oct 17]. Available from: https://www.nerc.com/news/Pages/FERC,-NERC-Issue-Followup-Report-to-Grid-Restoration,-Recovery-Plans-Absent-SCADA,-EMS.aspx.

Forner E, Meixel B. Out of control: Demonstrating SCADA device exploitation - YouTube Black Hat 2013. USA; 2013 [cited 2018 Oct 23]. Available from: https://www.youtube.com/watch?v=FTzAkEnwx_c.

Giannopoulos, G., 2018. European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 Edition. Available from: https://ec.europa.eu/jrc.

Grassi P, Garcia M, Fenton J. Digital Identity Guidelines. NIST Special Publication 800-63-3. 2017 [cited 2018 Sep 23]. Available from: https://openid-foundation-japan.github.io/800-63-3/sp800-63-3.html.

Grother P, Salamon W. NIST Special Publication 800-76-2, biometric specifications for personal identity verification. 2013.

Hadley M, Huston K. AGA 12, Part 2 Performance Test Plan. 2006. Available from: http://cipbook.infracritical.com/book3/chapter8/ch8ref4.pdf.

Hildick-Smith A. Security for critical infrastructure scada systems. SANS Reading Room, GSEC Practical Assignment, Version. 2005;1:498–506.

Holloway M. Slammer Worm and David-Besse Nuclear Plant. coursework for PH241, Stanford University. 2015 [cited 2019 Jan 7]. Available from: http://large.stanford.edu/courses/2015/ph241/holloway2/.

Homeland Security. Primer control systems cyber security framework and technical metrics. 2009;(June):1–30. Available from: https://ics-cert.us-cert.gov/sites/default/files/documents/Metrics_Primer_7-13-09_FINAL.pdf.

Homeland Security. Configuring and Managing Remote Access for Industrial Control Systems - CPNI Centre for the Protection of National Infrastructure. 2010;(November):1–66.

Homeland Security. NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team. 2015. Available from: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY2015_Annual_Vulnerability_Coordination_Report_S508C.pdf.

Igure, VM, Laughter, SA, Williams, RD, 2006. Security issues in SCADA networks. Comput. Secur. 25 (7), 498–506.

IIC. Industrial Internet Consortium. 2019 [cited 2019 Aug 4]. Available from: https://www.iiconsortium.org/.

INFOSEC. How to prevent cross-site scripting attacks. [cited 2019 Aug 5]. Available from: https://resources.infosecinstitute.com/how-to-prevent-cross-site-scripting-attacks/#gref.

INL. NSTB assessments summary report: common industrial control system cyber security weaknesses. 2010.

ISA, 2007. Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models Draft 5. In: Proceedings of the International Society for Automation. Durham.

Kent K, Souppaya MP. Guide to computer security log management. Gaithersburg, MD; 2006. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

Kesler B. The Vulnerability of Nuclear Facilities to Cyber Attack. Strategic Insights, Spring 2011. 2011 [cited 2018 Oct 15];10(1):15–25. Available from: http://www.wired.com/threatlevel/2011/02/hoover/.

Knapp, E, 2011. Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier - Syngress.

Kolias, C, Kambourakis, G, Stavrou, A, Voas, J, 2017. DDoS in the IoT: Mirai and other botnets. Computer 50 (7), 80–84.

Konstantinos, M, Adrian, P., 2013. Good Practices for an EU ICS Testing Coordination Capability. (ENISA), European Union Agency for Network and Information Security.

Kumar S, Sethi Ericsson M. Internet Research Task Force (IRTF) O. Garcia-Morchon Request for Comments: 8576 Philips Category: Informational. 2019 [cited 2019 Aug 4]; Available from: https://trustee.ietf.org/license-info.

Leszczyna, R., 2018. Standards on cyber security assessment of smart grid. Int. J. Crit. Infrastruct. Protect. 22, 70–89.

Li, D, Guo, H, Zhou, J, Zhou, L, Wong, JW, 2019. SCADAWall: A CPI-enabled firewall model for SCADA security. Comput. Secur 80, 134–154. Available from: https://doi.org/10.1016/j.cose.2018.10.002.

Lin, J, Yu, W, Zhang, N, Yang, X, Zhang, H, Zhao, W, 2017. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J. 4 (5), 1125–1142.

Mackenzie H. SCADA Security Basics: Why Industrial Networks are Different than IT Networks | Tofino Industrial Security Solution. 2012 [cited 2018 Sep 5]. Available from: https://www.tofinosecurity.com/blog/scada-security-basics-why-industrial-networks-are-different-it-networks.

Matthew, F, 2004. Protocol Implementation Testing: Challenges and Opportunities. National Infrastructure Security Co-ordination Center (NISCC) workshop.

Mattioli, R, Levy-Bencheton, DC., 2014. Methodologies for the Identification of Critical Information Infrastructure Assets and Services. ENISA - European Union Agency for Network and Information Security, Europe.

National Vulnerability Database. NVD - Home. Web Database. [cited 2018 Sep 5]. Available from: https://nvd.nist.gov/.

Nazir, S, Patel, S, Patel, D, 2017. Assessing and augmenting SCADA cyber security: a survey of techniques. Comput. Secur. 70, 436–454. Available from: https://doi.org/10.1016/j.cose.2017.06.010.

NCCIC, 2016. ICS-CERT Annual Vulnerability Coordination Report 2016 I ICS-CERT Annual Vulnerability Coordination Report Available from: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf.

NERC. Security guidelines for the electricity sector: patch management for control systems NERC guideline guideline title: patch management for control systems. 2005. Available from: https://www.controlglobal.com/assets/Media/MediaManager/wp_037_nerc_secguide.pdf.

NERC, 2011. Proceedings of the Workshop Focuses on SCADA Successes and Challenges. [cited 2019 Oct 16]. Available from: https://www.nerc.com/news/Pages/Workshop-Focuses-on-SCADA-Successes-and-Challenges.aspx.

NERC. Security guideline for the electricity sector: physical security. 2012. Available from: https://www.nerc.com/comm/CIPC/SecurityGuidelinesDL/PhysicalSecurityGuideline2012-05-18-Final.pdf

NERC. Security management in the North American electricity sub-sector a guideline. 2016. Available from: https://www.mro.net/MRODocuments/SecurityManagementintheElectricitySub-SectorVersion1.1September2016.pdf.

NERC. CIP standards. 2017 [cited 2018 Dec 7]. Available from: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Nicholson, A, Webber, S, Dyer, S, Patel, T, Janicke, H, 2012. SCADA security in the light of cyber-warfare. Comput. Secur. 31 (4), 418–436.

NISCC, CPNI. Firewall Deployment for Scada and Process Control Networks. 2005.

Office of Electricity. National SCADA Test Bed | Department of Energy. 2003 [cited 2018 Aug 8]. Available from: https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

Oliveira F. Full Disclosure: Rapid Scada - 5.5.0 - Insecure Permissions. 2018 [cited 2018 Oct 23]. Available from: https://seclists.org/fulldisclosure/2018/Mar/11.

Pauna, A, Moulinos, K., 2013. Window Exposure - A Real Problem for SCADA Systems? Recommendations for Europe on SCADA patching. European Union Agency for Network and Information Security.

Qiu, T, Chen, N, Li, K, Atiquzzaman, M, Zhao, W, 2018. How can heterogeneous Internet of Things build our future: a survey. IEEE Commun. Surv. Tutor. 20 (3), 2011–2027.

Quinn, SD, Souppaya, M, Cook, M, Scarfone, K, 2009. National Checklist Program for IT Products—Guidelines for Checklist Users and Developers. NIST Special Publication.

RAMI 4.0. The Internet of Things and Services Graphics © Bosch Rexroth AG. Available from: https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf.

Ranathunga, D, Roughan, M, Nguyen, H, Kernick, P, Falkner, N, 2016. Case studies of SCADA firewall configurations and the implications for best practices. IEEE Trans. Netw. Serv. Manag. 13 (4), 871–884.

Rao, S, R, K, Ganga Prasad, G.L.BBS, 2017. Impact analysis of attacks using agent-based SCADA Testbed. Springer, Singapore Lecture No.

Roukounaki, A, Efremidis, S, Soldatos, J, Neises, J, Walloschke, T, Kefalakis, N, 2019. Scalable and configurable end-to-end collection and analysis of IoT security data: towards End-to-End Security in IoT systems. In: Proceedings of the Global IoT Summit (GIoTS). IEEE, pp. 1–6.

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

Samtani, S, Yu, S, Zhu, H, Patton, M, Chen, H, 2016. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. In: Proceedings of the IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data. ISI 2016.

Sauter, T, Schwaiger, C., 2002. Achievement of secure Internet access to fieldbus systems. Microprocess. Microsyst. 26, 331–339.

SCADA Vulnerabilities and Exposures Database. Critifence® SCADA Vulnerabilities and Exposures Database (SVE). Web Database. [cited 2018 Sep 13]. Available from: http://www.critifence.com/sve/.

SDP Database. CRITIFENCE®. Web Database. [cited 2018 Nov 7]. Available from: http://www.critifence.com/default-password-database/.

SecureAuth Labs. Exploits. Web Database. [cited 2018 Sep 30]. Available from: https://www.secureauth.com/labs/exploits.

SecurityFocus. Advantech WebAccess ICSA-18-135-01 Multiple Security Vulnerabilities. 2018 [cited 2018 Oct 29]. Available from: https://www.securityfocus.com/bid/104190/info.

Shaikh, F, Bou-Harb, E, Neshenko, N, Wright, AP, Ghani, N, 2018. Internet of malicious things: correlating active and passive measurements for inferring and characterizing internet-scale unsolicited IoT devices. IEEE Commun. Mag. 56 (9), 170–177.

Siemens ProductCERT. SSA-592007:Denial-of-service vulnerability in industrial products. 2018. Available from: https://www.first.org/cvss/.

Stouffer K, Falco J, Kent K. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security recommendations of the national institute of standards and technology. Gaithersburg; 2006. Available from: https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf.

Stouffer K, Falco J, Proctor F. The NIST process control security requirements forum (PCSRF) and the future of industrial control system security. Atlanta; 2004. Available from: http://cipbook.infracritical.com/book3/chapter8/ch8ref8.pdf.

Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A. NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic. 2015. Available from: http://dx.doi.org/10.6028/NIST.SP.800-82r2.

Tangermann M. The IAONA Handbook for Network Security. Magdeburg; 2006. Available from: http://www.ininet.ch/vpi-initiative/download/IAONA-Security-Guide-15-draft.pdf.

TechNavio. Global SCADA Market 2017-2021 - Research and Markets. 2017 [cited 2018 Sep 4]. Available from: https://www.researchandmarkets.com/research/3n9d25/global_scada.

Yardley T. SCADA: issues, vulnerabilities, and future directions. 2008. Available from: https://www.usenix.org/system/files/login/articles/258-yardley.pdf.

Darshana Upadhyay is currently a Ph.D. student in the Faculty of Computer Science at Dalhousie University. She holds a Masters degree in Computer Science from Nirma University, Ahmedabad, India, where she also served as a lecturer before moving to Canada to pursue her PhD degree. Darshana's research is in the areas of security protocols, embedded systems, hardware design, algorithm conceptualization. For her Masters thesis, she has completed an novel project in the area of linear feedback shift register design for secure systems. She is the co-recipient of the Indo-Shastri research grant in the area of wireless security and intrusion detection systems.

Srinivas Sampalli holds a Bachelor of Engineering degree from Bangalore University and a Ph.D. degree from the Indian Institute of Science (IISc.), Bangalore, India, and is currently a Professor and 3M National Teaching Fellow in the Faculty of Computer Science, Dalhousie University. He has led numerous industry-driven research projects on Internet of Things, wireless security, vulnerability analysis, intrusion detection and prevention, and applications of emerging wireless technologies in healthcare. He currently supervises 5 Ph.D. and 10 Masters students in his EMerging WIreless Technologies (MYTech) lab and has supervised nearly 150 graduate students in his career. Dr. Sampalli's primary joy is in inspiring and motivating students with his enthusiastic teaching. Dr. Sampalli has received the Dalhousie Faculty of Science Teaching Excellence award, the Dalhousie Alumni Association Teaching award, the Association of Atlantic Universities' Distinguished Teacher Award, a teaching award instituted in his name by the students within his Faculty, and the 3M National Teaching Fellowship, Canada's most prestigious teaching acknowledgement. Since September 2016, he holds the honorary position of the Vice President (Canada), of the International Federation of National Teaching Fellows (IFNTF), a consortium of national teaching award winners from around the world.