International Journal of Critical Infrastructure Protection 34 (2021) 100433

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

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

Architecture and security of SCADA systems: A review

Geeta Yadav [a,*], Kolin Paul [a,b]

[a] Khosla School of Information Technology, IIT Delhi, India
[b] Department of Computer Science, IIT Delhi, India

ARTICLE INFO

Article history:
Received 29 October 2020
Revised 8 February 2021
Accepted 28 March 2021
Available online 8 April 2021

MSC:
Research exposition (monographs survey articles)
Distributed systems

Keywords:
SCADA systems security
Critical infrastructure
Cyber-physical systems
IIoT
SCADA attacks
IDS
Testbed

ABSTRACT

Pipeline bursting, production lines shut down, frenzy traffic, trains confrontation, the nuclear reactor shut down, disrupted electric supply, interrupted oxygen supply in ICU – these catastrophic events could result because of an erroneous SCADA system/ Industrial Control System (ICS). SCADA systems have become an essential part of automated control and monitoring of Critical Infrastructures (CI). Modern SCADA systems have evolved from standalone systems into sophisticated, complex, open systems connected to the Internet. This geographically distributed modern SCADA system is more vulnerable to threats and cyber attacks than traditional SCADA. Traditional SCADA systems were less exposed to Internet threats as they operated on isolated networks. Over the years, an increase in the number of cyber-attacks against the SCADA systems seeks security researchers' attention towards their security. In this review paper, we first review the SCADA system architectures and comparative analysis of proposed/implemented communication protocols, followed by attacks on such systems to understand and highlight the evolving security needs for SCADA systems. A short investigation of the current state of intrusion detection techniques in SCADA systems is done, followed by a brief study of testbeds for SCADA systems. The cloud and Internet of things (IoT) based SCADA systems are studied by analyzing modern SCADA systems' architecture. In the end, the review paper highlights the critical research problems that need to be resolved to close the security gaps in SCADA systems.

1. Introduction

Critical Infrastructures (CI) are often described as the infrastructures which provide essential services and serves as the foundation for any nation's security, economy, and healthcare systems. Cyber-Physical Systems (CPS)/ Internet of Things (IoT) are supplementing traditional CI with data-rich operations. The list of sectors under critical infrastructure varies from country to country. It generally includes agriculture, healthcare, nuclear reactor, transportation, energy sector, civil and chemical engineering, water plants, research, etc. as depicted in Fig. 1. Supervisory Control and Data Acquisition (SCADA) systems, Industrial Control Systems (ICS), have a pivotal role in managing and controlling the CI. SCADA systems control and monitor geographically distributed assets. Historically, SCADA frameworks were limited to power transmission, gas conveyance, and water appropriation control frameworks. Advancements in technology have led to SCADA being deployed in steel-making, chemical processing industries, telecommunications, experimental, and manufacturing facilities [1]. With Industries 4.0 / Industrial Internet of Things (IIoT) evolution, modern SCADA systems have adopted CPS/ IoT, cloud technology, big data analytics, artificial intelligence, and machine learning. The integration of these technologies has significantly improved interoperability, ease the maintenance, and decreased the infrastructure cost. Therefore, modern SCADA systems are leading to a near real-time environment.

SCADA systems improve the efficiency of the ICS's operation and provide better protection to the utilized equipment. Moreover, it enhances the productivity of the personnel. SCADA frameworks give valid identification and quick alerts/ warnings to the observing stations using an attested monitoring stage, advanced communications, and state-of-the-art sensors. Traditional SCADA systems were designed to work in a standalone way and relied on air-gapped networks and proprietary protocols for securing the system. Therefore, the initial designs of SCADA never incorporated security features [2,3]. In recent years, due to the expansion of business and the need for central monitoring of distributed software, SCADA systems have evolved into sophisticated, complex open systems connected to the Internet using advanced technology. Associating SCADA system to the web has helped numerous SCADA systems to work from topographically inaccessible areas. However,

* Corresponding author.
E-mail address: anjugeeta11@gmail.com (G. Yadav).

https://doi.org/10.1016/j.ijcip.2021.100433
1874-5482/

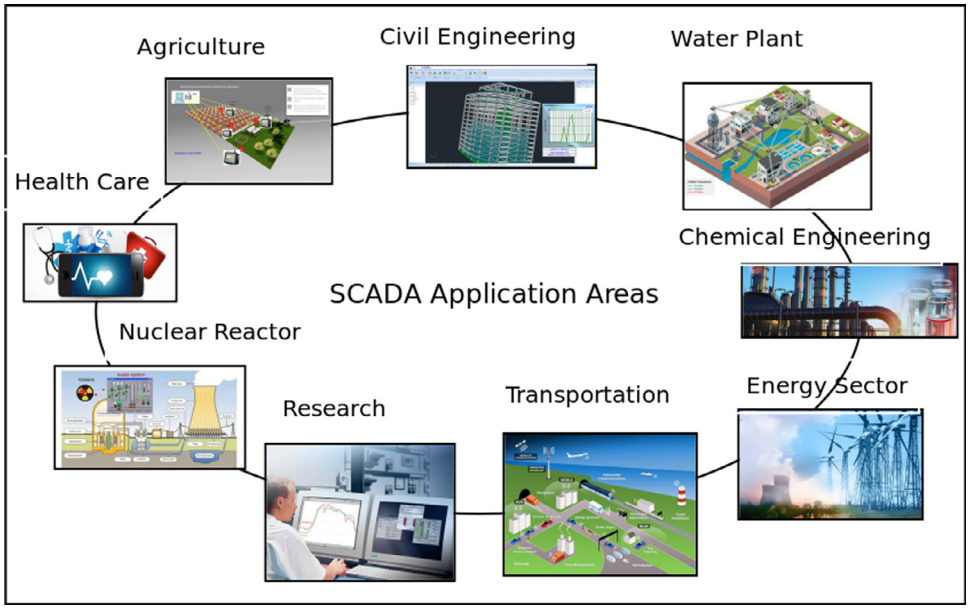

Fig. 1. SCADA Application Areas.

this has lead the SCADA system more vulnerable for attackers to target from anywhere in the world [4].

The modernization of the SCADA system, standardization of communication protocols, and growing interconnectivity have drastically increased the cyber-attacks on the SCADA system. These types of attacks are becoming more sophisticated to commit more traditional cyber espionage and sabotage in addition to cyber-crimes. The smooth and genuine operation of the SCADA framework is one of the key concerns for enterprises because the outcome of the break down of the SCADA system may range from financial loss to environmental damage to loss of human life [5]. A cyber-attack on a nuclear plant will have a global impact. Moreover, the security spillage in small networks can lead to a loss of services and financial loss to the utility company.

1.1. Scope

Several published works have reviewed SCADA systems over a period. Miller, and Rowe [4] have analyzed several cyber-security incidents targeted to CI and SCADA systems based on source sector, method of operations, target sector, and impact. Rakas et al. [149] provide an extensive study of network-based SCADA Intrusion Detection Systems. Suaboot et al. [150] survey supervised learning based intrusion detection systems for SCADA by categorizing them in nine categories, i.e., the probabilistic method, divide & conquer method, rule-based method, lazy learning method, boundary method, evolutionary method, unary classification, density-based method, ensemble-based method. Nazir et al. in [151] survey tools and techniques to identify SCADA system vulnerabilities. Qassim et al., in [133], studied SCADA testbed implementation Approaches. Guillermo et al. [152] presents an overview of wireless security and vulnerabilities of SCADA systems followed by proof-of-concept methods of attacking wireless vulnerabilities on SCADA systems.

However, all these surveys fail to connect the End-to-End (E2E) security of the SCADA system. A single dimension of SCADA systems security lacks the knowledge of the real challenges of the ICS. To overcome these shortcomings, we discuss and seek to interconnect the various aspects of SCADA systems ranging from architecture, vulnerabilities, and attacks, Intrusion Detection Systems & techniques, and the testbeds, as shown in Fig. 2. Our survey allows a more complete and holistic view of SCADA system security. We seek to answer the question "where to look for security vulnerabilities" by explaining the interconnection between SCADA architecture and communication protocols. The linking between the communication protocols and the systems' vulnerabilities helps answer "what to look for?"i.e. "what are the potential vulnerabilities, sectors, countries that are target most". Detection and Prevention of security issues can be best handled if the mutual dependencies of the protocols, existing intrusion detection, prevention mechanisms, and the vulnerabilities are considered. The lessons learned and the hardening techniques developed can only be deployed on the SCADA systems post rigorous validation using testbeds. The surveys published so far discuss and detail only one aspect of the SCADA security and thus fail to show the interconnections between various dimensions essential to design security mechanisms for the complex IIoT systems of the future. Thus, the motive of this review is to study the different aspects (Fig. 2) of SCADA security while considering their known loopholes.

1.2. Review methodology

This section describes the approach taken for selecting the various relevant papers and then classifying their work. We choose a semi-systemic literature review approach proposed in [153], as we look at the SCADA system security in a broader perspective. For identifying the related literature in the last fifteen years, the keywords searches are done on the IEEE Xplore, ACM, Elsevier, and SCOPUS, Google Scholar, which lead to excellent coverage of state-of-art publications. The keywords used are "SCADA architecture", "SCADA communication protocols", "SCADA security", "SCADA attacks", "SCADA intrusion detection systems", "SCADA testbeds", and "SCADA cloud. Then we categorized papers based on our taxonomy discussed in Section 2 manually. Next, we reviewed documents, section by section, based on examining the title, abstract, and full text in case paper provides a novel idea. We then correlated the various work done with the different SCADA security dimensions, resulting in a corresponding taxonomy. Table 1 lists all the references we cover for studying the dimensions of SCADA architecture and security.

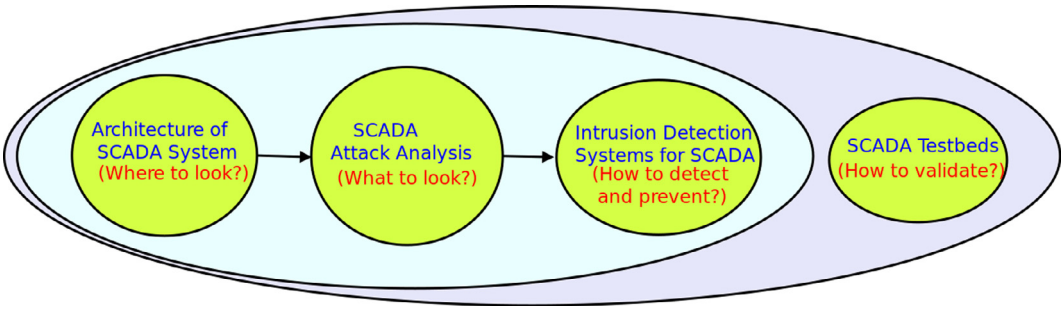

Fig. 2. Relation between different dimensions of SCADA security.

Table 1
Selected research for review.

Topic	References	Count
SCADA architecture & Communication protocol	[6–46]	41
SCADA attacks	[4,34,35,47–74]	31
SCADA IDS	[75–115]	41
SCADA Testbed	[116–133]	18
IoT-based SCADA	[55,79–81,134–148]	19

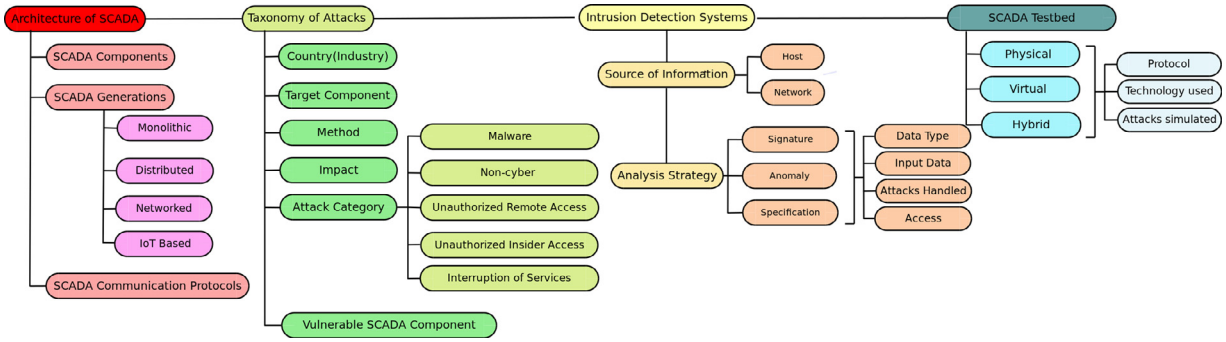

Fig. 3. Taxonomy of Research.

2. Taxonomy

We propose a taxonomy for studying architecture and the security aspect of SCADA depicted in Fig. 3. We study SCADA components, SCADA generations followed by SCADA communication protocols in Section 3 to understand SCADA architecture deeply. SCADA systems have evolved into four generations, i.e., Monolithic, Distributed, Networked, and IoT based fourth generation. Afterward, we discuss SCADA specific commonly used communication protocols considering their reference architecture, addressing, and security state, as explained in detail in Section 3.

An analysis of attacks on the SCADA system is necessary to develop technology for handling new attacks. We report some real-time SCADA attacks to demonstrate the impact of these attacks on a nation. We aim to show the urgent need for securing SCADA systems. Therefore, we have analyzed the attacks based on the country (industry) of attack, the target component, the impact of the attack, the type of attack, and vulnerable SCADA component. We have classified the attacks in four categories, i.e., Malware, Non-cyber attack, Unauthorised remote access, Interruption of services in Section 4.

IDSs are used to detect and prevent these attacks and recognizing vulnerabilities in the systems. We have categorized IDSs based on the source of information and based on the analysis strategy. The source of information can be the host or the network. The analysis strategy can be signature-based, specification-based, anomaly detection. These IDSs are studied considering the threat model, required input data, and technique considering our taxonomy,and mapping with access based classification. This analysis helps to link the security measures taken to avoid a particular attack. A detailed analysis of IDSs is done in Section 5.

Most IDS tools need to be trained and tested on a relevant and validated dataset, which will be unique for each industry and each SCADA system. To overcome the lack of validated datasets, researchers are focusing on creating testbeds for data sets. Moreover, deploying these IDSs on a running SCADA system is a challenging task as these are part of critical infrastructure which cannot bear a shutdown, delay, etc. Therefore, the testbed plays a vital role in testing each technique and its post-consequences rigorously. We have classified testbeds into four categories based on their implementation strategies, i.e., physical testbed, virtual testbed and hybrid testbed. We survey their advantages and disadvantages in Section 6. Section 7 discusses IoT-Cloud based SCADA systems. The review ends with Section 8, where we identify the future scope of research in SCADA systems.

3. SCADA system architecture

SCADA framework consists of hardware components and software programs where hardware includes a “Remote Terminal Units (RTU)”, “Master Terminal Unit (MTU)”, actuators and sensors, and software includes “Human Machine Interface (HMI)”, a central database (Historian) and other user software [16]. These software provide a communication interface between hardware and software. The physical environment is linked to the actuators and sensors, which are further connected to RTUs. RTUs gather the sen-

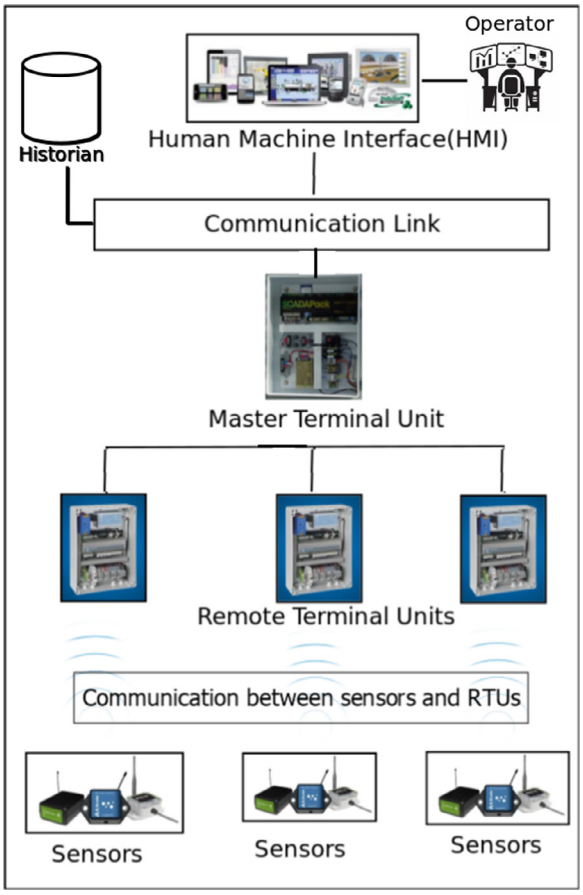

Fig. 4. Interrelation of SCADA system components.

sors' information and data and forward telemetry data to the MTU for observing and controlling the SCADA framework. We discuss this in greater detail in the next section.

3.1. SCADA components

The generic interrelation of SCADA system components MTU, RTU, HMI, Historian, and SCADA communication links is represented in Fig. 4.

RTU is responsible for collecting real-time data and information from sensors that are connected to the physical environment using link LAN/WAN. RTUs forward information to MTU. These are additionally in charge of conveying the present status data of physical devices associated with the system. Apart from RTUs, Programmable Logic Controllers (PLCs) and Intelligent Electronic Devices (IEDs) are also used to interface the sensors/ actuators through input and output modules. They act as a more modern alternative or a complement of a setup with RTUs. IEDs can control several different aspects of a piece of a sensor/actuators compared to PLC, which are developed for a specific task. IEDs are easier to configure and require less wiring as compared to traditional RTUs. Generally, IEDs have a communication port and they can communicate to a substation PLC directly or act as a gateway towards the SCADA server.

MTU is the central monitoring station. It is in charge of controlling and commanding the RTU machine over communication links. It also responds to messages from RTU and processes and stores them for succeeding communication.

HMI provides a communication interface between SCADA hardware and software components. It is responsible for controlling SCADA operational information, for example, controlling, monitoring, and communication between several RTU and MTU in the form of text, statistics, or other comprehensible content.

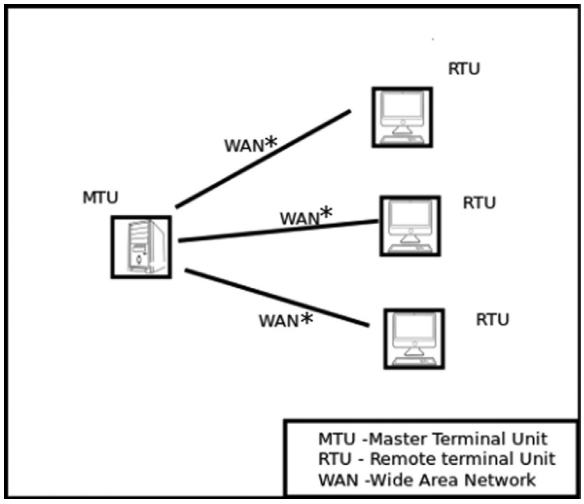

Fig. 5. Monolithic SCADA system Architecture.

Historian is used for accumulating two-way communication data, events, and alarms between the SCADA control center. It can be described as a centralized database or a server located at a distant location. Historian is queried to populate graphical trends on the HMI.

Communication network provides communication services between various components in the SCADA network framework. The medium utilized can be either wireless or wired. Presently, wireless media is generally used as it interfaces geologically circulated areas and less available zones to communicate effortlessly [6].

3.2. SCADA generations

The advancement of communication paradigm is divided into four primary ages, such as the first era: Monolithic, second era: Distributed, third era: Networked, fourth era: IoT-based SCADA.

3.2.1. Monolithic SCADA systems

It refers to those systems which work in an isolated environment and do not have any connectivity to the other systems. The motive of these systems is to work in a solitary way. Large minicomputers were used for SCADA system computing. PDP-11[1] series, which was developed by Digital Equipment Corporation, is an example of a first-generation SCADA system. In this architecture, RTUs communicate to MTU using Wide Area Networks (WAN), as shown in Fig. 5. However, the WAN protocols used at that time were completely different than the current WAN protocols. Hence we represent it with *WAN**. The *WAN** protocols used that time were in the preliminary stage. The communication protocols were proprietary, which can be used only to connect RTUs with proprietary MTU from the same vendor. These protocols were limited to permit scanning, control, and data exchange between MTU and RTUs. In the absence of network connectivity, the connection between MTU and RTUs was done at the bus level (e.g. using RS-232 communication standards) or using proprietary adapter pluging into the CPU backplane [7,40]. Connecting different vendor RTUs to MTU was an impossible task resulting in an urgent requirement for the open standards. In some cases, to provide redundancy to the SCADA system, an equally equipped sys-

[1] https://en.wikipedia.org/wiki/PDP-11 .

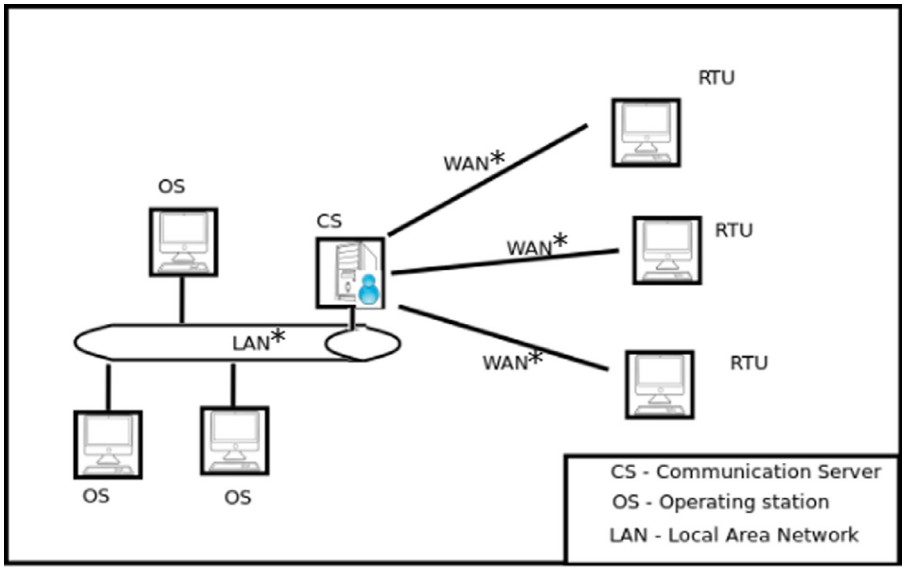

Fig. 6. Distributed SCADA system Architecture.

tem, working as a backup system was connected to the master system.

3.2.2. Distributed SCADA systems

These systems were inter-connected and confined inside small range networks like Local Area Networks (LAN), as shown in Fig. 6. However, the WAN/LAN protocols used in this generation were completely different than the current WAN/LAN protocols. Hence we represent it with *WAN**, *LAN** respectively. This generation distributes the computation overhead on multiple systems connected using *LAN**, i.e., some of the systems work as communications processors, some as operator interfaces, some as a database server, etc. [7], resulting in more processing power, redundant, and reliable system. Distributed architecture is used in the case of multiple clients and stations. The information was shared using the *LAN**. However, some of the *LAN** protocols used were proprietary nature, which again kept a restriction on the systems connected to a *LAN** to work as a distributed MTU. WAN was used to the intercommunication between RTUs and MTU. The *LAN** protocols have a range limited to the local environment. The total cable length limit between systems on the network was limited to 600 feet, limiting multiple system connections in a room itself [40]. Similar to the monolithic SCADA, distributed SCADA systems were also confined to proprietary hardware, software, network protocols, and peripheral devices supplied by the vendor [154,155]. All the devices that are connected to SCADA *LAN** were unable to communicate with external devices using other communication protocols. Their communication was restricted to proprietary protocols supplied by vendors. In shorts, disrtibuted SCADA systems were more open at MTU but still lack the capabilitiies at the RTU [41]. The security of SCADA systems was not of concern in this generation also.

3.2.3. Networked SCADA systems

It utilizes networks and the web broadly because of the standardization and cost-effective solutions for large-scale systems. This is also referred to as a modern SCADA system [6]. In this design, SCADA systems may be geographically distributed. However, Networked SCADA is closely related to Distributed SCADA, with a significant difference in the usage of open protocols and standards for communication rather than proprietary protocols resulting in distributing MTU functionality across a WAN shown in Fig. 7. Due to the use of open standards, third-party peripheral devices can be

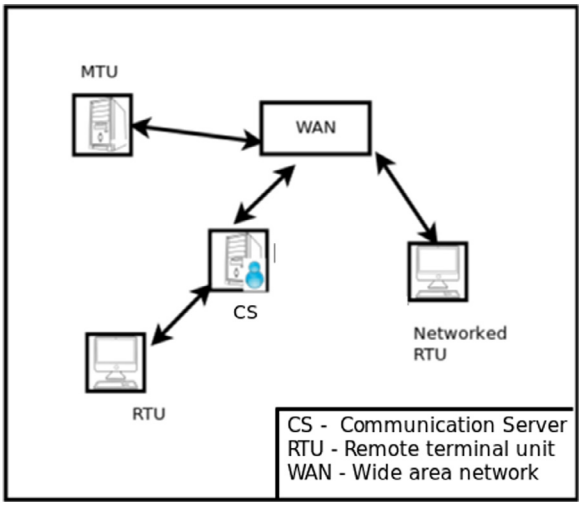

Fig. 7. Networked SCADA system Architecture.

connected to the network [7]. The significant game-changing improvement in networked SCADA was the Intenet Protocol's use for the communication between MTU and RTUs, resulting in disaster survivability.

3.2.4. IoT-based SCADA

The industries have been utilizing the power of technology to build, monitor, and control the systems. IoT innovation and economically accessible cloud computing with SCADA systems have considerably lessened its infrastructure and deployment costs. Moreover, the integration and maintenance are also easy as compared to the previous generations [8]. Industries 4.0 is an example of a fourth-generation SCADA system, as shown in Fig. 8. It includes distributed cognitive computing, CPS, IoT, and cloud computing[2]. SCADA systems already share a few characteristics of IoT, e.g., data access, manipulation, and visualization. IoT differs in terms of interoperability, scalability, and capability of big data analytics. The collection and control of all data are done using

[2] https://www.i-scoop.eu/industry-4-0/ .

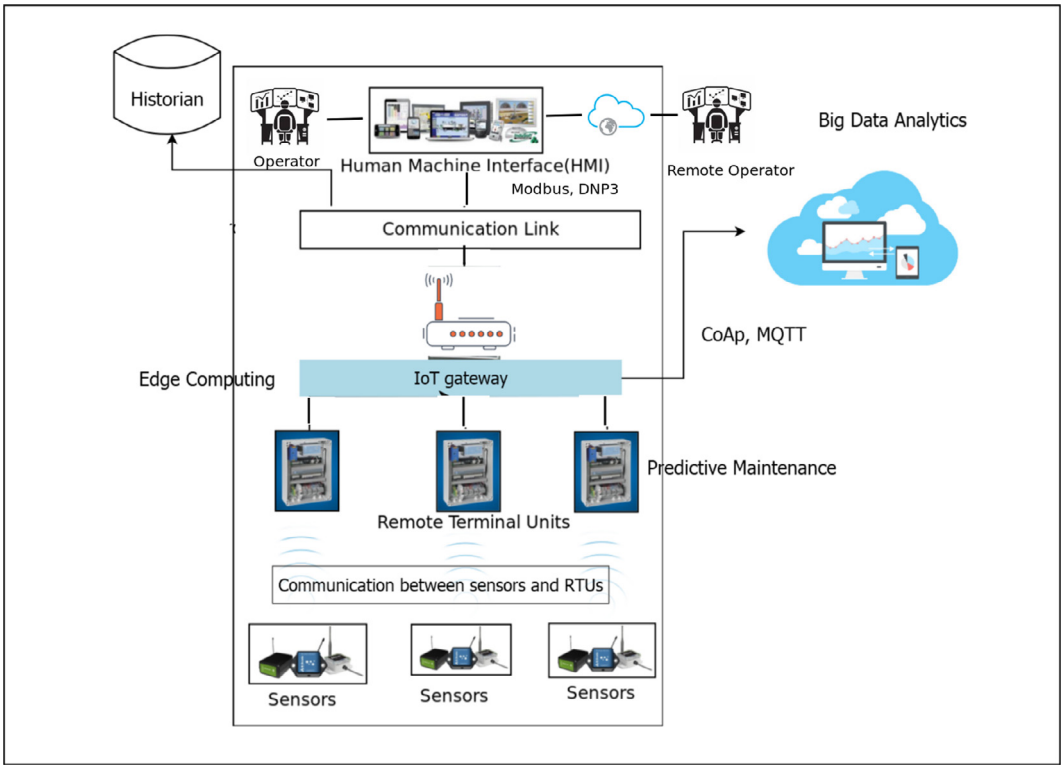

Fig. 8. IoT-based SCADA.

an open communication standard. The collected data is stored on clouds and extraction to get valuable insights from data. IIoT or Industry 4.0 refers to the developments in fourth-generation SCADA systems. IIoT is described as IoT in industries. It is a network of devices with a significant focus on transfer, control of critical information, and large data insights. Therefore, to inculcate IIoT in SCADA, several devices, protocols need to be integrated into the existing system. IIoT has also improved its resilience by identifying anomalous behavior using data-driven techniques [9,10,75]. Scheduling downtime in CI is a challenging task. However, using predictive maintenance, these downtimes can be reduced [11].

Over the evolution of SCADA from a monolithic architecture to an IoT-based SCADA, these systems rely on effective information communication to collect, analyze and display data from heterogeneous devices using different protocols and networks over wired or wireless network. However, a wide heterogeneity in the technologies, protocols, and proprietary architectures increases complexity, cost, and efforts to achieve seamless interconnection and sometimes results in faulty communication [36]. A series of standards were introduced to provide a homogeneous system development utilizing open communication protocols. OPC foundations established Object Linking and Embedding (OLE) for Process Control) to develop common standards for open connectivity of industrial automation devices and systems in 1996. Later, OLE for Process Control was released as an Open Platform for Communication (OPC) to adapt to other applications' standards. OPC is built on a client-server architecture. In 2008, OPC Unified Architecture (OPC UA) was released, which is a platform-independent service-oriented architecture. It supported interoperability for Industrie 4.0 and IoT. It integrates all the functionality of the individual OPC Classic specifications into a single extensible framework that supports functional equivalence to all classical OPC and a secure, extensible, and platform-independent, unlike classical OPC. The standard for OPC-UA is IEC 62541 [37].

3.3. SCADA communication protocols

The communication protocols are regulations for the data depiction and exchange over a communication link. SCADA communication protocols play a pivotal role in MTU-RTU interactions. At first, instruments and protective relays permitted remote communications using local RS232 association or a dial-up modem interface. But due to scalability issues, they have moved to more advanced protocols [12].

As the SCADA system is a composition of many components, if each component uses a vendor-specific protocol, it will not communicate with other components. Each vendor-specific SCADA protocol has its own rules and communication procedures, which can vary from data presentation and conversion, assignment of addresses to command generation, and status information. Therefore, to support interoperability and cost efficiency, some open standards were presented.

To encourage open protocols, the Open System Interconnection (OSI) model was introduced in 1984 [13]. The OSI model shows the data communications process composed of seven independent layers, and each of the layers describes how the data is handled in the different stages of transmission. Open protocols increase the availability, interoperability of the devices, minimize dependency on vendors, optimize cost, ease technical support, etc.

A study of various communication protocols is categorized into two parts, i.e., wired and wireless. Wired communication is also known as wireline communication. It considers the transmission of data over a wire-based (e.g., ethernet cables) communication technology. However, in wireless transmission, communication does not rely on the wire. Radio waves are popular wireless technology. Different wired and wireless SCADA protocols are discussed below.

3.3.1. Wired SCADA communication protocols

Modbus: Gould Modicon developed the Modbus transmission protocol, an application layer messaging protocol for their Modicon

programmable controller [14]. It is the most commonly used protocol for connecting the electronic devices due to openly published and easy to use. Moreover, it is used for the interactions between MTU and RTUs.

A typical Modbus network supports one master and a maximum of two hundred forty-seven slaves. RTUs only reply to messages targeted to them but avoid responding to the broadcasts [15]. It uses four types of communication messages, such as to request/response message to/from MTU, acknowledgment message for the successful delivery of the message at the MTU, and RTUs. MTU can send messages to the slaves and assign an address to each of the slaves, varying from 1 to 247. Modbus/TCP, an enhanced variation of Modbus, is also available, which focuses on reliable communication over the Internet and Intranet. It follows TCP/IP's error detection methods to detect the errors.

Modbus plus protocol is proposed to overcome the master terminal vulnerability issues. It is a token-based protocol. Modbus protocol assembles the request message transmitted from the remote terminal to the master terminal into PDU, an amalgam of the data request, and a function code. PDU changes over into an application information unit by including function code fields at the OSI layer. Similarly master terminal will send a reply to the remote terminal. However, due to extra cable and other communication issues, it is not preferred for real-time communication. Chen at el. [42] analyzed the Modbus/TCP protocol security by implementing attacks (MiTM attack and DoS) on a real-Time CPS Test Bed. They used LabVIEW and PXI modules to simulate SCADA systems and IED The communication system was simulated using Opnet's system-in-the-loop.

DNP3 Distributed Network Protocol (DNP) protocol is based on the Enhanced Performance Architecture (EPA) model. EPA is a streamlined type of OSI layer architecture. It was developed by Harris, Distributed Automation Products [16]. The DNP3 protocol development motive was to obtain open and standards-based interoperability between RTUs, MTU, and Programmable Logic Controller (PLC).

Data link layer convention, transport functions, application conventions, and data link library are the core components of the DNP3 protocol. A user layer is appended to the EPA architecture responsible for multiplexing, data fragmentation, prioritization and error checking, etc. In the DNP3 protocol's layered architecture, the application layer details the packet design, services, and procedure for the application layer. This message is then forwarded to the pseudo-transport layer, which forwards the segmented data unit to the data link layer. It further forwards the message to the physical layer [17]. It supports multiple-slave, peer-to-peer, and multiple-master communication. Lu et al. [18] proposed a cryptography-based design to enhance the security of DNP3-protocol. The authors observe that the upgraded DNP3 protocol can overcome Man-in-the-Middle (MitM) and replay attacks without any overhead. The strategy consists of four stages: identify authentication, key agreement, critical update, and communication protocol. Marian et al. in [19] experimented on DNP3 protocol using digital signatures. *IEC 60870-5 Protocol* The International Electro-Technical Commission (IEC) 60870-5 protocol also follows EPA model. The application layer is included as an additional top layer of EPA architecture, which indicates the functions related to the telecontrol framework. Telecontrol framework based variations e.g., T101, T102, T103, T104 characterize various particulars, data objects, and function codes at the application convention level [20]. For the efficient transmission, the DNP3 layer stack adds a pseudo-transport layer, but it is not used in IEC 60870-5. Pidikiti et al. [43] discussed the IEC 60870-5-101 protocol vulnerabilities and its exploitation by coordinated attacks. IEC 60870-5-101 lack the application layer and the data link layer security. *Foundation Fieldbus Protocol* This protocol was presented by FieldComm Group[3]. The user, application, data link, and physical, the four-layer stack is used in Foundation Fieldbus. The architecture of Foundation Fieldbus follows the OSI layer model in which the user layer is added as an additional top layer of the application layer. The user layer acts as a gateway between software programs and field devices. Easy process integration, multifunctional devices, open standard, and decreased massive wire cost features of Foundation Fieldbus are superior to other protocols. *Profibus Protocol* Process Field Bus (Profibus) protocol was promoted by BMBF (Germany). The communication of data between MTU and RTUs is a cyclic process. MTU reads RTUs input data and writes RTUs output data. Field bus message specification, distributed peripheral, and Profibus variations are the three versions of Profibus protocol. Profibus is most popularly used in discrete manufacturing and process control [16]. *IEC 61850 Protocol* The International Electro-Technical Commission(IEC) 61850 protocol was developed by the IEC Technical Committee 57[4]. A group of manufacturers (ABB, Alstom, Schneider, SEL, Siemens, Toshiba, etc.) proposed this protocol to improve equipment interoperability [21]. This protocol differs from other OSI reference models in the sense that it also describes how data is executed and stored apart from how it is sent and received. The source and destination address are 48 bits each [22]. IEC 61850 is generally used in electrical substations for communication among intelligent electronic devices [23]. Moreover, IEC 61850 abstract data models can be mapped to many other protocols, e.g., MMS, GOOSE, and SMV [24]. *HART* Highway Addressable Remote Transducer (HART) is a very popular request/reply based bi-directional communication protocol that was initially developed by Rosemount Inc. It was made an open protocol in 1986. It is widely used in small automation applications to highly sophisticated industrial applications for industrial process measurement and control applications. It is called a hybrid protocol as it provides two simultaneous communication channels, analog and one digital communication channel. It uses frequency shift keying for data modulation. The digital signal uses 1.2 kHz for bit 1 and 2.2 kHz for bit 0. HART supports both point-to-point, multidrop network topologies. In point-to-point mode, both digital as well analog signals are used. The primary measured value signal is generally specified to be the 4–20 mA analog signal and other devices' information is sent digitally using FSK on the same 4–20 mA wiring [38]. In the multidrop topology, a two-wire system is used to connect the field devices. Unlike traditional analog devices that communicate only a single process variable, HART supports other types of information transmission with the process variable. However, message broadcasting is not supported in HART. *Comparison of wired communication protocols* Accordingly, SCADA communication conventions have advanced from restrictive to business/open-source conventions. SCADA framework's unwavering quality relies on its correspondence conventions. A brief and comparative analysis of communication protocols available for SCADA is Table 2. Since DNP3, IEC 60870-5-101, and Foundation Fieldbus are open Standards [25]. These protocols are more widely used. DNP3 and IEC 60870-5-101 focus on providing the first level solutions of Data Acquisition Interoperability. These are required to communicate outside the substation [17]. DNP3 allows SCADA systems to poll at a different frequency while IEC 60870-5-101 poll at the same frequency, which helps it is a case of limited bandwidth. The packet size in DNP is larger than IEC 60870-5-101. Hence for long-distance DNP3 protocol is favored. Modbus is, for the most part, utilized for applications where the volume of information exchange is low [12]. It is a quick and safe convention, and a ton

[3] https://en.wikipedia.org/wiki/FOUNDATION_fieldbus .

[4] https://en.wikipedia.org/wiki/IEC_61850 .

Table 2
Comparison of wired SCADA communication protocols.

Attribute	Modbus	DNP3	IEC 6870-5-101	Foundation Fieldbus	Profibus	**IEC 61850**	HART
Year	1979	1993	1995	2004	1989	2005 (Project started in 1995)	1986
Organization	Gould Modicon	Harris, Distributed Automation Products	IEC	FieldComm Group	Promoted by BMBF (Germany)	IEC Technical Committee 57	Rosemount Inc.
Architecture	Single layer i.e. Application layer	4 layer architecture	3 layer architecture based on EPA model.	4 layer architecture	3 layer architecture	3 layer architecture	5 layer architecture
Addressing	8-bit address	16-bit source and destination addresses	0, 8, 16-bit addresses are supported	8, 16, 32-bit addresses are supported	7-bit address (0–3 address are used by master and rest by slaves)	48-bit source and destination addresses	4-bit addresses (newer version support 32 bit address)
Users	Target low volume data applications	China, North America, and Australia	Europe, China	America and France	All over the world	All over the world	All over the world
Source	Open source	Open source	Commercially available	Open source	Commercially available	Open source	Open source
Security state	No encryption and authentication control	DNP3-SA support encryption and authentication control	No encryption but supports authentication control	No encryption and authentication control	Supports encryption and authentication control	No encrption but supports authentication control	No encryption and authentication control
Possible attacks	DoS, MiTM [42]	Response replay, MiTM attack [44]	DoS [43]	DoS, MiTM [45]	DoS	DoS, Spoofing, MiTM [46]	Spoofing attacks, Lack of authentication and XML injection attack

of data is loaded in one message [26]. Modbus is a single layer protocol while DNP3, Foundation Fieldbus, uses four-layer architecture. Modbus is mainly targeted for low volume data applications. Only DNP3-SA and Profibus support encryption and authentication control, while Modbus is an insecure communication protocol. IEC-6870-5-101 and IEC 61850 do not support encryption but allow authentication control. Foundation Fieldbus is preferred when considering the power availability as HART signal can only be around 35 milliwatts and 4mA. Many factors affect the protocols selection for communication, such as the utility of the system, location where the SCADA system will be implemented. Choosing the best protocols ensures that if needed, the developed system will have good potential for scalability. Systems should have the flexibility to incorporate security in communication protocols.

3.3.2. Wireless SCADA communication protocols

Apart from the traditional communication protocols, in IIoT based SCADA, other IoT protocols, e.g., IEEE 802.15.4, Zigbee, Bluetooth Low Energy (BLE), Long Range (LoRA), WirelessHART, Wi-Fi etc. are used for communication. *802.15.4.* IEEE 802.15.4 standard is a basis for many other wireless protocols, e.g., Zigbee, WirelessHART, 6LoWPAN, etc. These protocols are developed by extending the upper layer to IEEE 802.15.4 standard. It specifies the physical layer and media access control for low-rate wireless personal area networks. It works on 2.4 GHz ISM. It is generally preferred for low-cost, low-speed (≈100 kbits/s) and low-data rate (≈250 kbits/s), low-range (≈10 m) communication. It supports real-time communication, collision avoidance, and secure communication. The standard mentions the lower layers, i.e., physical and medium access control in the OSI model. It supports peer-to-peer and star network topologies. *Zigbee* Zigbee, an IEEE 802.15.4 based communication protocol, is developed by the Zigbee alliance. Zigbee was standardized in 2003 and revised in 2006. The range of Zigbee communication is between 10 to 100 m line-of-sight, depending on environmental characteristics. Zigbee architecture includes three types of devices, i.e., fully functional device (act as a router), reduced functional device, and a coordinator. It enables wireless personal area networks and provides a communication protocol with low power digital radios. In short, it is a low data rate, low-power, and low communication range wireless ad hoc network, which is secured by 128-bit symmetric encryption keys and a data rate of 250 kbps. *Bluetooth* Bluetooth special interest group developed with a motive to decrease the power consumption as compared to classic Bluetooth technology. The protocol stack in BLE is the same as in classic Bluetooth. BLE supports a quick transfer of small data packets with 1 Mbps data rate. It does not support data streaming and follows master-slave architecture; master behaves like a central device that connects to many slaves, resulting in the need for power-efficient devices. The energy is saved by keeping the slave nodes in sleep mode by default and wake up these nodes periodically to send data packets to the master node and receive control packets from the slave node. BLE is 2.5 times energy efficient than Zigbee [27]. *LoRA* LoRA, a long-range communication protocol, was developed by Cycleo of Grenoble, France. In 2012, it was acquired by Semtech. It supports long-range communication up to 10 Km and a data rate of less than 50kbps with low power consumption. It is most suitable for the non-real-time application, which is fault-tolerant. It works in the physical layer combined with Long Range Wide Area Network, in the upper layers.

Apart from these device-to-device communication protocols, other application layer protocols e.g., MQTT, Constrained Application Protocol (CoAP), and Message Queue Telemetry Transport (MQTT) are developed for the IoT environment as HTTP, HTTPs are not suitable due to resource constraints.[5] *CoAP* CoAP, a specialized Internet Application Protocol, is an replacement of HTTP for resource constraint IoT based devices [31,32]. Low overhead, multicast, and ease to use are the basic pillar for IoT devices. IoT devices have much less memory and power supply in comparison to traditional Internet devices. It uses an efficient XML inter-

[5] https://www.checkpoint.com/downloads/products/top-10-cybersecurity-vulnerabilities-threat-for-critical-infrastructure-scada-ics.pdf .

Table 3
Threats to the SCADA systems.

Threats	Description
Physical security	SCADA systems are geographically distributed. Hence their physical security is a big issue [28,29].
Operating System Vulnerabilities	The SCADA system is expected to be running continuously without interruption. So any patch to the SCADA system cannot be applied.
Authentication Vulnerabilities, i.e., Permission, Privileges, and Access controls	Generally, for employee convenience, the passwords are shared, which eliminates the sense of authentication and accountability. Also, some vendors put default passwords, which are used without modification by the user. Moreover, password policies also very weak [30].
Improper authentication, i.e., Unauthorized remote access	Due to the geographic distribution, to monitor the system, remote access is required. Remote access is more vulnerable to unauthorized access.
Audit and Accountability, i.e., Monitoring and Defenses	Cryptographic communications, Intrusion detection system (IDS), firewall are not universally used. It is challenging to implement these cryptographic approaches on sensors or actuators, considering the resource capability and scale. Security documentation is also limited. The potential for zero-day attacks is always present. The security assessments tools are also lacking to achieve up to the mark performance.
Wireless communication network	In SCADA systems, the communication link is mainly wireless. Depending on the implementation these links are vulnerable to the security attacks.
Legacy SCADA Software	Most of the SCADA systems use legacy software which was designed long ago. Security of the system was not a consideration at that time [30].
Upgrade restriction	The processors are constrained by low computation power and memory resources, and also these systems are not compatible with upgrades [30].
Public Information	In most of the application sectors, the design and architecture of SCADA system are published making it available to attackers. Also, employees working on a firm leak the information from their past working place [29].

changes data format that leads to a more space-efficient protocol. It also supports resource discovery, message exchange, autoconfiguration, built-in header compression, etc. It uses four types of messages, i.e., confirmable, non-confirmable, acknowledgment, and reset. Confirmation messages are used for reliable communication; acknowledge message is used to deliver the message successfully. By default, CoAP is bound to User Datagram Protocol (UDP), and security is provided using datagram transport layer security. *MQTT* MQTT, a publish-subscribe-based messaging protocol, was developed by IBM. It is a client/server protocol, where clients act as a publisher or subscriber, and the server behaves like a broker. The information is arranged in a topic hierarchy. The topic name is generally in text format, which increases the overhead. A client sends a control message to the server when it wants to publish a message. The server distributes the message to the subscribers later. Neither publisher nor subscribers need to share their configurations, location. MQTT is supported over the Transmission Control Protocol(TCP), which restricts its use for all types of IoT devices. MQTT control message size varies between 2 bytes to 256 megabytes. It supports 14 control messages to manage publisher-broker-subscriber communication [33].

Apart from MQTT, few extensions, e.g., MQTT-S/ MQTT-SN, are proposed, which specifically focus on cost and power effective solutions. These include replacing topic text with topic Ids, buffering procedure for nodes in sleep mode, etc. MQTT-SN is proposed to use over UDP or Bluetooth. The communication network protocols do not support security features. Therefore, they are prone to cyber-attacks.

WirelessHART Wireless communication support to HART is added in WirelessHART while maintaining compatibility with existing HART devices, tools, and commends. WirelessHART, released in 2007, is supported by multiple vendors and follow interoperable wireless standards [39]. It uses a 2.4 GHz ISM radio band and is based on wireless mesh technology. *Wi-Fi(802.11a/b/g/n/ac)* Wireless Fidelity (Wi-Fi)[6] is based on IEEE 802.11a/b/g/n/ac standard family and designed seamlessly with its wired sibling Ethrnet. It uses 2.4 GHz and 5GHz ISM radio band. It supports communication in the range of 20 m indoor, 150 m outdoors and can achieve speeds of 1 Gbits/s. It supports star and mesh network topologies [156]. In comparison to SCADA wired communication protocols, Wi-Fi protocols are more vulnerable to attack because an adversary within range of a network having a wireless network interface controller can try to get the network access. *Cellular network* It supports several frequency bands depending upon the regions and type of network and ranges up to several kilometers. The data rate supported is up to 10 Mbits/s. It has single antenna reception. Cat-1 and LTE-M are the fully-available cellular IoT option and are generally preferred for IoT applications that require a browser interface or voice.

In the next section, we discuss the inherent vulnerability of SCADA systems by looking at reported attacks.

4. Taxonomy of attacks

Recently, the number of security-related attacks on SCADA system has drastically increased. Threats like Stuxnet [34], Aurora[7], Maroochy [35] give us a clear idea of how much damage a determined adversary can cause even on the general public.

Table 3 summarises the various threats to the SCADA systems. The physical security of these systems remains a significant issue due to geographical distribution. These systems are expected to run without any interruption, so any patch or upgrade cannot be applied without compromising its productivity. Moreover, most of the communication happens on the wireless network, making it vulnerable to network security attacks. The architecture and design of SCADA systems are available in the form of patents or publications, which make it accessible to hackers. We have also highlighted the vulnerable SCADA component w.r.t. Each threat. Sensors and actuators are prone to physical security as they are generally deployed in remote areas. PLC, MTU, and RTUs still use legacy SCADA software and are restricted from updating. Therefore, these are even prone to well-known vulnerabilities exploitations.

A lot of attacks have been detected even with advanced security solution enforced in the system. The first known cyber-security attack occurrence, including the SCADA framework, was in 1982, in which the enemy implanted a Trojan in the SCADA framework that was responsible for controlling the Siberian Pipeline. A brief analysis of the reported attacks is given in the next subsection.

4.1. Analysis of attacks

To analyze the SCADA specific attacks, we searched for the available databases. The Repository of Industrial Security Incidents

[6] https://en.wikipedia.org/wiki/Wi-Fi .

[7] https://en.wikipedia.org/wiki/Operation_Aurora .

(RISI) [47] database is the only database that indexes the SCADA specific attacks. The other common vulnerabilities databases are NVD [55], ICS-CERT[8], WhiteSource[9]. A brief analysis of SCADA vulnerabilities extracted from the National Vulnerability Database (NVD) is done in [56]. Authors observe that approximately 89% of the vulnerabilities can only be exploited on the network. Approximate 19% of the reported vulnerabilities are due to buffer errors; that arise due to insecure and legacy operating systems. Since our primary focus is analyzing attacks rather than the potential vulnerabilities, we use RISI to investigate the attacks feature.

In 2020, the RISI database [47], a publicly available online database, contains 242 incidents that are recorded from 1982 to 2015. This data set is considered one of the richest to date to understand the attack's taxonomy. The real count of such attacks is much more than because many real-time attacks are not reported [4]. The database has not been updated from 2015, yet it provides a realistic understanding of the security state of SCADA systems. RISI is the only reliable source in best of our knowledge that focuses on SCADA system attacks. It is necessary to analyze the previous security assaults to prevent future attacks, i.e., how the attacks have been carried out [4]? How can the system be made more robust against these attacks? Moreover, Henrie in [57] commented on the current cyber state of the SCADA system that these attacks are "real and expanding". An in-depth analysis of these security incidents can provide the capability to detect and prevent these attacks priorly. Miller and Rowe analyzed past attack records based on the originating sector, how the attack was implemented, and the attack target sectors. Their study on previous attacks gives the nature of those attacks.

In Table 4, We summarise some of the high-impact SCADA security incidents chronologically. The table highlighted the country and industry in which the attack was reported. It also lists the target component, impact of the attack, the method used to launch the attack, and vulnerable SCADA component. The attack's impact is categorized into six categories, i.e., Financial Loss, System Damage, Production Loss, Daniel of Service, Latency, and Intellectual loss. We further classified the type of attacks into five categories, i.e., Malware, Noncyber attack, Unauthorised Remote Access, Interruption of Service, and Unknown. Unknown denotes the attack category for which the source is still unknown. Vulnerable SCADA component specifies the SCADA component whose vulnerability was exploited during the attack on the SCADA system. The attacks in Table 4 are chosen to cover a maximum number of impacted industries over the years. According to the RISI repository, about 17 countries have one reported security attack per country. The entire RISI dataset was analyzed to find out patterns and highlight key points. Organized hacking groups cause 5% of the reported attack. The result of the analysis in Fig. 9 number of reported attacks vs. country shows that the USA and UK are the countries most affected by cyber-attacks. Sixteen reported attacks do not mention the country name. There are seven countries that have two cyber-attacks per country. However, this observation depends on the quality and completeness of the RISI database. The completeness of the RISI data set depends on the nations who report these attacks. Moreover, 20% of the attacks on critical infrastructure are unknown [58].

In Fig. 10, we analyze which application sector is more prone to the attacks. Forty-eight attacks have been reported in the transportation sector, which is followed by 46 attacks in power and utilities. The reason for the more vulnerable industry may depend on the revenue obtained due to the attack. Moreover, an attack can originate from many sources to harden the mitigation processes.

Fig. 11 shows that approximately 28% of the reported attacks are due to malware attack. Unauthorized access is also another cause of many attacks. Therefore, adequate security policies should be practiced in industries.

The standard vulnerable configuration includes default username-password, unencrypted communication, weak firewall policies. 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 [59]. Securing SCADA systems is a challenging task as compared to the traditional IT systems.

As per the Dell security annual threat report[10], the number of attacks against SCADA systems doubled in 2014 on the year-to-year basis. The expert also confirmed that most of these attacks are politically motivated. The countries which have extensive SCADA systems are Finland, the United Kingdom, and the United States. We need to strengthen cyber-security measures of SCADA systems to shield them from cyber assault [60,61].

The network's primary security mechanism applicable to IT sectors is invalid for SCADA due to legacy-inherited cybersecurity vulnerabilities and their potential exploitation. The IT network is primarily focused on the confidentiality of the data at all costs compared to SCADA, where the SCADA systems need to be available at all prices. Traditional security mechanisms are effective for the IT network, but these mechanisms are not developed considering the availability requirement.

Security mechanism, e.g., patching, up-gradation, etc. is a challenging task to apply without rebooting the device, i.e., affecting the plant's communication. So, the daily maintenance and timely application of patches is a tedious task. A strategic and efficient patch prioritization approaches specific to the SCADA systems need to be explored in such a case. Alshawish et al. in [62] provided an integrated risk-based decision-support methodology for patch prioritization. The approach considers the interdependencies in the network, attacker behavior, and publicly available information regarding the vulnerability and exploit. They used the Time-To-Compromise security metric for assessing the compromise risk. Granadillo et al. [63] proposed a geometrical model that calculates the volume of systems (risks), attacks, and countermeasures. The approach recommends the application of security mechanisms in the decreasing order of volume of systems. Yadav et al. [64] proposed an updates ordering mechanism PatchRank by considering the functional dependency of the SCADA systems, attacker behavior, resource constraint, and NVD vulnerability assessment. The authors demonstrated a comparative analysis of PatchRank with other benchmark algorithms to show that PatchRank converges to a usable, secure state faster. However, all these approaches need to be adequately validated before using them in the field. Yadav et al. [65] addresses the need for patch sequencing in the SCADA chain in smart grid systems. The proposal recommends using system criticality and attacker behavior-based decision making. The method's primary focus is to identify a patch sequencing strategy that minimizes the possible attacks' impact in a resource-constrained scenario.

The attacks on SCADA have miserable effects. New secure architectures are required for SCADA systems. Cardenas et al. first explored research challenges for the security of the cyber-physical system (CPS). [66]. The authors focus on the requirement of secure CPS and also discussed some of the vulnerabilities that might occur due to the fusion of cyber and physical systems. Clifford Neu-

[8] https://us-cert.cisa.gov/ics/advisories .

[9] https://www.whitesourcesoftware.com/vulnerability-database/ .

[10] https://www.silicon.es/wp-content/uploads/2015/12/2015-dell-security-annual-threat-report-white-paper-15657.pdf.

Table 4
Some of the Important Attacks during 1982–2016.

Attack title (Year)	Country (Industry)	Target	Impact	Type	Vulnerable SCADA component
Siberian Gas Pipeline Explosion (1982) [47]	Russia (Petroleum)	Pipeline	Financial Loss, System Damage	Malware	Controller
Sellafield Nuclear plant system error (1991)[47]	Uinited Kingdom (Power and Utilities)	Shielding Door	Production Loss	Noncyber attack	Sensor
Virus in Nuclear Power Plant (1992) [47]	Lithuania(Power and Utilities)	Reactor	System Damage	Malware	RTU
Hacking of Salt river project (1994) [47]	United State (Power and Utilities)	Software system	Financial Loss, Data Loss	Unauthorised Remote Access	Communicarion Protocol
Worcester Air Traffic System Hack (1997) [47]	United State (Transportation)	Control System	System Damage	Noncyber attack	Controller
Maroochy (2000) [35]	Australia (Sewage Control System)	Flood gate	Environmental Damage	Unauthorised Remote Access	Communication protocol
Utility SCADA system attack (2001) [47]	United State (Power and Utils)	SCADA control system	System Damage, Financial Loss	Unauthorised Remote Access	Communication Protocol
SQL Slammer (2003) [48]	United State (Petroleum)	Automation Segment	Daniel-of-Service	Interruption of Service	Communication Protocol
Virus injected in CSX train signaling system (2003) [4]	United State (Transportation)	Signal dispatching system	Latency	Malware	Communication Protocol
Nuclear plant slammer attack (2003) [47]	United State (Power and Utilities)	Nuclear power plant	System Damage, Financial Loss	Malware	Communication Protocol
Nachi worm on control servers (2003) [47]	France (Chemical)	Advanced process controller (APC)	Latency	Malware	Historian
Sasser worm (2004) [47]	United State (Chemical)	Decentralised control system (DCS)	System Damage	Malware	Controller
Sasser worm (2004) [47]	United Kingdom (Transportation)	Check-in controller system	Latency	Interruption of Service	RTU
Water company hack in Pennsylvania (2006) [47]	United State (Water/Waste Water)	Water plant computer system	System Damage	Unauthorised Remote Access	Computer system in SCADA network
Phishing attack (2007) [47]	Unknown (Power and Utilities)	Employee computer	System Damage	Malware	None
Emergency siren Activation (2008) [47]	United State (Other)	Emergency Siren	Daniel-of-Service, System Damage	Interruption of Service	Communication Protocols
Road Sign Hack (2009) [47]	United State (Transportation)	Digital Road Sign	None	Unauthorised Remote Access	Sensor
Power Company Hack in Texas (2009) [47]	United State (Power and Utilities)	Energy forecast system	Financial Loss	Unauthorised Remote Access	Communication Protocols
Stuxnet (2010) [34,49–51]	Iran (Power/Utilities)	Centrifuges PLCs	System Damage, Financial Loss	Unauthorised Remote Access	PLC
South Houston Water Treatment Plant Hack (2011) [47]	United State (Water/Waste Water)	Plant controller	None	Unknown	PLC
Auto manufacturer hacked (2012) [47]	United State (Automotive)	Company computer	Intellectual loss	Malware	Communication Protocols
New York Dam attack (2013)	United State (Water/Waste Water)	Computerized control of Dam	Intellectual loss, System Damage	Unauthorised Remote Access	Controller
Godzilla Attack (2014) [4]	United State (Transportation)	Sign Board	System Damage, Intellectual loss	Unauthorised Remote Access	Communication protocols
Steel Mill Cyber attack (2014) [52]	Germany (Metal)	Furnace	System Damage	Unauthorised Remote Access	Access to SCADA network
Ukrainian Power Outage (2015) [53,54]	Ukraine(Power and Utilities)	Computer network	System Damage	Malware	Historian
Operation Ghoul (2016) [53,54]	Middle Eastern Countries(Cyber Security Company)	Computer system	Data Loss	Malware	Computer system in SCADA network

man in [67] focuses on the design for the secure CPS. He has also enlightened the possible research area that will enhance the security of the CPS. In the proposed work, the author suggests combining security as an integral part of CPS's basic design. For the SCADA system, the security goal is generally the reverse of the prioritized security goals for traditional information technology systems, as shown in Fig. 12. Therefore, attackers generally target to interrupt the SCADA system availability.

With time, attackers have started using more sophisticated techniques to compromise the security of SCADA systems than ever, so the threats are increasing. An attack scenario using electric vehicle infrastructure is described in [68]. Till now, attackers have mainly focused on high-level systems, i.e., HMI and communication protocols. Surprisingly, field device firmware exploitation is the least focused research area [69–71].

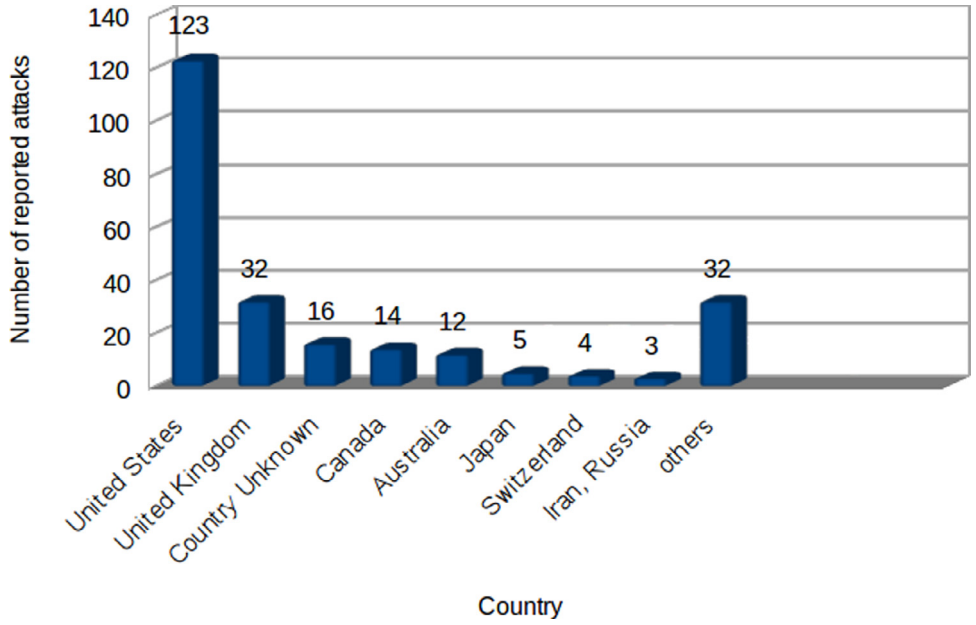

Fig. 9. Statistical view for Country vs Attacks count.

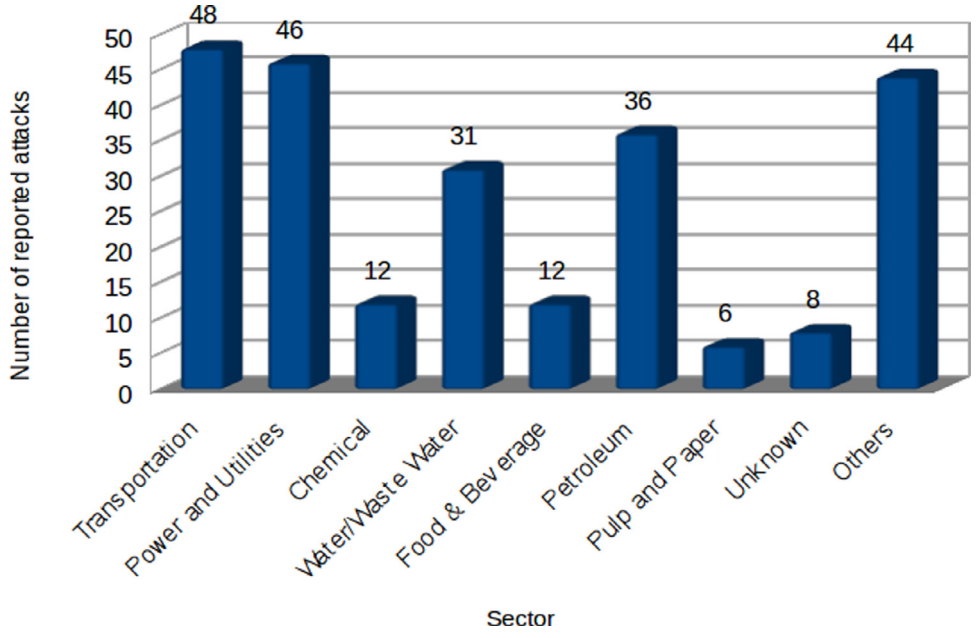

Fig. 10. Statistic view for Sector vs Attack count.

Many international institutes e.g. IEEE, Centre for the Protection of National Infrastructure (CPNI)[11], American Gas Association (AGA)[12], North American Electric Reliability Corporation (NERC)[13] and National Institute of Standards and Technology (NIST)[14], Industrial Automation and Control System Security (ISA)[15] etc. publish guidelines frequently for secure SCADA implementation. The industries are recommended to follow these security guidelines.

A quick and efficient attack detection systems are required, and we will discuss attack detection systems in the next section.

5. Intrusion detection systems

NIST [72] characterizes IDS as the procedure of observing events in a host system or network, and these events are analyzed for signs of unusual incidents [73,74]. IDSs monitors the traffic and operation of the network and host system; if it senses some security violation, the system administrator is notified. The research work for IDSs has been carried out since the 1980s by Aderson. Generally, for analyzing system behavior, IDSs need training and validation data sets of anomaly and attacks. The research work for the

[11] https://www.cpni.gov.uk/ .
[12] https://www.aga.org/ .
[13] http://www.nerc.com/Pages/default.aspx .
[14] https://cve.mitre.org .
[15] https://www.isa.org/ .

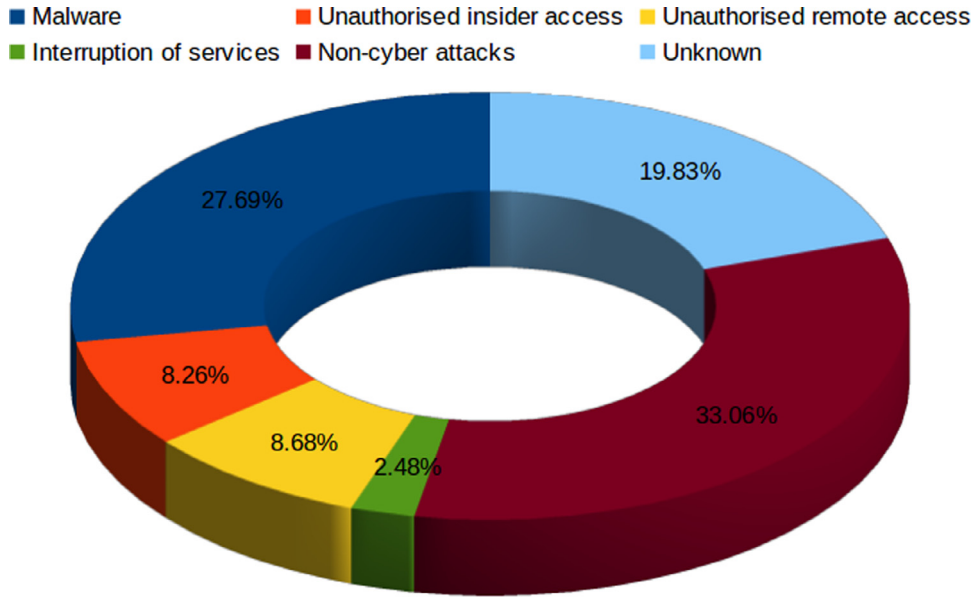

Fig. 11. Threats statistic view for Attack category.

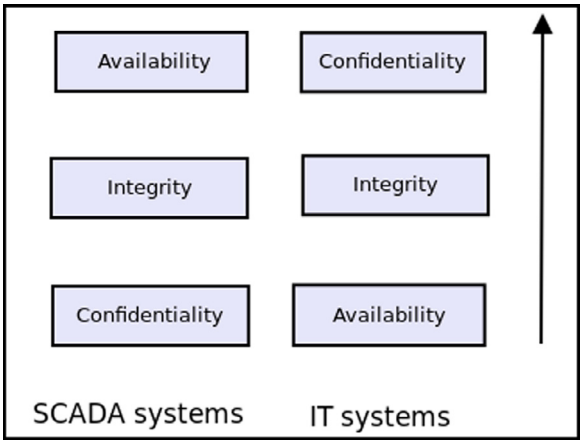

Fig. 12. Priority order for General IT and SCADA.

IDSs suffers from the lack of datasets to verify the functionality of their algorithms.

We surveyed some of the widely used publicly available datasets. Power system dataset [76] includes measurements related to the electronic transmission system, control, cyber-attacks behavior collected from Snort. Gas pipeline and water storage tank dataset [77,78] consists of cyber-attacks against two lab-scale frameworks. This was created using re-enactment of actual defective and ordinary operations of a gas pipeline and water tank separately. It consists of three categorical features, which include payload info, ground truth, and network info. 2,74,623 instances with twenty-row features have been involved in this dataset. Moreover, some unusual patterns were identified in this dataset, which helps machine learning algorithms to detect attacks. KDD99 [79] is a widely used dataset since 1999 for the evaluation of IDSs. It is created by using data collected in DARPA'98 IDS. It consists of forty dimensional 49,00,000 single connection records. However, this dataset does not include analytical or experimental validation of data's false alarm characteristics. It also has redundant and duplicate instances. Therefore, a re-sampled version of the KDD dataset NSS-KDD [80] dataset was created. The first DAPRA dataset, simulated over an air force base, was published by MIT Lincoln Lab in 1998 [81]. However, in 1999, an improved version of this dataset, which includes computer security communities' suggestion, was released. This dataset provides raw host and network dataset which need to be preprocessed to use for verifying machine learning IDSs. Apart from the above-discussed databases, NVD, an extensive and publicly available database for the software and hardware vulnerabilities in a different domain, is a good source for extracting SCADA specific vulnerability. NVD includes an examined analysis of all these reported vulnerabilities using the Common Vulnerability Scoring System (CVSS) framework and provides a base severity score for vulnerability by considering the attack's scope, vulnerability component, impacted component, attack vector and complexity, frequency, privilege required, etc. NVD indexes reported the vulnerability to Common Vulnerability Enumeration (CVE)[16] Ids that enable automated vulnerability management. CVE Ids help to provide a common name for publicly available vulnerabilities. However, a lack of the complete SCADA attack data sets inhibits cybersecurity research for SCADA. There is not a comprehensive dataset covering all the attacks worldwide. Therefore, researchers are required to create the datasets by simulating test-bed with attacks. Moreover, only a few algorithms exist for datasets creation. For zero-day attack detection, advancement in these algorithms is required. Rodofil et al. [82] proposed a modular dataset generation framework for SCADA cyber-attacks. Yang et al. [83] simulated the influence of a simple cyber attack in a smart grid compromising the system's integrity. The authors highlighted an immediate need to look for a robust and timely technical solution to detect and prevent cyber-attacks.

An IDS consists of sensors, an analysis and detection engine, a notification system. Sensors that are deployed either on the host or network are responsible for collecting network and host data. The received data is sent to the analysis and detection engine, which investigate and detect the presence of intrusions. If an intrusion is detected, a notification system notifies the system administrator. IDS techniques can be studied based on the source of information and analysis methodology. A brief analysis of these detection techniques is given below.

[16] https://cve.mitre.org .

Table 5
Comparison of various type of IDSs.

Intrusion detection systems (IDSs) classification	Input	Advantages	Limitations	Examples
Host Intrusion Detection System (HIDS)	Relies on the host activity and states information.	1. Lower cost of entry 2. No additional hardware required. 3. Detect attacks that NIDS miss. 4. Near-real-time detection and response. 5. Monitors specific system activites.	1. Fail to detect internal attacks and DoS. 2. The host, where HIDS resides is susceptible to disablement.	Tripwire[17] OSSEC[18]
Network Intrusion Detection System (NIDS)	Relies on the traffic generated on the network by various set of devices.	1. Real-time detection and response. 2. Detect attacks that HIDS miss. 3. Independent from operating system. 4. Removal of evidence of NIDS is difficult.	1. It fail to analyze encrypted information. 2. Fail to block the host-based attacks.	Snort[19] Zeek[20]

5.1. Classification based on the source of information

Based on the source of information, IDSs are generally divided into Host-Based Intrusion Detection (HIDS) and Network Intrusion Detection System (NIDS). HIDS relies on the host activity and states information, which can be file-system modifications, application logs. To specify/detect host-level misbehavior is easy as HIDS auditing is distributed [84]. NIDS relies on the traffic generated on the network by the various set of devices.

Table 5 shows an analysis of classification of IDSs. HIDS provides approximate real-time intrusion detection without requiring extra equipment.

HIDS such as Tripwire[17] and OSSEC[18] uses whitelists of the filesystem. It is performing file integrity scans that identify any abnormalities which can classify possible intrusions. Moreover, NIDS provides real-time detection, and it is hard to remove evidence of NIDS. NIDS such as Snort[19] and Zeek[20] use rule sets that define a type of intrusion or unacceptable behaviors such as a port scan or a Denial-of-Service (DoS) attack attempt. Shekari et al. [85] proposed a radio frequency-based distributed intrusion detection system (RFDIDS) for SCADA systems. Even if the entire SCADA system is considered untrusted, RFDIDS remains reliable. The monitoring of the power grid substation activities is done using radiofrequency emissions (particularly at low frequencies). Flosbach et al. [86] proposed an extensible and scalable network-based IDS to secure control networks in the domain of power distribution. They are mainly targeted to detect process-based attacks, e.g., manipulated control commands by continuously assessing the local physical process and all control commands. They have also successfully deployed their model at a Dutch power distribution substation.

Radoglou-Grammatikis [87] proposed an IDS for the DNP3 SCADA system and called it DIDEROT (Dnp3 Intrusion DetEction pReventiOn sysTem). DIDEROT uses supervised as well as an unsupervised algorithm. The unsupervised learning algorithm is activated if the supervised algorithm identifies the network flow as abnormal. However, DIDEROT can act either as HIDS or NIDS, depending upon the monitoring module's placement. A consolidated DNP3 parser and validation policy are used in Wireless Bro to apprehend and handle the data communicated by SCADA devices. HIDS sensors are avoided to use in the SCADA components due to resource constraints. In comparison to HIDS, NIDS is generally preferred in SCADA networks. HIDS sensors cannot be installed owing to constrained resources of SCADA components.

5.1.1. Classification based on analysis strategy

In the analysis strategy, signature detection and anomaly detection are the major intrusion detection techniques. Apart from this, specification-based approaches are discussed under analysis strategy. An analysis of these approaches is discussed below.

5.1.2. Signature based intrusion detection technique

In signature detection techniques, network traffic is matched with an attack signature, i.e., misuse pattern of the IDS's intrusive detection. The behavior of the system is compared based on the attribute of the network traces. If any host or network activity matches with stored signatures, an alert is triggered. This approach can achieve good accuracy for intrusion detections, which depends on the misuse pattern's correctness. This technique effectively detects known attacks, but it fails to detect new attacks due to the absence of the signature of new or variants of known attacks. Oman et al. [88] presented a signature-based SCADA test setup for the power-grid sector to detect the adversaries and help the operators identify the common configurations errors. A respective entry to command is made in the XML profile. Snort IDS signatures are generated for legal commands using a pearl script. The author generated 100 customized signature and recommended to research for automatically signature generator. Also, the signatures were generated for RTU only. Yang et al. [89] proposed a, rule-based IDS for IEC 60870-5-104 protocol. The abnormal events categorization is done based on non-IEC/104 communication, spontaneous messages storm, remote control commands, or remote adjustment commands from unauthorized client, reset process command from unauthorized client and potential buffer overflow. The authors represented their approach using a protocol traffic case-study. Anomaly detection systems can work efficiently if the traffic is regulated and have predictable behavior [90].

5.1.3. Anomaly detection based intrusion detection technique

An anomaly detection, the system compares current network traffic with standard behavior profile, and if something (significantly) unusual appears, then an alert is raised. In this system, known intrusions are not required. The distinctive patterns are learned over time with specific statistical profiling of the overall system's usual behavior. Machine learning-based techniques are

[17] https://www.tripwire.com/ .
[18] https://github.com/ossec/ossec-hids .
[19] https://www.snort.org/ .
[20] https://www.zeek.org/ .

a data-driven supervised & unsupervised intrusion detection approach. Its analysis can distinguish between normal and critical states and removes the requirement for domain experts. A combination of the status represents the standard states. The critical states take the form of noise, i.e., outliers. It also extracts efficient detection rules from the identified states. However, this technique can result in a false alarm rate because it is difficult to find a correct model for general behavior [91]. Machine learning-based approaches can detect zero-day attacks [92]. Gao et al. [93] demonstrated that a feedforward neural network is advantageous on uncorrelated attacks detection while long-short term memory outperforms in detecting the correlated attacks. The features used for anomaly detection are the source and destination IP address & port, TCP sequence number, transaction identifier, function code, reference number, register, exception, time, relative time, highest and lowest threshold, pump speed, and tank level, link utilization, CPU usage, login failure. The authors presented a categorization of correlated and uncorrelated attacks.

Silva et al. [94] presented an artificial neural network-based approach to detect Distributed Denial-of-service (DDoS) attacks in the smart-grid SCADA network using the IEC-61850 protocol. The method uses each sample's relative percentage error as a threshold to distinguish a normal situation, and DDoS attacked scenarios in communication networks for electric power substations. The authors used sixty-two prediction steps to reduce the percentage relative error up to 5%. Khan at el. [95] proposed a hybrid multilevel approach for detecting known attacks by comparing the signature followed by identifying the deviation from expected behavior using bloom filters. The method is divided into four parts: preprocessing techniques (standardization and normalization), dimensionality reduction, nearest-neighbor algorithm to balance the dataset, and known and zero-day attacks detection. Yang et al. [96] proposed a deep-learning-based network intrusion detection system for SCADA networks using the convolutional neural network to identify SCADA traffic's salient temporal patterns. They mainly used it to detect conventional and SCADA specific network-based attacks. The proposed IDS take SCADA network packets generated by the SCADA hosts on the network switch. The temporal network patterns extracted from the SCADA packets are used to identify the window containing abnormal patterns. Perez et al. [97] explored ML algorithms (support vector machine, random forest, bidirectional Long Short Term Memory (BLSTM)) and assessed them in terms of accuracy, recall, and precision using database Mississippi State University collected from a gas pipeline system. Random forest and BLSTM show 99% and 96%, respectively.

Kravchik et al. [98] presented a study of detecting cyber attacks on ICS using convolutional neural networks on a secure water treatment testbed dataset. Their research demonstrates that ID convolutional neural networks work better for anomaly detection than other classification algorithms. Almalawi et al. [99] have also tested this algorithm on eight databases, including five public databases. The presented algorithm approaches an average precision of 98% in recognizing the critical states. Bigham et al. [100] compared the performance of invariant induction and n-gram anomaly detection algorithms for the IEEE 24 bus test network. The database has 8736 files having snapshots of the network for each hour for a year. Invariant induction performs better for finding the anomaly in a file, while n-gram performs better to identify the database's corrupted file. The authors recommended using a hybrid model to reduce false positives and false negatives while identifying electricity data anomalies.

Linda et al. [102] presented an IDS based on the neural network (IDS-NNM) model. The algorithm uses a union of two neural network algorithms, i.e., Levenberg Marquardt and the error backpropagation. The IDS-NNM consists of two steps. In the first step, a particular training set is created. For data acquisition, an Allen Bradley PLC 5 controller connected to an ethernet network is used. The PLC is further connected to a control system via the hub. The data for various attacks were simulated through the hub using software tools, e.g., Nmap, Nessus, and Metaspoilt. Later, the neural network starts training using that training set. Once the training set is generated, it is used in the network communication system to identify intrusion endeavors. Valdes et al. [101] presented a pattern and flow-based anomaly detection system. Patterns based on time-stamp and IP-address are evaluated against an initially empty pattern library using similarity function. The mismatch to the trained pattern is labeled as an anomaly. Rrushi et al. [103] tried to leverage the evolution of the content of the specific locations in random access memory into means of characterizing the normalcy or abnormality of network traffic. The proposed algorithm uses estimation methods from probability theory and applied statistics to measure normal progressions of RAM content. Yang et al. in [104] have proposed an anomaly detection using the auto-associative kernel regression with Statistical Probability Ration test (SPRT) and applied them to the network traffic. Machine learning-based techniques, i.e., probabilistic model-based technique, neural network-based approach, clustering model, multivariate based analysis, are termed as statistical methods. Models are created based on these machine learning methods, and then these models serve as a reference model for intrusion detection.

5.1.4. Specification-based approach

A model is constructed in a specification-based approach, which imposes its predefined strategy and sends an alert if the observed behavior does not follow this policy. This technique defines what is allowable regarding patterns. It has the same purpose as the anomaly detection system. However, in specification-based approaches, a human expert defines the policy for each specification manually. This approach causes a lower false-positive rate due to a manually defined specification. Once the specification is set up, it can start functioning without the need for training. Krauß et al. [105], proposed a quick attack detection system. In the proposed ontology-based model, system logs provide suspicious logs. Suspicious logs with the previous vulnerability database lead to the detection of the ongoing attack. Yang et al. [75] recommend a multilayer framework without undermining the availability of real-time data. The proposed algorithm analyses multiple attributes so that the provided solution can diminish various cyber-attack threats. The proposal consists of 3 attributes, i.e., access-control whitelists, behavior-based rules, and protocol-based whitelists. Access-control whitelists are the first list verified for allowing access. The authors also presented a testbed containing an HMI, simulated attacker, IDS host, protocol gateway and IED simulator, and router. HMI, protocol gateway, and IED are simulated using windows-based systems. HMI and IED communicate via protocol gateway using IEC 60870-5-103 protocol. A Linux-based attacker host is used to simulate DoS, MitM.

Goldenberg and Wool [106] discuss a specification-based approach for IDS which works for Modbus/ TCP networks. A fixed sequence of the query and the response is observed in Modbus traffic; the fixed sequence is verified by operating over many SCADA network establishments. This DFA based IDS working on Modbus/TCP packets produces a very rigorous model, which has been evaluated using real traffic, and it shows a low false-positive rate.

Cuppens and Boulahia [107] presented an ontology that describes alert in IDMEF format. Based on the fitting attack's specific content, an alert is generated, and the system uses a rules-based algorithm to react. D'Antonio et al. [108] presented a secure, distributed architecture composed of IDS to monitor the network flow. The packet's source and destination are observed, and punctual and un-punctual classification is done based on behavior generalization.

Table 6
Comparison of IDSs.

Source	Data type	Input Data	Technique	Attacks handled	Acess
[88]	Not specified	RTUs packets	Signature	Failed login attempts	HIDS
[89]	Simulated	IEC 60870-5-104 packet data	Signature	Spontaneous Messages Storm, Buffer overflow, Reset Process Command from Unauthorised Client	NIDS
[101]	Modbus/TCP simulated data	Time-stamp, Ip address	Anomaly	Probes, DoS, attempts to introduce rogue traffic.	NIDS
[93]	Modbus/TCP simulated data	Extracted features (Modbus packet and SCADA system variables)	Anomaly	Correlated attack (DoS, MitM) & uncorrelated attack	NIDS
[94]	Simulated	IEC-61850 data	Anomaly	DDoS	NIDS
[95]	Existing dataset (simulated gas pipeline system dataset provided by Mississippi State University [77])	SCADA system variables from dataset	Hybrid (Signature, Anomaly based on bloom filter)	Statistical deviation	
[97]	Existing dataset (simulated gas pipeline data by Mississippi State University gassystemdataset)	SCADA system variables from dataset	Anomaly	Statistical deviation	NIDS
[98]	Simulated data from secure water treatment testbed built by the Singapore University of Technology	SCADA system variables	Anomaly (convolutional neural networks)	Specified attack scenarioes	NIDS
[99]	Eight datasets (Five: publicly available, and three : generated by simulation for a water distribution system)	Real-time data from the SCADA systems	Anomaly (The proximity-based etection rules from the identified states)	Variant of DoS & MitM	NIDS
[102]	Real network data	Packet information(Payload entries)	Anomaly	Statistical deviation	NIDS
[103]	Simulated	Protocol data units (PDU) packets	Anomaly (Probabilistic estimation)	Statistical deviation	NIDS
[104]	Created manually	Servers I/O flows and hardware working statistics	Anomaly (Auto-associative kernel regression model)	DoS variant	HIDS
[105]	Not specified	System logs	Specification	Violation of ontology	HIDS
[75]	Simulated on their testbed	SCADA traffic between the HMI and the protocol gateway	Specification (access-control, protocol-based, and behavior-based rules)	DoS, MitM	NIDS
[106]	Real network Data	Modbus data	Specification	Deviation from normal	NIDS
[107]	Created manually	Policies	Specification	Match to the content of fitting attack	
[108]	Real network data	Source and Destination IP, Source Port	Specification	DoS	NIDS
[100]	Existing database (IEEE reliability test system 1979)	Extracted features	Specification	Deviation from normal	NIDS

5.1.5. Discussion on IDSs

Apart from this, behavior patterns are associated with certain attacks. These types of attacks are used with the composition of other attacks. Moreover, some IDSs approaches have been proposed to specifically for resource constraint devices [109–111]. Signature detection, anomaly detection based approaches are knowledge-based techniques. Behavioral detection approaches rely on the behavior pattern. However, the specification approach uses knowledge as well as behavioral patterns. Only the anomaly-based detection approach can detect new attacks. Anomaly detection and behavioral approaches match the pattern, while signature and specification-based approaches need predefined specifications.

Table 6 shows a brief description of various intrusion detection systems, where data type represents whether the data used was simulated or collected on a real SCADA system. Input data and attacks handled represent the input to the framework and the threat model for respective IDSs. The technique represents the IDS characteristics. Most of the IDSs use either Modbus or DNP3 communication protocols. The data used for the verification of the systems are simulated due to the lack of the dataset. Current IDSs are designed to detect a fixed type of attack, i.e., DoS, MitM. Therefore, there is an urgent need to develop hybrid IDSs that combine various IDS characteristics and detect a larger set of attacks.

5.2. Firewall

SCADA firewall is a primary security device that is used to monitor and filter SCADA traffic. It inspects the entering and exiting packets in the SCADA network by following pre-configured firewall rules. SCADA firewalls are specifically designed to secure SCADA communication protocols and applications. The researcher recommended using both firewall and Intrusion Detection together as a defense-in-depth strategy to ensure the SCADA network security from the internet.

A commercial DPI-enabled firewall Tofino is one of the earliest firewall, designed for SCADA systems [112]. Nivethan et al. [113,114] proposed a Linux-based firewall for the DNP3 and Modbus protocol using the u32 byte-matching feature of the utilize Linux Iptables respectively. Li et al. [115] proposed a new SCADA firewall model, SCADAWall, using a comprehensive packet inspection technology and proprietary industrial protocols extension algorithm. The authors demonstrated that SCADAWall follows strict low-latency communication using the Metro SCADA system and Modbus protocol.

Researchers are creating testbeds for the SCADA systems to overcome the deficiency of well-validated datasets for the verification of IDSs. A brief survey of the testbeds is done in the next section.

Table 7
Testbed list.

Testbed	Technology used	Protocol	Type of Testbed	Attack simulated
A testbed for the gas-distribution system, water storage distribution and steel mining [116]	Communication between HMI and UART-based MTU over 900 MHz radio functioning as a repeater	DNP3, Modbus	Small-Scale Physical	DoS, response/ command injection attacks, and reconnaissance attack
An open-source low-cost ICS testbed [117].	Software : FreeRTOS, LwIP, OpenPLCv3, ScadaLTS, Logging, Custom, PyModbus. Hardware : STM32F7, Raspberry Pi 3, TP-Link, Fischertechnik	(HMI, PLC): based on TCP/IP, sensors: Modbus/TCP.	Small-Scale Physical	DDoS, MitM
A CPS testbed for Smart Grid [118]	Overcurrent relays, Opal-RT RTDS real-time digital simulator	DNP3, IEC61850	Small-Scale Physical	DoS, MitM
Industrial Control System (ICS) Security Testbed [119]	Electricity generation simulated using AC and DC motor pairs, PLCs and HMI.	EtherNet/IP	Small-Scale Physical	MitM, Local DNS poisoning
National SCADA Testbed [120]	Bolstered by various labs supporting more than twelve test sites with full-size devices like a power grid.	Not specified	Full-Scale Physical	Not specified
Cyber security backdrop [121]	MATLAB/Simulink based tool utilizing TrueTime.	Modbus/TCP	Virtual	DoS
TASSCS [122]	Opnet, Power World Simulation System and Automatic Software Protection System (ASPS).	Modbus	Virtual	Replay attack, MitM
VSSCADA [123]	iFix, MatrikonOPC, Power System Simulator for Engineering (PSS/E) software to simulate HMI, SCADA master control server, and power system respectively.	Modbus	Virtual	Not specified
ISAAC [124]	RTDS is used to simulate a powergrid utility. RSCAD, is used to build powersystem models for the simulator	IEC 61850, DNP3	Virtual	DoS
Water storage tank, Gas pipeline, Midstream oil terminal, Refrigerated liquefied petroleum gas pipeline testbed [125]	OpenPLC, Simulink/MATLAB, Hypervisor	DNP3	Virtual	Command injection, DoS
Testbed for cyber-power system setting [126]	Power system simulation and sub-station automation based on open platform communication client/server architecture.	DNP3	Virtual	Eavesdrop, modify packet
A HIL SCADA testbed [127]	Phasor measurement units synchronized with GPS reference signals	DNP3, Modbus	Hybrid	Not Specified
MSICST [128]	Combination of simulation software and actual hardware for each scenario	Modbus	Hybrid	Remote execution of arbitrary code and WannaCry
MATLAB based testbed [129]	MATLAB,Simulation packages such as OMNeT+, OPNET, and RINSE	Modbus	Hybrid	Worm attack
SCADA-SST [130]	OMNeT+ network simulator and INET framework	Modbus	Hybrid	DoS, DDoS

6. Testbeds for SCADA system

Many approaches are used for the implementation of SCADA systems. We review some of them in the context of vulnerability assessment of SCADA protocols and systems. The replication of a SCADA system can be physical, virtual, hybrid. Table 7 shows a analysis of testbeds reported in literature. Here, we studied different proposed testbeds based on the techniques used, the communication protocol used for simulating, the testbed type, and the replication strategy for the testbed.

A lot of theoretical security approaches have been presented in the last few years. However, the present research is still lacking a practical approach to [131]. Literature does not offer a remarkable number of ways to deal with CPS security because real empirical data for operational industrial is limited. NIST had also suggested a set of guidelines in carrying out security assessments on SCADA systems. However, the development of testbeds is an expensive process. These types of the event need substantial financial investments. Only some government-sponsored projects for testbed generation could afford such a vast investment [121]. Moreover, access to this testbed is restricted to the research community and academia. Thus, researchers focus on an inexpensive and flexible approach for the development of SCADA test tools.

We have categorized SCADA testbeds into three categories based on the replication strategy as discussed below.

6.1. Physical testbed

A physical testbed corresponds to the replicating the existing SCADA system and industrial utility. Therefore, it demonstrates an excellent representation of the reliable, exact physical system. The physical system's scalability and the cost is a great issue due to the need for hardware stacks. The physical testbed can be further divided based on the SCADA system's scalability, i.e., small-scale physical models and full-scale physical models.

The National SCADA Testbed (NSTB) [120] developed by the United States Department of Energy in Idaho National Labs is an example of full-scale physical models. It was designed for communication standards improvement. The maintenance of real hardware and software is a challenging task due to cyber-attacks. NSTB consists of a complex electrical grid with sixty-one miles, distribution lines of 13.8KV, a transmission loop of 128KV, and approximately three thousand points for monitoring. Many industrial protocols, e.g., internet protocol, GSM, ATM, MODBUS, DNP, are supported in NSTB. Apart from the communication network, it supports firewall and VPN testing. Yang et al. [132] proposed a testbed with SCADA software and communication infrastructure for investigating MitM attack using IEC 60870-5-103 protocol. The testbed have three windows based host to simulate the SCADA systems communication. Host A act as a MTU, host B as a protocol gateway and host C as a IED. Host A and B are connected using a switch. Sauer et al. in [117], presented an open-source low-cost ICS testbed. It enables researchers to get hands-on experience with industrial security testbed for about 500 Euro only. The authors demonstrated a real-world physical process controlled by an ICS. The communication between HMI, PLC is based on TCP/IP protocols to adhere to the industry 4.0 scenarios. However, the sensor's communication was done using Modbus/TCP. Morris et al. [116] presented a small-scale testbed for the gas-distribution system, water storage and steel making industry. The testbed support DNP3 and modbus protocols. The authors simulated DoS, response injections, and reconnaissance attack. Ashok et al. [118] presented a CPS testbed for CPS. In testbed, two substations are replicated as two overcurrent relays each connected to a single Opal-RT RTDS real-time digital simulator. Two software based RTUs that communicate through TCP/IP to a control unit connected to HMI and historian. The physical relay are connected to RTUs through IEC 61850 GOOSE protocol. RTUs are connected to the control centre using DNP3. The authros simulated DoS and Mitm on testbed. orkmaz et al. [119] presented a small-scale testbed for electricity generation. The testbed used real industrial equipment (PLCs, motors, generators, sensors, etc.). PLC used are Allen Bradley ControlLogix, and Allen Bradley Micro850PLC controller. The electricity generation process is simulated using AC and SC motor pairs. To control and monitor, HMI system uses the Proficy HMI/SCADA - iFIXsoftware. EtherNet/IP modules is used for the communication between controllers and HMI. The authors performed MitM, DoS, and DNS poisoning attacks on testbed.

6.2. Virtual testbed

The virtual testbed is developed to overcome the limitations of the software and physical testbed as it isolates activities in the test environment from the physical devices and the external components. It provides an abstraction between the software and hardware layer that provide an easy way to configure systems. Therefore, it is considered a controlled environment. TASSCS [122] falls in this category. It is developed by the NSF Center for Autonomic Computing, the University of Arizona. The testbed is built using power world simulation system, Opnet, and an automatic software protection system. To simulate the control networks, e.g., Modbus, Allen-Bradley data highway, TASSCS uses the Opnet tool, and to simulate the operation behavior, it uses the PowerWorldi simulation system. Simulation of detection of attack/ protection is done using autonomic software protection system. Farooqui et al. [121] have proposed a MATLAB based tool utilizing TrueTime. The proposed Power Cyber test setup brings together VPN devices, relays to protect against overcurrent, autotransformers, HMI, and RTU software modules.

VSSCADA [123], a power system testbed, virtualizes all the hardware components to maintain the actual behavior of all the components. A testbed is purely software-based on emulated communication, allowing the reconfigurability of virtual systems to simulate much real control and monitoring scenarios. VSSCADA supported Windows 7/Windows 8. It uses iFix, MatrikonOPC, power system simulator for engineering software to simulate HMI, SCADA master control server, and power system. SCADASim framework [133] developed at the Royal Melbourne Institute of Technology, Australia, is a software testbed. SCADASim uses OMNET++ to recreate SCADA components such as RTU, PLC, MTU, and communication protocols Modbus/TCP, DNP3. This can easily be scaled, integrated with other modules. It also proposes a gate concept, which is an interface between simulation and the external environment. SCADASim supports multiple gates at the same time. It can simulate the denial of service, MitM, eavesdropping, and spoofing attacks.

Oyewumi et al. in [124] introduced the design of ISAAC testbed under development at the University of Idaho. They designed ISAAC to be domain-independent, distributed, and reconfigurable. Alves et al. [125] proposed a modular, cost-efficient, and portable testbed to replicate sophisticated SCADA Systems on a virtual simulation. They also demonstrated their approach by simulating real-world critical infrastructures.

Hong et al. [126] presented a CPS testbed for power grid, consiting of two control centers, two substations and an external link to Iowa State university testbed. The control communicate to other controller using ICCP, and to substation using DNP3. The communications are done using SCADA and controller user interface. The testbed has three main parts: IED, user interface, and power system simulator. The authors simulated eavesdroping and packet modification attack.

6.3. Hybrid testbed

It is also called Hardware-In-the-Loop (HIL) testbed. In this approach, the physical part or the entire critical infrastructure can be replaced by a computer model. HIL usually involves connecting control devices with control components and data acquisition. The measurement of HIL is more realistic and cost-effective. HIL's measurement results, latencies, and communication patterns are more practical, reflecting the data present in the actual control system. Apart from this, vulnerability analysis, as well as behavior-based monitoring, is realizable in HIL. In this approach, replicating the SCADA system is done using simulated, virtualized, emulated, and physical devices. The main focus of the Hybrid testbed is to provide a testbed for the cyber-security purpose.

A hybrid testbed [127] is developed at the USF Smart Grid Power System lab. The testbed was constructed to test energy management schemes, power grid cyberattack detection, and prevention strategies. For visualization, it uses PI-system. Xu et al. in [128] presented the HIL ICS testbed Multiple-Scenario Industrial Control System Testbed (MSICST). The authors used a combination of simulation software and actual hardware to build the process scenario. MSICST can model thermal power plants, rail transit, intelligent manufacturing, and smart grid. An example of the Hybrid

Table 8
Testbed type analysis.

Type of Testbed	Advantages	Disadvantages	Examples
Physical Testbed	1. Highest Degree of Fidelity. 2. Excellent reliability.	1. Difficult to reconfigure and sustain real hardware and software. 2. Establishing a valid testbed is a costly operation. 3. Scalability is a big issue. 4. Poor repeatability.	[116], [117], [118], [119], [120],
Virtual Testbed	1. Secure from cyber-attacks as it enables a layer of abstraction between software and hardware. 2. Ease to develop and reconfigure. 3. Cost efficient and reliable 4. Good Scalability.	1. Incapable of reflecting the exact scenarios in the real SCADA systems due to the absence of real components and devices. 2. Low fidelity and reliability	[121], [122],[123], [124], [125], [126]
Hybrid testbed (Hardware-in-the-loop)	1.This approach enables the creation of a SCADA system using simulation, virtualization, emulation or simulation. 2. High degree of fidelity. 3. The communication pattern and latencies are more accurate. 4. Vulnerability analysis and behaviour- based analysis are more feasible then simulated testbed. 5. Provide cost cutting measure for the design and testing of a wide variety of systems.	1. Not cost efficient. 2. Scalability is a big issue.	[127], [128], [129], [130]

testbed is explained in [129]. In this testbed, a cyber-security scenario for the Modbus worm attack was implemented. The Hybrid SCADA system's architecture is divided into two-layer architecture, i.e., hybrid cyber layer and virtual physical layer, as shown. This two-layer can either be a real or simulated component. The hybrid test system's architecture consists of sub-units: item condenser, a recycle compressor, two-stage reactor, vapor/fluid separator, and product stripper.

Another example of hybrid SCADA testbed, i.e., SCADA-SST, is presented in [130] for smart-grid and water tanks control. The proposed testbed is scalable, lightweight, supports hybrid scenarios, and can be widely used in different SCADA systems. It also supports malicious nodes templates, network attack scenarios. It is specifically developed for SCADA security evaluation and testing using the OMNeT++ network simulator and INET framework. INET support the libraries needed to build communication network models. SCADA-SST components behavior is written in C++. It also supports the security analysis framework, e.g., signature for the malicious node, attack scenarios, capturing, and analysis of network traffic.

Table 8 shows the advantages and disadvantages of the various categories of testbeds. The physical testbed has the highest fidelity degree, but maintaining real hardware and software is a challenging task. It is also a costly operation. Virtual testbeds have the lowest degree of fidelity and reliability. However, they are easy to develop. Therefore, various factors such as fidelity, reliability, cost, and scalability issue should be considered to select the testbed type. Now, hybrid testbeds are preferred because they have good accuracy and cost-effective.

With the rapid advancement in technology, new technologies rapidly replace old techniques. In the next section, we will study the recent improvements, i.e., IoT based SCADA system.

7. IoT-based SCADA

The future Internet is considered as another game-changing idea for traditional SCADA frameworks. The current SCADA frameworks use a combination of characteristics of traditional and odern SCADA features, due to which their security is in greater danger. Generally, the SCADA system is inflexible, static, and follows centralized architecture. These weaknesses limit the SCADA system interoperability. Therefore, to overcome the existing SCADA limitation, a sensor IoT-based SCADA infrastructure has been proposed.

7.1. Architecture of IoT-based SCADA

A generic IoT-based architecture is discussed in Section 3.2.4. Alcaraz et al. [143] proposed VS-Cloud, a virtual SCADA architecture with primary focus on cloud storage. The SCADA system should offer dynamic sensing services management. It should allow dynamic creation and configuration of the provided services. The privacy of data should be provided. To ensure CIA requirements, the authors recommend searchable encryption, private information retrieval, digital signatures, proofs of storage, and anonymous routing (to provide anonymity to online communications) techniques. The proposed system should be scalable, fault-tolerant, interoperable, and energy-aware [144].

Khan et al. [136] proposed and validated a secure and seamless migration of legacy SCADA systems to the IoT-based SCADA. The authors observe minimal interruption to industrial functioning during migration to the cloud. The module includes two main components, i.e., Cloud Connectivity Kit (CCK) and cloud platform. CCK helps to have localized security for ICS security. It is attached to the SCADA components, e.g., PLC, RTU, actuator, sensor, etc. and provide an advanced firewall and VPN tunnel with VLAN segregation capability to secure the SCADA component connection. The approach is validated for time-critical systems, e.g., synchrophasor technology using the Amazon AWS cloud in the smart grid.

Kulik et al. [137] verified the compliance of cloud-connected SCADA systems with IEC-62443-3-3 standard. The system behavior and requirements of interest from IEC-62443-3-3 are formally defined using a labeled transition system. Their case-study considers authentication, malicious code protection, and data confidentiality (requirement 1.6, 3.2, 4.1, respectively) requirements from IEC-62443-3-3 to demonstrate the approach. An automated computing framework for IoT-based SCADA by combining the discrete knowledge-based approaches with cognitive approaches is proposed by Nazir et al. [138] by extending their work in [139]. The framework combines virtualization of computing and networking resources, a hierarchy of autonomic managers to identify threats at different scales, and reduce false alarms.

Ferrang et al. [140] classified the architecture of fog-based SCADA systems into four categories, i.e., the cloud layer, the for

layer, the end-device layer, and the SCADA layer. We can say that the integrated SCADA systems, an amalgamation of industrial business systems and the IoT, are more prone to attacks than the traditional SCADA due to the larger exposed space. Wei Ye and John Heidemann in [141] introduced a new IoT-based framework that is capable of virtualizing a wide range of sensing frameworks, comply new techniques for data processing, use cloud computing for managing a large amount of data collected from sensors. Baker et al. in [142] presented the implementation details of a prototype for a secure fog based platform. The performance evaluation results demonstrate the applicability of the proposed platform in realtime. These results can pave the way toward the development of a more secure and trusted SCADA based IoT critical infrastructure, which is essential to counter cyber threats against next eneration critical infrastructure and industrial control systems.

IoT provides interconnectivity among various real-time sensors and other intelligent electronic devices. A typical IoT application platform is used for data analysis, SCADA PLC, queries, reporting, remote terminal, process control, the web, cellular app, Historian, and monitoring. Therefore, it has become a tremendous development in the area of real-time industrial infrastructure. Industrial IoT is a new revolution in smart industrial sectors that provide enhanced automation and information sharing facilities manufacturing. It is a combination of cloud computing, cyber system, and connectivity. A smart industrial system based on the IoT system can predict the failure cases using the network devices.

7.2. Security concern of IoT-based SCADA

Real-time monitoring, Pay-per-use, licenses, cheaper capital, and operating expense are the advantages offered by cloud-service [134]. Cloud-service providers handle the maintenance, upgrade of these systems. Once they are upgraded, they are available to all users instantly. The main concern of cloud-SCADA is security and performance issues [135].

Tracking of hackers, information leakage, latency time, and privacy issue [145] reliability of the cloud servers should also be considered before shifting to cloud-SCADA. [146,147]. The communication link, relying on IoT-based communication, can suffer from the MitM attack, DoS attacks because the adversaries can still sniff, alter, or spoof the network's information. The reliance on cloud communication opens more back-doors to the SCADA systems and critical infrastructure. The traditional system's security risks will be carried forward due to the communication protocols used like Modbus/TCP, IEC 40, and DNP3, which are suffering from lack of protection. Moreover, these systems use commercial off-the-shelf solutions rather than the proprietary solution. The information communicated to the cloud is divided locally. The probe of system application running on the cloud can be done, and therefore, these can be attacked by the attacker.

The security and privacy issues associated with cloud services usage inhibit its adoption in critical infrastructures. The cloud-service provides should primarily focus on implementing countermeasures that can provide the visibility and control of data to its users [148]. The countermeasures can range from an authentication and authorization mechanism, encryption of stored data, privacy-preserving solutions, key management systems, etc.

Zhou et al. [157] proposed a DDoS mitigation approach by dividing the computation for traffic monitoring systems near the local devices using the Fog computing concept. However, the consolidating and coordination work that needs extensive computation is done at the cloud. The approach use firewall devices to filter the monitoring traffic using available signature packets. Therefore, to resolve the security and privacy concerns of cloud, fog computing-based solutions can be used. The data should be filtered before sending it to the cloud, followed by light-weight computation for security concern data that should be done at the fog.

Moreover, the industry system is searching for solutions that can provide fault tolerance, scalability, availability, and flexibility. One proposed solution is to integrate the CPS with IoT using cloud computing services. However, traditional SCADA systems cannot properly measure security parameters. The integration of traditional SCADA systems with IoT is more vulnerable to security threats. Therefore, these future concepts need more research efforts [145].

8. Future research directions

Even with the advanced security algorithm, a lot of attacks on the SCADA system have been detected. This section highlights the future research scope abridging the gap between SCADA's current state and an advanced, robust SCADA system.

8.1. Attacks database

The security incidents database is requiblue to analyze the various dimensions of attacks to develop strategies to prevent similar attacks in the future. Datasets KDD99 [79], NSS-KDD [80], DAPRA [81] are outdated and not synchronised with modern SCADA architecture. NVD dataset contains common vulnerabilities in all domains that fail to focus on SCADA specific vulnerabilities. Therefore, there is no proper database which has covered all security incidents. One global repository for all these incidents should be built. This repository should be publicly available to researchers to analyze these attacks. Industries should also report the attacks on their system rather than hiding it to save their image. Then only zero-day attacks can be handled.

8.2. IDSs for SCADA

We concluded that more research is required to define the performance metrics for the validation of IDSs. In most of the analysis, only attack discovery rates, false positive and false negative rates are provided. Time taken to detect the attack, an essential standard for performance measurement, is a missing parameter from current research. Therefore, even if it is guaranteed that IDSs will detect the attack and the latency is high, the attacker will have sufficient time to damage the system. We did not find any paper which compares the IDSs based on the placement of the detection system. Moreover, research work focuses on developing a detection system for specific attack types, i.e., MitM and DOS attack. Different attack detection schemes which are running under similar operational settings can be evaluated in further research.

However, Knowledge-based IDSs are still not capable of handling zero-day attacks. It is a challenging task to define acceptable behaviors upon environment change. The knowledge-based IDSs are not reliable for unknown attacks. Each attack's behavior differs from others, so the researcher should focus on identifying the attack model. Therefore researchers should make more effort to further refining the threshold monitoring techniques. These threshold models should be dynamic, which learns as per the severity of past attacks. The priority for IDSs should be eviction if the attacker is persistent, repairing if the attacker is transient, establishing attribution for the attack if the attacker is ineffective.

SCADA system security must be an overlap of computer security, communication network, and control engineering. IDSs should be able to record the features of a specific SCADA system, i.e., the versatility of the physical system, communication pattern, system architecture, etc. A new area of research can be alert post-processing for reducing false-positive alert and the development

of techniques for alert correlation. Multi-step intrusions techniques can be used to correlate isolated intrusions [158].

Moreover, not all intrusions can be prevented. The use of honeypots, is an attractive approach [159]. Shakarian et al. in [160] proposed a new and realistic approach to delay the impact of intrusion in-spite of stopping it. This will help to minimize the probability that the intrusion reached its goal by giving the target system more response time. These kinds of techniques integrated with SCADA IDSs can help to avoid catastrophic events.

8.3. Scalable testbeds & validation techniques

The development of testbeds is a costly process that needs a huge amount of funding. There is no such testbed that is cost-efficient, scalable, and have a high degree of fidelity. The researcher should focus on the scalable, higher degree of fidelity, cost-efficient, and interpolation solution. New communication protocols, new risk-assessments techniques, and IDS need to be validated before deploying directly to the field. There is an urgent requirement for trust-worthy validation approaches to assess the reliability of new techniques for the safety and security of SCADA systems. The government must invest in developing the physical testbeds for the critical infrastructures to analyze the security risks and test the security mechanisms.

8.4. New communication protocol

In communication protocols, the focus is needed on the application and network layer security. Network security protocols should be integrated into these communication protocols. Communication protocol for IoT-based SCADA, i.e., a reliable, secure, scalable, open, low latency communication protocol, is the researcher's new focus. With Industry 4.0 evolution, IoT protocols are used in the SCADA system. These protocols lack reliability, raising the need for reliable communication protocols. In the case of SCADA systems, network cryptographic solutions are not sufficient in blocking the attacks. There is still a need for extensive research for more robust cryptographic solutions, in-protocol authentication techniques, efficient key management scheme, distributed security mechanisms that apply to SCADA systems.

8.5. Safe and secure architecture and operating system

DOS, VMS, and UNIX operating systems, which have various vulnerabilities, were mostly used in SCADA. Now, Linux and Microsoft Windows-based operating systems have displaced DOS with UNIX based SCADA. However, Linux and Windows suffer from their vulnerabilities due to the large source code for operating systems. Microkernel architecture based operating systems can be used to reduce the attack surface for SCADA systems [161]. Apart from security, safety guidelines should always be followed to the maximum extent to avoid unacceptable risks. SCADA systems can be secured by utilizing a more error-resistant architecture, secure and robust operating system, and secure programming languages. Recently, Kaspersky launched a secure operating system for SCADA, which does not have traces of Linux [162,163]. Additionally, secure architectures for SCADA have been proposed recently[164,165]. The safety of CI is an important concern. Safety protocols need to be mandatory. With IoTization, the end-devices' safety is a big concern as these cheap devices are from different vendors, which rarely follow safety guidelines.

8.6. Research focus for IoT-based SCADA

The integration of IoT-cloud in the traditional SCADA system offers new vulnerabilities and opportunities to share data/information/services over the web. There is a dire need to grow new strategies that are fit for managing complex and large-scale frameworks. Research should be focused on continuously enhancing the security of these systems. In IoT-based system, bandwidth overload and latency are a big issue. These parameters are dependent on cloud service providers. Delay in decision making, i.e., latency delay, can cause a loss of production. So research should be focused on making this system robust. The high bandwidth and low latency providers should be encouraged. The potential of these systems is dependent on the cooperation among the responsible platforms.

To assure industries about these complex collaborations, more research is required. New development tools that can handle the complexity of service creation are needed. Apart from these, more productive and upgraded use of worldwide assets is needed. Sustainable development goals should also be considered in parallel to achieve robustness, scalability, reliability, real-time system. In IoT based system, a massive amount of data gets generated. Therefore, the security, analytics, storage, and complexity of this data are the principal concern.

8.7. Tuned predictive maintenance approaches for plant machines

The modern IoT based SCADA systems generate a large amount of data that can be leveraged for predicting the health of the plant machines by detecting early faults or threats. Predictive maintenance utilizes the sensed condition monitoring data to predict the future machine conditions followed by decisions upon this prediction. Kiangala et al. [166] proposed a predictive maintenance approach for predicting conveyor motor health in a bottling plant using a decentralized monitoring system by monitoring the vibration speed states. Similarly, Gigoni et al. [167] focus on a scalable predictive maintenance model, machine learning, and statistical process control tools. Researchers should focus on more tuned prediction detection approaches to timely detect system failures. It will enhance not only productivity but also reduces the safety risks.

8.8. Advanced approaches for supply-chain risk assessment

Since the inception of SCADA systems, the heterogeneity of SCADA components was always a concern for industries and consumers due to security, and incompatibility issues. Outsourcing the manufacturing of some parts of a system may be economical in terms of time and cost, but it has substantial security risks due to fabricated parts, hidden vulnerabilities, intentionally added loopholes, etc. Supply chain risks have grown in importance, yet it has received little attention from academics. Researchers should focus on a theoretical as well practical framework to mitigate the securing concern raised due to the anomalous supply chain. A public-private analytics exchange program report [168] focuses on man-made supply chain risks to SCADA systems and recommends risk mitigation strategies.

8.9. Advanced penetration testing approaches for SCADA

Penetration testing/ pen-testing/ ethical hacking is generally used to test a computer system, network or web application to seek security vulnerabilities that an attacker could exploit. Luswata et al. [169] studied possible attacks on the SCADA system by using penetration tools. Similarly, Hilal et al. [170], presented an approach to pentest SCADA system testbed using Kali Linux and data traffic analysis on SCADA network using Wireshark. State-of-the-art commercial penetration tools, i.e., Nessus, Netsparker, Idappcom, Acunetix, Probably, BackTrack, Metasploit and opensource tools, i.e., Wapiti, ZAP (Zed Attack Proxy), Vega, W3af may not be a

suitable choice for SCADA systems due to its different characteristic as compared to general IT systems. Yadav et al. [171] presented an E2E penetration testing approach IoT-PEN to discover all possible attackers way to breach the target system. IoT-Pen works in four stages, i.e., i) Pentesting initial setup installation. ii) Extracting current state information of each system. iii) Extract CPE info from a.xml file generated by Nmap. iv) Generation of prerequisites and post-conditions for all the reported vulnerabilities & Target-graph generation. v) Analysis of target-paths & Recommendations. The researchers should focus on novel techniques to detect zero-day vulnerabilities as most of the state-of-art approaches focus on identifying the already published vulnerabilities.

8.10. Need for timely updates to SCADA

The increased internet connectivity of SCADA systems to control and monitor geographically distributed systems has increased the attack surface. State-of-art SCADA are more vulnerable to the attacks. Yadav et al. in [56] observed that SCADA system vulnerabilities from NVD reveal that approximately 30% of the reported SCADA vulnerabilities belong to the critical severity group. Therefore, to avoid potential attacks, the SCADA systems need to be updated periodically and timely [172]. The patches must have been validated using rigorous testing, as SCADA systems can not bear any post-development consequences of the patches. The complex and interdependent architecture of SCADA systems causes timely patching a challenging task. Also, not all vulnerabilities are always exploited. Only 15% of the reported vulnerabilities are exploited [173]. Therefore, system administrators should focus on patch prioritization strategies to avoid potential attacks under resource constraints.

9. Conclusion

SCADA systems have evolved from a standalone system into sophisticated, complex open systems based on advanced technology systems connected to the Internet. SCADA systems are composed of hardware as well as software components, i.e., RTUs, MTU, HMI, historian. These components communicate with each other using wired and wireless industrial communication protocols. The modern communication protocols enable remote monitoring and controlling over geographically distributed SCADA systems. The new advancements have not only increased productivity and efficiency but also led the SCADA system more vulnerable to attacks. The buffer overflow and input invalidation are the most commonly exploited vulnerability in SCADA systems due to legacy softwares and upgrade restriction issues. Over the period, many attacks on SCADA industrial control system have been reported, e.g., Stuxnet, Maroochy, Operation Ghoul, Ukraine Power grid attack. The SCADA framework's smooth and genuine operation is one of the key concerns for enterprises because the consequences of breaking down the SCADA system may range from financial loss to environmental damange to loss of human life. The attackers mostly targeted the legacy communication protocols that are widely used, e.g., Modbus, DNP3, etc.

As per the RISI SCADA attack database analysis, the number of attacks on SCADA systems is increasing over time. RISI database has listed 48 attacks in the transporatation sector itself. United States industries have reported a maximum number of attacks. Most of the industries do not report cyber-attacks on their control system or SCADA for the sake of their reputation. Therefore, the completeness of the assessment depends on the completeness of the RISI database. The increasing trend and severity of attacks on SCADA systems raise an urgent need for securing SCADA systems. To timely detect the possible zero-day attack, the experts recommend penetration testing. There is a requirement of a responsive intrusion detection system that can alert the system managers about the possible attack on the system and network. These detection systems can use signature, specification, machine learning-based models for enhanced security. Moreover, the machine learning-based approaches assume that the training data is benign, that is not always true with the increase in adversarial learning algorithm [174]. The researcher should focus on developing defense mechanisms for adversarial learning before using machine learning approaches. There are many cryptographic approaches discussed in the research community. Still, we kept it out of scope for our review, as modern SCADA includes many resource constraint devices, which render the cryptographic solutions inappropriate. Since the security solution, e.g., IDS, patches are regressively tested before deployed on the SCADA systems due to the critical need of availability. The patches are generally tested on testbeds to analyze any post-deployment consequences. We divided the SCADA testbeds into three categories, i.e., physical, virtual, and hybrid. Hybrid testbeds provide a good balance between fidelity and cost.

In short, This paper gives a structured and multidimensional overview of SCADA systems' security. The major contributions of this paper are:-

1. It provides a novel approach to SCADA security by studying various security aspects.
2. A comprehensive analysis of the attacks on SCADA systems over the years is done.
3. A detailed and comparative analysis of state-of-the-art IDSs and SCADA testbeds.
4. Due to the IoTization SCADA, the research problems for secure SCADA has been widened. Therefore, a brief discussion about future research directions is done in Section 8.

This review indicates that despite many approaches present for IDS, and testbeds, there is still a lot of scope for further improvements. IDSs can be improved in sectors of placement policy, validation strategy, attack coverage, low latency, and low false-positive rate. Similarly, testbeds can be improved pertaining to cost, scalability, and high fidelity solution.

Apart from this, industries are currently shifting to IoT-based SCADA systems as they are economical and easily scalable. But IoT-based SCADA system is hampered by performance issues, i.e., high latency and low bandwidth. Therefore, there is a need to build viable and efficient system architectures and frameworks to model such issues. A large amount of data being generated in IoT-based SCADA that can be leverage for the security and safety of SCADA systems. The SCADA systems need to be up-to-date to avoid any security exploitation due to existing vulnerabailities. In short, SCADA systems are the foundation of critical infrastructure security, and their safety and security are critical issues for any nation.

Declaration of Competing Interest

We do not have any conflict of interest.

References

[1] P.M. Nasr, A.Y. Varjani, An alarm based access control model for SCADAsystem, in: Smart Grid Conference (SGC 2015), 2015, pp. 23–24, doi:10.1109/SGC.2015.7857424.
[2] A. Rezai, P. Keshavarzi, Z. Moravej, Key management issue in SCADA networks: a review, Eng. Sci. Technol.Int. J. 20 (August) (2016) 354–363, doi:10.1016/j.jestch.2016.08.011.
[3] S. Papa, W. Casper, T. Moore, Securing wastewater facilities from accidental and intentional harm: a cost-benefit analysis, Int. J. Crit. Infrastruct.Prot. 6 (2) (2013) 96–106, doi:10.1016/j.ijcip.2013.05.002.
[4] B. Miller, D. Rowe, A survey SCADA of and critical infrastructure incidents, in: Proceedings of the 1st Annual Conference on Research in Information Technology, in: RIIT '12, ACM, New York, NY, USA, 2012, pp. 51–56, doi:10.1145/2380790.2380805.

[5] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart, A review of cyber security risk assessment methods for SCADA systems, Comput. Secur. 56 (2016) 1–27, doi:10.1016/j.cose.2015.09.009.
[6] N.H. Pathak, Modern SCADA systems, Int. J. Eng. Dev. Res. 2 (2) (2014) 1693–1699.
[7] Edvard, 3 generations of SCADA system architectures you should know about, 2013, http://electrical-engineering-portal.com/three-generations-of-scada-system-architectures
[8] Watelectronics, Know all about SCADA systems architecture and types with applications, 2017, https://www.watelectronics.com/scada-system-architecture-types-applications/.
[9] C. Feng, V.R. Palleti, A. Mathur, D. Chana, A systematic framework to generate invariants for anomaly detection in industrial control systems, 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24–27, 2019, 2019.
[10] X. Lyu, Safety and security risk assessment in cyber-physical systems, IET Cyber-Phys. Syst. 4 (2019) 221–232(11).
[11] Z. Zhang, Data mining approaches for intelligent condition-based maintenance: a framework of intelligent fault diagnosis and prognosis system (IFDPS), 2014.
[12] M. Uzair, Communication methods (protocols, format & language) for the substation automation & control, http://www.eng.uwo.ca/people/tsidhu/Documents/project%20report%20Uzair.pdf.
[13] T. Sheldon, McGraw-Hill's Encyclopedia of Networking and Telecommunications, McGraw-Hill Professional, 2001.
[14] W. software development, Modbus protocol, 2004–2017, http://wingpath.co.uk/modbus/modbus_protocol.php.
[15] B+B SmartWorx, What is modbus?, 2016, https://www.bb-elec.com/Learning-Center/All-White-Papers/Modbus/The-Answer-to-the-14-Most-Frequently-Asked-Modbus.aspx.
[16] A. Shahzad, S. Musa, A. Aborujilah, M. Irfan, The SCADA review: System components, architecture, protocols and future security trends, Am. J. Appl. Sci. 11 (8) (2014) 1418–1425, doi:10.3844/ajassp.2014.1418.1425.
[17] K.C. Mahapatra, S. Magesh, Analysis of vulnerabilities in the protocols used in SCADA systems, Int. J. Adv. Res.Comput. Eng. Technol. 4 (3) (2015).
[18] Y. Lu, T. Feng, Cryptography security designs and enhancements of dnp3-sa protocol based on trusted computing., IJ Netw. Secur. 21 (1) (2019) 130–136.
[19] M. Marian, A. Cusman, F. Stng, D. Ionic, D. Popescu, Experimenting with digital signatures over a dnp3 protocol in a multitenant cloud-based SCADA architecture, IEEE Access 8 (2020) 156484–156503.
[20] IPCOMM, IEC 60870-5-102, 2004–2017,
[21] R. Czechowski, P. Wicher, B. Wiecha, Cyber security in communication of SCADA systems using IEC 61850, in: 2015 Modern Electric Power Systems (MEPS), 2015, pp. 1–7.
[22] P. Xin, IEC 61850 testing and documentation, 2010,https://www.theseus.fi/bitstream/handle/10024/17035/Peng_Xin.pdf.
[23] Wikipedia, IEC 61850, 2018, https://en.wikipedia.org/wiki/IEC_61850.
[24] Y. Yang, H.Q. Xu, L. Gao, Y.B. Yuan, K. McLaughlin, S. Sezer, Multidimensional intrusion detection system for IEC61850-based SCADA networks, IEEE Trans. Power Deliv. 32 (2) (2017) 1068–1078, doi:10.1109/TPWRD.2016.2603339.
[25] M.K. Choi, R.J. Robles, Z. Vale, C. Ramos, H. Ko, G. Marreiros, Utilization of different encryption schemes for securing SCADA component communication, Information 16 (2 B) (2013) 1503–1508.
[26] U. Perera, Comparisons of SCADA communication protocols for power systems, 2015, https://www.linkedin.com/pulse/comparisons-scada-protocols-power-systems-udara-perera.
[27] P. Sethi, S.R. Sarangi, Internet of things: architectures, protocols, and applications, J. Electr. Comput. Eng. 2017 (2017) 9324035:1–9324035:25.
[28] H. Kim, Security and vulnerability of SCADA systems over ip-based wireless sensor networks, Int. J. Distrib. Sens.Netw. 8 (11) (2012) 268478, doi:10.1155/2012/268478.
[29] J.D. Markovic-Petrovic, M.D. Stojanovic, Analysis of SCADA system vulnerabilities to DDOSattacks, in: 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 02, 2013, pp. 591–594, doi:10.1109/TELSKS.2013.6704448.
[30] T. Yardley, SCADA: issues, vulnerabilities, and future directions, 2008, https://www.usenix.org/system/files/login/articles/258-yardley.pdf.
[31] W.Colitti, K.Steenhaut, N.DeCaro, B.Buta, V.Dobrota, Evaluation of constrained application protocol for wirelesssensor networks (2011).
[32] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (coap)(2014).
[33] P. Sethi, S.R. Sarangi, Mq telemetry transport (mqtt) v3. 1 protocolspecification (2010).
[34] N. Falliere, L.O. Murchu, E. Chien, W32.stuxnet dossier, Symantec-Security Response Version 1. (February 2011) (2011) 1–69. 20 September 2015
[35] J. Slay, M. Miller, Lessons learned from the maroochy water breach, IFIP Int. Feder. Inf.Process. 253 (2007) 73–82, doi:10.1007/978-0-387-75462-8_6.
[36] M.H. Schwarz, J. Brcsk, A survey on OPC and OPC-UA: About the standard, developments and investigations, in: 2013 XXIV International Conference on Information, Communication and Automation Technologies (ICAT), 2013, pp. 1–6, doi:10.1109/ICAT.2013.6684065.
[37] Interoperability between OPC UA and automationml, Procedia CIRP 25 (2014) 297–304 8th International Conference on Digital Enterprise Technology - DET 2014 Disruptive Innovation in Manufacturing Engineering towards the 4th Industrial Revolution, doi:10.1016/j.procir.2014.10.042.
[38] R. Sindhu, J. Mathew, L.R. Sreedhanya, C.S. Lajitha, Design of hart compliant analog input module for indigenous SCADA system, in: 2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2017, pp. 1–6, doi:10.1109/SPICES.2017.8091345.
[39] P. Pongpipatpakdee, T. Thepmanee, S. Pongswatd, A. Rerkratn, Integration of wireless hart network system into SCADA software for operation management, in: 2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), 2016, pp. 549–554, doi:10.1109/SICE.2016.7749200.
[40] R.H. McClanahan, The benefits of networked SCADA systems utilizing ip-enabled networks, in: 2002 Rural Electric Power Conference. Papers Presented at the 46th Annual Conference (Cat. No. 02CH37360), 2002, pp. C5–1, doi:10.1109/REPCON.2002.1002297.
[41] I. Stoian, E. Stancel, S. Ignat, S. Balogh, O. Dancea, Federative SCADA consideration, in: 2010 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 3, 2010, pp. 1–6, doi:10.1109/AQTR.2010.5520682.
[42] B. Chen, N. Pattanaik, A. Goulart, K.L. Butler-purry, D. Kundur, Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed, in: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), 2015, pp. 1–6, doi:10.1109/CQR.2015.7129084.
[43] D.S. Pidikiti, R. Kalluri, R.K.S. Kumar, B.S. Bindhumadhava, SCADA communication protocols: vulnerabilities, attacks and possible mitigations, CSI Trans. ICT 1 (2) (2013) 135–141, doi:10.1007/s40012-013-0013-5.
[44] S. East, J. Butts, M. Papa, S. Shenoi, A taxonomy of attacks on the dnp3 protocol, in: C. Palmer, S. Shenoi (Eds.), Critical Infrastructure Protection III, Springer, Berlin, Heidelberg, 2009, pp. 67–81.
[45] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, E. Panaousis, Attacking IEC-60870-5-104 SCADA systems, in: 2019 IEEE World Congress on Services (SERVICES), 2642-939X, 2019, pp. 41–46, doi:10.1109/SERVICES.2019.00022.
[46] A. Elgargouri, M. Elmusrati, Analysis of cyber-attacks on IEC 61850 networks, in: 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT), 2017, pp. 1–4, doi:10.1109/ICAICT.2017.8686894.
[47] RISI, Risi online incident database, 2015, http://www.risidata.com/Database.
[48] R.J. Robles, M. kyu Choi, E. suk Cho, S. soo Kim, G.-c. P, S.-S. Yeo, Vulnerabilities in SCADA and critical infrastructure systems, Int. J. Future Gener. Commun. Netw. 1 (1) (2008) 99–104.
[49] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, Taxonomy for description of cross-domain attacks on CPS, in: Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems, in: HiCoNS '13, ACM, New York, NY, USA, 2013, pp. 135–142, doi:10.1145/2461446.2461465.
[50] T.M. Chen, S. Abu-Nimeh, Lessons from stuxnet, Computer 44 (4) (2011) 91–93, doi:10.1109/MC.2011.115.
[51] R. Langner, Stuxnet: dissecting a cyberwarfare weapon, IEEE Secur. Privacy 9 (3) (2011) 49–51, doi:10.1109/MSP.2011.67.
[52] R.M. Lee, M.J. Assante, T. Conway, German steel mill cyber attack, Ind. Control Syst. (2014) 1–15.
[53] S. Trisal, 3 cyber attacks that rocked industrial control systems, 2017, https://cyware.com/news/3-cyber-attacks-that-rocked-industrial-control-systems-817fee48.
[54] D. Bisson, 3 ICS security incidents that rocked 2016 and what we should learn from them, 2016, https://www.tripwire.com/state-of-security/ics-security/3-ics-security-incidents-rocked-2016-learn/.
[55] I.T. Laboratory, National vulnerability database, https://nvd.nist.gov/general.
[56] G. Yadav, K. Paul, Assessment of SCADA system vulnerabilities, in: 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1737–1744.
[57] M. Henrie, Cyber security risk management in the SCADA critical infrastructure environment, Eng. Manag. J. 25 (2) (2013) 38–45, doi:10.1080/10429247.2013.11431973.
[58] R.I. Ogie, R. I., Cyber security incidents on critical infrastructure and industrial networks, in: Proceedings of the 9th International Conference on Computer and Automation Engineering - ICCAE '17, 2017, pp. 254–258, doi:10.1145/3057039.3057076.
[59] D. Upadhyay, S. Sampalli, SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations, Comput. Secur. 89 (2020) 101666, doi:10.1016/j.cose.2019.101666.
[60] E. Luiijf, M. Ali, A. Zielstra, Assessing and improving SCADA security in the dutch drinking water sector, Int. J. Crit. Infrastruct.Prot. 4 (3) (2011) 124–134, doi:10.1016/j.ijcip.2011.08.002.
[61] C.-R. Chen, C.-J. Chang, C.-H. Lee, A time-driven and event-driven approach for substation feeder incident analysis, Int. J. Electr. Power Energy Syst. 74 (2016) 9–15, doi:10.1016/j.ijepes.2015.07.017.
[62] H. Alshawish, A. de Meer, Risk mitigation in electric power systems: where to start? Energy Inform. 2 (1) (2019) 34.
[63] G.D. Gonzalez Granadillo, J. Garcia-Alfaro, E.Y. Alvarez Lopez, M. El Barbori, H. Debar, Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the rori index, Comput. Electr. Eng. 47 (2015) 13–34.
[64] G. Yadav, P. K., Patchrank: ordering updates for SCADA systems, in: 2019 24th IEEE ETFA, 2019, pp. 110–117, doi:10.1109/ETFA.2019.8869110.
[65] G. Yadav, P. Gauravaram, A.K. Jindal, Smartpatch: a patch prioritization frame-

work for SCADA chain in smart grid, MobiCom '20, Association for Computing Machinery, New York, NY, USA, 2020, doi:10.1145/3372224.3418162.
[66] A.A. Cárdenas, S. Amin, S. Sastry, Research challenges for the security of control systems, in: Proceedings of the 3rd Conference on Hot Topics in Security, in: HOTSEC'08, USENIX Association, Berkeley, CA, USA, 2008, pp. 6:1–6:6.
[67] C. Neuman, Challenges in security for cyber-physical systems, in: Workshop on Future Directions in Cyber-physical Systems Security, 2009, pp. 1–4.
[68] A.C.F. Chan, J. Zhou, On smart grid cybersecurity standardization: issues of designing with nistir 7628, IEEE Commun. Mag. 51 (1) (2013) 58–65, doi:10.1109/MCOM.2013.6400439.
[69] C. Schuett, J. Butts, S. Dunlap, An evaluation of modification attacks on programmable logic controllers, Int. J. Crit. Infrastruct.Prot. 7 (1) (2014) 61–68, doi:10.1016/j.ijcip.2014.01.004.
[70] Z. Basnight, J. Butts, J. Lopez, T. Dube, Firmware modification attacks on programmable logic controllers, Int. J. Crit. Infrastruct.Prot. 6 (2) (2013) 76–84, doi:10.1016/j.ijcip.2013.04.004.
[71] R. Zhu, B. Zhang, J. Mao, Q. Zhang, Y. an Tan, A methodology for determining the image base of arm-based industrial control system firmware, Int. J. Crit. Infrastruct.Prot. 16 (2017) 26–35, doi:10.1016/j.ijcip.2016.12.002.
[72] NIST, National institute of standards and technology, 2017, https://www.nist.gov/.
[73] I. Garitano, R. Uribeetxeberria, U. Zurutuza, A review of SCADA anomaly detection systems, in: E. Corchado, V. Snášel, J. Sedano, A.E. Hassanien, J.L. Calvo, D. Ślęzak (Eds.), Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 357–366.
[74] A. Singhal, S. Jajodia, Data Mining for Intrusion Detection, Springer, Boston, US, MA, pp. 1171–1180. 10.1007/978-0-387-09823-4_61
[75] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E.G. Im, B. Pranggono, H.F. Wang, Multiattribute SCADA-specific intrusion detection system for power networks, IEEE Trans. Power Deliv. 29 (3) (2014) 1092–1102, doi:10.1109/TPWRD.2014.2300099.
[76] U. Adhikari, S. Pan, T. Morris, Industrial control system (ICS) cyber attack datasets, 2014, https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.
[77] J.M. Beaver, R.C. Borges-Hink, M.A. Buckner, Industrial control system (ICS) cyber attack datasets, 2013a, https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.
[78] J.M. Beaver, R.C. Borges-Hink, M.A. Buckner, An evaluation of machine learning methods to detect malicious SCADA communications, in: Machine Learning and Applications (ICMLA), 2013 12th International Conference on, 2, IEEE, 2013, pp. 54–59.
[79] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, A detailed analysis of the KDD cup 99 data set, in: Proceedings of the Second IEEE International Conference on Computational Intelligence for Security and Defense Applications, in: CISDA'09, IEEE Press, Piscataway, NJ, USA, 2009, pp. 53–58.
[80] A. Ozqur, H. Erdem, A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015, PeerJ PrePrints 4 (2016) e1954.
[81] L. Laboratory, Darpa intrusion detection evaluation dataset, https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset.
[82] N.R. Rodofile, K. Radke, E. Foo, Framework for SCADA cyber-attack dataset creation, in: Proceedings of the Australasian Computer Science Week Multiconference, in: ACSW '17, ACM, New York, NY, USA, 2017, pp. 69:1–69:10, doi:10.1145/3014812.3014883.
[83] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, H.F. Wang, Impact of cyber-security issues on smart grid, in: 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, 2011, pp. 1–7, doi:10.1109/ISGTEurope.2011.6162722.
[84] R. Mitchell, I.-R. Chen, A survey of intrusion detection techniques for cyber-physical systems, ACM Comput. Surv. 46 (4) (2014) 55:1–55:29, doi:10.1145/2542049.
[85] T. Shekari, C. Bayens, M. Cohen, L. Graber, R. Beyah, RFDIDS: radio frequency-based distributed intrusion detection system for the power grid, 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24–27, 2019, 2019.
[86] R. Flosbach, J. Chromik, A. Remke, Architecture and prototype implementation for process-aware intrusion detection in electrical grids, in: 38th International Symposium on Reliable Distributed Systems 2019, SRDS 2019; Conference date: 01-10-2019 Through 04-10-2019, 2019.
[87] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A. Karypidis, A. Sarigiannidis, Diderot: an intrusion detection and prevention system for dnp3-based SCADA systems, in: Proceedings of the 15th International Conference on Availability, Reliability and Security, in: ARES '20, Association for Computing Machinery, New York, NY, USA, 2020, doi:10.1145/3407023.3409314.
[88] P. Oman, M. Phillips, Intrusion Detection and Event Monitoring in SCADA Networks, Springer, Boston, US, MA, pp. 161–173. 10.1007/978-0-387-75462-8_12
[89] Y. Yang, K. Mclaughlin, T. Littler, S. Sezer, H. F. Wang, Rule-based intrusion detection system for, SCADA networks (2013), doi:10.1049/cp.2013.1729.
[90] B. Genge, F. Graur, P. Haller, Experimental assessment of network design approaches for protecting industrial control systems, Int. J. Crit. Infrastruct.Prot. 11 (2015) 24–38, doi:10.1016/j.ijcip.2015.07.005.
[91] P. Düssel, C. Gehl, P. Laskov, J.-U. Bußer, C. Störmann, J. Kästner, Cyber-Critical Infrastructure Protection Using Real-Time Payload-Based Anomaly Detection, Springer, Berlin, Heidelberg, pp. 85–97. 10.1007/978-3-642-14379-3_8
[92] H. Lahza, K. Radke, E. Foo, Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the goose and mms protocols, Int. J. Crit. Infrastruct.Prot. 20 (2018) 48–67, doi:10.1016/j.ijcip.2017.12.002.
[93] J. Gao, L. Gan, F. Buschendorf, L. Zhang, H. Liu, P. Li, X. Dong, T. Lu, Omni SCADA intrusion detection using deep learning algorithms, IEEE Internet Things J. (2020) 1.
[94] L. da Silva, D. Coury, Network traffic prediction for detecting DDOS attacks in IEC 61850 communication networks, Comput. Electr. Eng. 87 (2020) 106793, doi:10.1016/j.compeleceng.2020.106793.
[95] I.A. Khan, D. Pi, Z.U. Khan, Y. Hussain, A. Nawaz, Hml-ids: a hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems, IEEE Access 7 (2019) 89507–89521.
[96] H. Yang, L. Cheng, M.C. Chuah, Deep-learning-based network intrusion detection for SCADA systems, in: 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1–7, doi:10.1109/CNS.2019.8802785.
[97] R.L. Perez, F. Adamsky, R. Soua, T. Engel, Forget the myth of the air gap: Machine learning for reliable intrusion detection in SCADA systems, EAI Endorsed Trans. Secur. Saf. 6 (2019) e3.
[98] M. Kravchik, A. Shabtai, Detecting cyber attacks in industrial control systems using convolutional neural networks, in: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, in: CPS-SPC '18, ACM, New York, NY, USA, 2018, pp. 72–83, doi:10.1145/3264888.3264896.
[99] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. Alghamdi, A.Y. Zomaya, An efficient data-driven clustering technique to detect attacks in SCADA systems, IEEE Trans. Inf. Forensics Secur. 11 (5) (2016) 893–906, doi:10.1109/TIFS.2015.2512522.
[100] J. Bigham, D. Gamez, N. Lu, Safeguarding SCADA Systems with Anomaly Detection, Springer, Berlin, Heidelberg, pp. 171–182. 10.1007/978-3-540-45215-7_14
[101] A. Valdes, S. Cheung, Communication pattern anomaly detection in process control systems, in: 2009 IEEE Conference on Technologies for Homeland Security, 2009, pp. 22–29, doi:10.1109/THS.2009.5168010.
[102] O. Linda, T. Vollmer, M. Manic, Neural network based intrusion detection system for critical infrastructures, Int. Jt. Conf. Neural Netw. (2009) 1827–1834, doi:10.1109/IJCNN.2009.5178592.
[103] J.L. Rrushi, Composite Intrusion Detection in Process Control Networks Composite Intrusion Detection in Process Control Networks, The University of Milan, 2008 Ph.D. thesis.
[104] D. Yang, A. Usynin, J. Hines, Anomaly-based intrusion detection for SCADA systems, in: 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC and HMIT 05), 2005, pp. 12–16.
[105] D. Krauß, C. Thomalla, Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures, in: 2016 6th International Conference on Digital Information and Communication Technology and Its Applications, DICTAP 2016, 2016, pp. 70–73, doi:10.1109/DICTAP.2016.7544003.
[106] N. Goldenberg, A. Wool, Accurate modeling of modbus/TCP for intrusion detection in SCADA systems, Int. J. Crit. Infrastruct.Prot. 6 (2) (2013) 63–75, doi:10.1016/j.ijcip.2013.05.001.
[107] N. Cuppens-Boulahia, F. Cuppens, J.E. Lopez de Vergara, E. Vázquez, J. Guerra, H. Debar, An ontology-based approach to react to network attacks, in: Proceedings 2008 3rd International Conference on Risks and Security of Internet and Systems, CRiSIS 2008, 2008, pp. 27–35, doi:10.1109/CRISIS.2008.4757461.
[108] S. D'Antonio, F. Oliviero, R. Setola, High-Speed Intrusion Detection in Support of Critical Infrastructure Protection, , Berlin, Heidelberg, pp. 222–234. 10.1007/11962977_18
[109] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, S. Smith, Intrusion detection for resource-constrained embedded control systems in the power grid, Int. J. Crit. Infrastruct.Prot. 5 (2) (2012) 74–83, doi:10.1016/j.ijcip.2012.02.002.
[110] J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, S. Smith, Lightweight intrusion detection for resource-constrained embedded control systems, in: J. Butts, S. Shenoi (Eds.), Critical Infrastructure Protection V, Springer, Berlin, Heidelberg, 2011, pp. 31–46.
[111] S. Parthasarathy, D. Kundur, Bloom filter based intrusion detection for smart grid SCADA, in: 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2012, pp. 1–6, doi:10.1109/CCECE.2012.6334816.
[112] E. Byres, Understanding Deep Packet Inspection for SCADA Security, 12, White paper Tofino Security, 2012, p. 2012.
[113] J. Nivethan, M. Papa, A linux-based firewall for the dnp3 protocol, in: 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1–5.
[114] J. Nivethan, M. Papa, On the use of open-source firewalls in ICS/SCADA systems, Inf. Secur. J. 25 (1–3) (2016) 83–93, doi:10.1080/19393555.2016.1172283.
[115] D. Li, H. Guo, J. Zhou, L. Zhou, J.W. Wong, SCADAwall: a CPI-enabled firewall model for SCADA security, Comput. Secur. 80 (2019) 134–154, doi:10.1016/j.cose.2018.10.002.
[116] T. Morris, R. Vaughn, Y.S. Dandass, A testbed for SCADA control system cybersecurity research and pedagogy, in: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research – CSIIRW '11, 2011, p. 1, doi:10.1145/2179298.2179327.
[117] F. Sauer, M. Niedermaier, S. Kieling, D. Merli, Licster a low-cost ICS security testbed for education and research (2019). 10.14236/ewic/icscsr19.1
[118] A. Ashok, A. Hahn, M. Govindarasu, A cyber-physical security testbed for smart grid: System architecture and studies, in: Proceedings of the Seventh

Annual Workshop on Cyber Security and Information Intelligence Research, ACM, 2011, p. 20.
[119] M.D. Emrah korkmaz, A. Dolikh, V. Skormin, Industrial control system security testbed, in: Proceedings of Annual Symposium on Information Assurance, 2016.
[120] NSTB, National SCADA testbed –fact sheet, U.S. department of energy, 2009, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf.
[121] A.A. Farooqui, S.S.H. Zaidi, A.Y. Memon, S. Qazi, Cyber security backdrop: a SCADA testbed, in: Proceedings - 2014 IEEE Computers, Communications and IT Applications Conference, ComComAp 2014, 2014, pp. 98–103, doi:10.1109/ComComAp.2014.7017178.
[122] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, S. Hariri, A testbed for analyzing security of SCADA control systems (tasscs), in: IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe, 2011, pp. 1–7, doi:10.1109/ISGT.2011.5759169.
[123] A. Dayal, A. Tbaileh, S. Shukla, VSCADA: a reconfigurable virtual SCADA testbed for simulating power utility control center operations, in: 2015 IEEE Power Energy Society General Meeting, 2015, pp. 1–5, doi:10.1109/PESGM.2015.7285822.
[124] I.A. Oyewumi, A.A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B.K. Johnson, Y. Chakhchoukh, M.A. Haney, F.T. Sheldon, D.C. de Leon, Isaac: the idaho CPS smart grid cybersecurity testbed, in: 2019 IEEE Texas Power and Energy Conference (TPEC), 2019, pp. 1–6, doi:10.1109/TPEC.2019.8662189.
[125] T. Alves, R. Das, A. Werth, T. Morris, Virtualization of SCADA testbeds for cybersecurity research: a modular approach, Comput. Secur. 77 (2018) 531–546, doi:10.1016/j.cose.2018.05.002.
[126] J. Hong, S.S. Wu, A. Stefanov, A. Fshosha, C.C. Liu, P. Gladyshev, M. Govindarasu, An intrusion and defense testbed in a cyber-power system environment, IEEE Power Energy Soc. Gen. Meet. (July) (2011), doi:10.1109/PES.2011.6039375.
[127] H.G. Aghamolki, Z. Miao, L. Fan, A hardware-in-the-loop SCADA testbed, in: 2015 North American Power Symposium, NAPS 2015, 2015, pp. 1–6, doi:10.1109/NAPS.2015.7335093.
[128] W. Xu, Y. Tao, C. Yang, H. Chen, Msicst: multiple-scenario industrial control system testbed for security research, Comput. Mater. Continua 58 (2019) 691–705, doi:10.32604/cmc.2019.05678.
[129] D. Chen, Y. Peng, H. Wang, Development of a testbed for process control system cybersecurity research, in: Proceedings of the 3rd International Conference on Electric and Electronics, 2013, pp. 158–161, doi:10.2991/eeic-13.2013.37.
[130] A. Ghaleb, S. Zhioua, A. Almulhem, SCADA-sst: a SCADA security testbed, Wcicss (2016) 34–39, doi:10.1109/WCICSS.2016.7882610.
[131] E. Bou-Harb, Passive inference of attacks on SCADA communication protocols, in: 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1–6, doi:10.1109/ICC.2016.7510609.
[132] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E.G. Im, Z.Q. Yao, B. Pranggono, H.F. Wang, Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems, in: International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), 2012, pp. 1–8, doi:10.1049/cp.2012.1831.
[133] Q. Qassim, N. Jamil, I.Z. Abidin, M.E. Rusli, S. Yussof, R. Ismail, F. Abdullah, N. Ja, H.C. Hasan, M. Daud, A survey of SCADA testbed implementation approaches, Indian J. Sci. Technol. 10 (July) (2017), doi:10.17485/ijst/2017/v10i26/116775.
[134] S. Dustdar, Cloud computing, Computer 49 (2) (2016) 12–13, doi:10.1109/MC.2016.46.
[135] E. Daalder, B.D. Manager, SCADA Cloud Computing, Technical Report, Yokogawa Electric Corporation Global SCADA Center
[136] R. Khan, K. McLaughlin, B. Kang, D. Laverty, S. Sezer, A seamless cloud migration approach to secure distributed legacy industrial SCADA systems, in: 2020 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2020, pp. 1–5.
[137] T. Kulik, P.W.V. Tran-Jrgensen, J. Boudjadar, Compliance verification of a cyber security standard for cloud-connected SCADA, in: 2019 Global IoT Summit (GIoTS), 2019, pp. 1–6.
[138] S. Nazir, S. Patel, D. Patel, Cloud-Based Autonomic Computing Framework for Securing SCADA Systems, pp. 276–297. 10.4018/978-1-7998-3038-2.ch013
[139] S. Patel, D. Patel, S. Nazir, Autonomic computing architecture for SCADA cyber security, Int. J. Cognit. Inform. Nat. Intell. 11 (4) (2017) 66–79, doi:10.4018/IJCINI.2017100104.
[140] M.A. Ferrag, M. Babaghayou, M.A. Yazici, Cyber security for fog-based smart grid SCADA systems: solutions and challenges, J. Inform. Secur. Appl. 52 (2020) 102500, doi:10.1016/j.jisa.2020.102500.
[141] W. Ye, J. Heidemann, Enabling interoperability and extensibility of future 'SCADA' systems, in: Proceedings of the National Workshop on Beyond 'SCADA': Networked Embedded Control for Cyber Physical Systems, 2006. Pittsburgh, PA, USA
[142] T. Baker, M. Asim, Á. MacDermott, F. Iqbal, F. Kamoun, B. Shah, O. Alfandi, M. Hammoudeh, A secure fog-based platform for SCADA-based IoTcritical infrastructure, Software 50 (5) (2020) 503–518, doi:10.1002/spe.2688.
[143] C. Alcaraz, I. Agudo, D. Nuñez, J. Lopez, Managing incidents in smart grids ala Cloud, in: Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, 2011, pp. 527–531, doi:10.1109/Com.2011.79.
[144] Y. Ben Dhief, Y. Djemaiel, S. Rekhis, N. Boudriga, A novel sensor cloud based SCADA infrastructure for monitoring and attack prevention, in: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, in: MoMM '16, ACM, New York, NY, USA, 2016, pp. 45–49, doi:10.1145/3007120.3007169.
[145] A. Sajid, H. Abbas, K. Saleem, Cloud-assisted IoT-based SCADA systems security: areview of the state of the art and future challenges, IEEE Special Section on the Plethora of Research in Internet of Things (IoT), 4, 2016, doi:10.1109/ACCESS.2016.2549047.
[146] I. Automation, Cloud computing for SCADA, 2011, http://www.controlglobal.com/assets/11WPpdf/111202-inductiveautomation-cloud.pdf.
[147] P. Church, H. Mueller, C. Ryan, S.V. Gogouvitis, A. Goscinski, Z. Tari, Migration of a SCADA system to IAAS clouds – a case study, J. Cloud Comput. 6 (1) (2017) 11, doi:10.1186/s13677-017-0080-5.
[148] R. Kumar, R. Goyal, On cloud security requirements, threats, vulnerabilities and countermeasures: a survey, Comput. Sci. Rev. 33 (2019) 1–48, doi:10.1016/j.cosrev.2019.05.002.
[149] S.V.B. Rakas, M.D. Stojanovic, J.D. Marković-Petrović, A review of research work on network-based SCADA intrusion detection systems, IEEE Access 8 (2020) 93083–93108.
[150] J. Suaboot, A. Fahad, Z. Tari, J. Grundy, A.N. Mahmood, A. Almalawi, A.Y. Zomaya, K. Drira, A taxonomy of supervised learning for idss in SCADA environments, ACM Comput. Surv. 53 (2) (2020), doi:10.1145/3379499.
[151] S. Nazir, S. Patel, D. Patel, Assessing and augmenting SCADA cyber security: A survey of techniques, Comput. Secur. 70 (2017) 436–454, doi:10.1016/j.cose.2017.06.010.
[152] G. Francia, D. Thornton, T. Brookshire, Wireless vulnerability of SCADA systems, in: Proceedings of the 50th Annual Southeast Regional Conference, in: ACM-SE '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 331–332, doi:10.1145/2184512.2184590.
[153] H. Snyder, Literature review as a research methodology: An overview and guidelines, J. Bus. Res. 104 (2019) 333–339, doi:10.1016/j.jbusres.2019.07.039.
[154] N.C. System, Supervisory control and data acquisition (SCADA) systems, Tech. Inf. Bull. 04-1 (October) (2004) 76.
[155] N. Meghanathan, N. Chaki, D. Nagamalai, Advances in Computer Science and Information Technology. Networks and Communications: Second International Conference, CCSIT 2012, Bangalore, India, ... And Telecommunications Engineering), Springer Publishing Company, Incorporated, 2012.
[156] J. Lee, Y. Su, C. Shen, A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi, in: IECON 2007 – 33rd Annual Conference of the IEEE Industrial Electronics Society, 2007, pp. 46–51, doi:10.1109/IECON.2007.4460126.
[157] L. Zhou, H. Guo, G. Deng, A fog computing based approach to DDOS mitigation in IIOT systems, Comput. Secur. 85 (2019) 51–62, doi:10.1016/j.cose.2019.04.017.
[158] L. Wang, A. Liu, S. Jajodia, Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts, Comput. Commun. 29 (15) (2006) 2917–2933 Computer Communications, doi:10.1016/j.comcom.2006.04.001.
[159] A. Belqruch, A. Maach, SCADA security using SSH honeypot, in: Proceedings of the 2Nd International Conference on Networking, Information Systems & Security, in: NISS19, ACM, New York, NY, USA, 2019, pp. 2:1–2:5, doi:10.1145/3320326.3320328.
[160] P. Shakarian, D. Paulo, M. Albanese, S. Jajodia, Keeping intruders at large: a graph-theoretic approach to reducing the probability of successful network intrusions, in: 2014 11th International Conference on Security and Cryptography (SECRYPT), 2014, pp. 1–12.
[161] M. Hentea, Improving security for SCADA control systems, Interdiscip. J. Inf.Knowl. Manag. 3 (1) (2008) 73–86.
[162] N. Bene, Kaspersky Lab Developing Its Own Operating System? We Confirm the Rumors, and End the Speculation!, 2012, https://eugene.kaspersky.com/2012/10/16/kl-developing-its-own-operating-system-we-confirm-the-rumors-and-end-the-speculation/: .
[163] M. Bamburic, Kaspersky launches 'secure operating system' – with no trace of linux in it, 2017, https://betanews.com/2017/02/22/kaspersky-os/.
[164] V.L. Priya, C.B. Subramanian, A proposed architecture for SCADA network security, in: 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), 2011, pp. 142–145, doi:10.1109/ICCCET.2011.5762455.
[165] J. Slay, M. Miller, Improving security for SCADA control systems, Interdiscip. J. Inf. Knowl. Manag. 3 (2008).
[166] K.S. Kiangala, Z. Wang, Initiating predictive maintenance for a conveyor motor in a bottling plant using industry 4.0 concepts, Int. J. Adv. Manuf.Technol. 97 (9) (2018) 3251–3271, doi:10.1007/s00170-018-2093-8.
[167] L. Gigoni, A. Betti, M. Tucci, E. Crisostomi, A scalable predictive maintenance model for detecting wind turbine component failures based on SCADA data, in: 2019 IEEE Power Energy Society General Meeting (PESGM), 2019, pp. 1–5, doi:10.1109/PESGM40551.2019.8973898.
[168] T.P.-P. A. E. Program, Supply chain risks of SCADA/industrial control systemsin the electricity sector:recognizing risks and recommended mitigation actions, 2017, https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf.
[169] J. Luswata, P. Zavarsky, B. Swar, D. Zvabva, Analysis of SCADA security using penetration testing: A case study on modbus tcp protocol, in: 2018 29th Biennial Symposium on Communications (BSC), 2018, pp. 1–5, doi:10.1109/BSC.2018.8494686.

[170] H. Hilal, A. Nangim, Network security analysis SCADA system automation on industrial process, in: 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), 2017, pp. 1–6, doi:10.1109/BCWSP.2017.8272569.
[171] G. Yadav, K. Paul, A. Allakany, K. Okamura, Iot-pen: an e2e penetration testing framework for IoT, J. Inf. Process. 28 (2020) 633–642, doi:10.2197/ipsjjip.28.633.
[172] N. Tariq, M. Asim, F.A. Khan, Securing SCADA-based critical infrastructures: challenges and open issues, Procedia Comput. Sci. 155 (2019) 612–617 The 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019),The 14th International Conference on Future Networks and Communications (FNC-2019), The 9th International Conference on Sustainable Energy Information Technology, doi:10.1016/j.procs.2019.08.086.
[173] K. Nayak, D. Marino, P. Efstathopoulos, T. Dumitraş, Some vulnerabilities are different than others, in: A. Stavrou, H. Bos, G. Portokalidis (Eds.), Research in Attacks, Intrusions and Defenses, Springer International Publishing, Cham, 2014, pp. 426–446.
[174] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, G. Loukas, A taxonomy and survey of attacks against machine learning, Comput. Sci. Rev. 34 (2019) 100199, doi:10.1016/j.cosrev.2019.100199.