Research Article

Comprehensive Risk Identification Model for SCADA Systems

Abdelghafar M. Elhady ^{1,2}, Hazem M. El-bakry,¹ and Ahmed Abou Elfetouh¹

¹Faculty of Computers and Information, Mansoura University, Egypt

²Deanship of Scientific Research, Umm Al-Qura University, Saudi Arabia

Correspondence should be addressed to Abdelghafar M. Elhady; abdelghafar.elhady@gmail.com

Received 24 January 2019; Revised 19 April 2019; Accepted 11 June 2019; Published 6 August 2019

Academic Editor: Jesús Díaz-Verdejo

Copyright © 2019 Abdelghafar M. Elhady et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The world is experiencing exponential growth in the use of SCADA systems in many industrial fields. The increased and considerable growth in information and communication technology has been forcing SCADA organizations to shift their SCADA systems from proprietary technology and protocol-based systems into internet-based ones. This paradigm shift has also increased the risks that target SCADA systems. To protect such systems, a risk management process is needed to identify all the risks. This study presents a detailed investigation on twenty-one scientific articles, guidelines, and databases related to SCADA risk identification parameters and provides a comparative study among them. The study next proposes a comprehensive risk identification model for SCADA systems. This model was built based on the risk identification parameters of ISO 31000 risk management principles and guidelines. The model states all risk identification parameters, identifies the relationships between those parameters, and uses a hierarchical-based method to draw complete risk scenarios. In addition, the proposed model defines the interdependency risk map among all risks stated in the model. This risk map can be used in understanding the evolution of the risks through time in SCADA systems. The proposed model is then transformed into a benchmark database containing 19,163 complete risk scenarios that can affect SCADA systems. Finally, a case study is presented to demonstrate one of the usages of the proposed model and its benchmark database. This case study provides 306 possible attack scenarios that Hactivist can use to affect SCADA systems.

1. Introduction

SCADA refers to “Supervised Control and Data Acquisition.” SCADA systems are one of the Industrial Control Systems (ICS) [1] that are used to automate and control all processes and operations. Nowadays, SCADA systems are used in various large-scale fields such as power, energy production, transmission, and distribution (oil and gas, transportation, and water and wastewater) [2, 3]. In these fields, the components of the system are distributed geographically over a very large distance, and they need to be centrally monitored and controlled [4]. To achieve the monitoring and controlling functions, SCADA systems consist of a set of field sites, which are located in different places [5]. Each field site consists of one or more of Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), and Intelligent Electronic Devices (IED). Those are connected directly to the plants’ sensors and/or actuators to capture data from the plant

operation, perform limited control commands to the field site, and send site data to central control stations known as Master Stations (MS) [6, 7]. The system also has one master station, which collects data from all field sites through a powerful communication network, analyzes these data, and displays results on a graphical terminal called a Human Machine Interface (HMI) [8].

Through time, the number of stockholders that need to connect with SCADA systems directly (system employees and third parity companies) or indirectly through enterprise systems connecting to SCADA systems (customers) has increased. This has pushed SCADA systems toward using open standard protocols, unified technologies, public hardware, well-known software, and connecting to the internet [9, 10]. This paradigm switch has improved the system’s support at any time and from any place, and the integration of SCADA systems with other information systems has become trivial. Consequently, the system’s vulnerability has also increased,

making it easier to attack systems from any place using different exploits and attacking tools [11, 12]. Through 2016, the research team at the Kaspersky lab found that there are 220,558 SCADA components that can be accessed through the Internet. These components have been distributed across 170 countries [13]. All these components represent entry points for human agents attacking SCADA systems. They can be exposed to different types of natural phenomena, such as flooding and lightning [14].

The need for a powerful and collaborative risk management framework for SCADA systems has become urgent to identify, evaluate, and treat various types of risks targeting SCADA systems. All possible scenarios that may happen and affect the system either directly or indirectly should be well-described according to a set of parameters [15, 16]. These parameters could be defined as:

- (1) Risks that can happen to the system (what).
- (2) Agents who can do it (who).
- (3) Motivation for making the risk (why).
- (4) Penetration tools and methodologies used for performing the risk (how).
- (5) System components that can be targeted (where).
- (6) Component vulnerabilities that can be exploited by agents (when).

There is a shortage of accurate historical data on SCADA incidents that can be used in the risk management process because of the confidential nature of this field [17]. However, there are some sources that gave us indications on the growing risk to SCADA systems. One of these sources is the RISI database [18], which contains 242 incidents through 2015. Another source is the ICS-CERT database [19], which recorded a growing number of vulnerabilities detected in ICS components (from 2 in 1997 to 189 vulnerabilities in 2015). There is also Bompard et al. [20], who counted 133 blackouts in SCADA systems in the field of power only from 1965 to 2011.

According to state-of-the-art methods, there was a gap in providing complete risk identification scenarios that fulfill the risk identification scenarios related to the six parameters stated in ISO 31000 [15]. Zhu et al. [21] gave abstracted information about system components and system vulnerabilities. Hewett et al. [22] focused on four types of attacks that target wireless sensor networks. ICS-CERT [19] linked system components and component vulnerabilities. Stouffer et al. [23], Bompard et al. [20], and Zhu et al. [21] provided two individual maps, one between the risk and agent and the other between the risk and affected components without trying to merge the two maps and expanding them to include the other risk identification parameters. Miller et al. [24], Gabriel et al. [25], and Nan et al. [11] defined the relation among risk, system components, and vulnerabilities without providing the relationship between these parameters with the agent, his motivation, and the penetration tools used.

This paper proposes an extensive model for identifying the risks to SCADA systems, which can be used as a base for the automatic generation of many SCADA risk scenarios.

In building the model, six parameters determined in ISO 31000 [15] and a hierarchical-based method were used, in which all risk parameters were defined with the most possible values and organized in the first level of the model. Then, these parameters were synchronously organized by linking each parameter with the most related ones in the form of matrices. Consequently, seven 2D matrices were built at the second level, which were gathered into four 3D matrices in the next level. Finally, the four 3D matrices were merged to build the complete proposed model based on a 6D matrix. This resulting matrix connected all the parameters together. The risk interdependency map was defined to represent the relationships among all risks in the model. This map illustrated the direct and indirect dependency among the risks. Also, this model was transformed into a benchmark database, which contains 19,163 risk scenarios for SCADA systems. This benchmark database can be used to generate a risk scenarios knowledgebase that might help risk managers and decision makers to analyze, evaluate, and resolve the expected risks with either a proactive or reactive risk management approach. Another use for this model and its benchmark database is in risk management simulation software, such as in the SCADA Risk Identification & Classification Engine (SRICE), a component of the Generic Software Risk Management Framework for SCADA Systems designed by Elhady et al. [26].

This paper is structured as follows. In Section 2, a review on previous work is provided. This review focused on risk identification phases of SCADA and ICS systems. Section 3 shows a comparative study among the available previous scientific articles, guidelines, and databases as well as a statistical summary. Section 4 defines the problem statement of the study. Then, the proposed comprehensive risk identification model for SCADA systems is presented in Section 5. The transformation of the model into a benchmark database and the brief statistics are presented as a DB summary in Section 6. Section 7 presents two case studies of the scenarios that could be provided by the proposed model and its database. Section 8 presents the conclusion and future work.

2. Risk Identification Literature Review

The literature review is outlined in three main categories: ICS/SCADA Risk Scientific researches, ICS/SCADA Risk repositories, and ICS/SCADA Risk reports and guides. This review covers the last decade from 2009 till 2018 to make it up to date with the latest ICT expressions and principles.

The main set of scientific papers was formed from the searches run on SCOPUS, ACM, Web of Science, and IEEE Explore, as recommended in Kitchenham and Brereton [27]. The search keywords were based on two groups of words, with each paper containing at least one word from each group. The first group includes the words “risk,” “security,” “threat,” and “vulnerability”; whereas, the second group contains “SCADA” and “Industrial control system (ICS).” After that, the collected papers were filtered by focus on those that had interest in more than two parameters of risk identification in SCADA and ICS.

The second and third categories concentrated on databases and reports that had been issued by accredited academic and research organizations in the field of risk in SCADA and ICS systems. These organizations, like the National Institute of Standards and Technology (NIST) [28], European Union Agency for Network and Information Security (ENISA) [29], and the United States Department of Homeland Security (DHS) [30].

Our search produced thirteen papers, two databases, and six reports and guides, which will be presented in the next section. Then, a comparative study between them and the proposed model will be made in the last section of this paper.

2.1. ICS/SCADA Risk Scientific Studies (Papers). Nasser et al. [36] investigated cyber threats targeting physical systems. They proposed a classification based on five parameters (types of attack, target sector, intention, impact, and incident category). They provided a matrix of these threats in conjunction with simple statistical data. Moreover, Finogeev and Finogeev [37] focused on attacks that target the SCADA wireless sensor network and that have been initiated by external agents. They classified attacks based on innovative impacts on SCADA components. Furthermore, Eden et al. [38] presented a global taxonomy for SCADA incidents' response. They classified system assets into five categories based on risk impact. Three categories were based on safety process, timing, and location, while the other two categories are mission critical and business critical. They distinguished attacks into three types: hardware, software, and communication attacks. Woo and Kim [39] also identified fifteen types of threads and four SCADA system components. First, they linked between each thread and target component, and then they determined the vulnerabilities for each system component based on historical data and the component's characteristics.

Hewett et al. [22] defined four types of attacks that can target SCADA sensor networks: Sybil attack, node compromise, eavesdropping, and data injection. For each attack, the researchers specified the methodology the attacker used to achieve the attack and the system components they may target. Miller et al. [24] proposed a framework for classifying cyber physical systems incidents. This framework relies on four dimensions: seven different source types, methods used in the incident, direct and indirect impact of incident, and victim of incident. However, Bompard et al. [20] classified threat origins into four types: natural threats, accidental threats, malicious threats, and emerging threats. They provided detailed descriptions on each type of threat and displayed their possible impacts on the system.

Gabriel et al. [25] proposed new approach for risk identification and assessment in electricity infrastructure. They identified 21 main risks and 142 sub risks and classified them based on three criteria. The first criterion is the type of risk divided into technical and nontechnical risks. The second criterion is according to effect, in four categories: operational, environmental, financing, and quality compliance. The last criterion is according to risk severity, divided into critical, important, tolerable, and acceptance. Finally, they used a semi-quantitative methodology to rank these risks based on subjective assessment and specialist opinions. Nan et al. [11]

provided further investigation on the vulnerabilities resulting from the interdependency between the SCADA system and System Under Control (SUC). They displayed the negative impacts on each linking component: such as sensors, actuators, and RTU, due to attackers using these vulnerabilities and how to minimize these negative impacts. Guillermo et al. [40] distinguished the SCADA system into five main components: system, network, physical, employee, and information. They stated a very simplified set of vulnerabilities for each one of them. They also stated a few threats that can affect the system. Zhu et al. [21] outlined a general set of SCADA system vulnerabilities, such as insecure network, vulnerable operating system, and misuse of encryption. They also classified threats based on target components like hardware, software, and communication stack and implemented protocols. Tsang [41] discussed SCADA network attacks and incidents and distinguished between accidental and intentional threats caused by threats agents and how they cause these threats. Further, they displayed a set of vulnerabilities in a SCADA network that can be used by threat agents. They summarized the set of actual attacks on a real-world SCADA network. Dong Kang et al. [42] presented thirty-two common computer system threats and spread them across four parts of a SCADA system: control devices, communication links, control center, and communication with corporate network. This mapping was based on the probability of targeting these threats on those parts.

2.2. ICS/SCADA Risk Databases (Repositories). In 2001, Eric Byres and Mark Fabro developed a database for Industrial Control Systems (ICS). They called it the Repository of Industrial Security Incidents (RISI) [18]. This database focused on incidents, their caused agents, and which system's components were affected. This database is flawed due to its small number of incidents recorded and the fact that it hasn't been updated since January 2015.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in the U.S. DHS developed a database that concentrates on the vulnerabilities of an ICS components' platform rather than any other risk identification parameters like risk agents, their motivations, and the used penetration tools [19].

2.3. ISC/SCADA Risk Reports and Guides. Stouffer et al. [23] with NIST presented a guide for ICS security. This guide classified threats sources into four classes: adversarial, accidental, structural, and environmental. For each threat source, they described a sample of threats that can be caused by this class. Then they categorized the system into six categories: policy and procedure, architecture and design, configuration and maintenance, physical, software development, and communication and network. For each category, they listed its vulnerabilities.

The European Union Agency for Network and Information Security (ENISA) team presented report on communication network dependencies for ICS/SCADA Systems [32]. This report listed threats and vulnerabilities related to ICS/SCADA and showed eight attack scenarios. Each scenario targeted a main component of an ICS/SCADA

system and discussed the steps that should be taken to prevent that attack scenario.

Brown and Wylie [33] from SANS Institute-InfoSec Reading Room team collected data from hundreds of specialists in the field of ICS security to produce an annual report on ICS's most common risks. They provided statistics on the risks for each component in an ICS system and the threat agents that cause these risks.

The Trusted Information Sharing Network (TISN) for critical infrastructure reliance developed a generic SCADA risk management framework for Australian critical infrastructure [34]. They classified threat agents into five classes based on scope, malicious intent, and nature. They also distinguished the system components into four main categories: people, products, process, and reputation. Finally, they mapped each category of system components with all of their vulnerabilities and what class of threat agents can exploit these components.

DHS presented a report on Common Cyber Security Vulnerabilities in ICS [35]. They classified these vulnerabilities into three categories: ICS software, ICS configuration, and ICS network security.

Schwab and Poujol from the Kaspersky lab team provided a report that summarized the state of ICS cybersecurity in 2018 in each geographical region all over the world [31]. They listed sixteen risks that could affect industrial systems' operations. They also stated twelve vulnerabilities that can cause a negative impact on these systems.

3. Comparative Study

In this section, a comparative study among all previous studies is presented. The comparative study depends on two levels of comparison. The first level of comparison concentrates on individual risk identification parameters. Then these parameters are merged in two dimensions, three dimensions, and six dimensions parameter matrices and state the corresponding previous studies.

3.1. Single Parameter Mapping Comparison. In this comparison, the previous works are distinguished based on number of risk identification parameters stated. As shown in Table 1, no single previous work had presented all parameters of risk identification.

The total number of parameters stated in each previous work is visualized in Figure 1. This figure shows that the biggest number of parameters stated in a previous work was five parameters, which was presented only one time in a scientific paper (Tsang [41]). There is one ICS report (ENISA [32]) and three scientific papers (Bompard et al. [20], Gabriel et al. [25], and Guillermo et al. [40]) that stated four parameters. The most parameters stated in a previous work were three parameters, which were stated in ten of the previous works. These ten works were classified as one database, three ICS reports and guides, and six scientific papers. Finally, the fewest parameters stated in a previous work was two, which was presented in six previous works, which are distributed as ICS-CERT database [19], two ICS reports and guides, and three scientific papers [11, 36, 37].

FIGURE 1: Total no. of risk identification parameters stated per previous works.

Another statistic is presented in Figure 2. This figure displays the total number of previous works stating each risk identification parameter. This shows that the most risk identification parameters stated in previous works were risk (What?) and system components (Where?), which were stated in sixteen previous works. Next parameter was component vulnerabilities (When?) in thirteen previous works, and then risk agent parameter in eleven previous works. Penetration technique (How?) was stated in six previous works. Finally, the risk identification parameter least presented in previous works was risk motivation (Why?), stated once in ENISA [32].

3.2. Multi-Parameters Mapping Comparison. In this section, all the previous works are compared based on mapping risk identification parameters into two, three, and six dimensional matrices. All the previous works were examined to discover if they stated these parameter mappings or if they provided another mapping. Finally, this examination is summarized in Table 2.

The comparative study data in Table 2 were collected based on the total number of mapping matrices stated in each previous work as shown in Figure 3. This figure shows that the maximum number of mapping matrices stated in the previous works were three mapping matrices, which were presented in only three previous works: ENISA [32], Gabriel et al. [25], and Tsang [32]. Then, there are five previous works that mentioned only two mapping matrices and nine previous works that mentioned only one mapping dimension. There are four previous works that didn't mention any mappings between two or more of risk identification parameters.

Another statistic on the previous works was based on the total number of previous works mentioning each risk identification mapping matrix, as shown in Figure 4. This figure shows that the mapping between risk (What?) and system components (Where?) was the most-stated mapping in previous works, mentioned eight times. Then, the mapping between system components (Where?) and component vulnerabilities (When?) was mentioned in several previous works. The mapping between risk agent (Who?) and penetration techniques (How?) in a two-dimensional matrix was the

TABLE 1: Risk parameters stated in each work.

Paper	Risk Agent (WHO?)	Risk Motivations (WHY?)	Risk (WHAT?)	Penetration Technique (HOW?)	System Components (WHERE?)	Component Vulnerabilities (WHEN?)	Risk Interdependency
SCADA & ICS Risk Databases							
ICS-CERT [19]					✓	✓	
Byres and Fabro [18]	✓		✓		✓		
SCADA & ICS Reports and guides							
Schwab and Poujol [31]			✓			✓	
ENISA [32]	✓	✓	✓	✓			✓
Brown and Wylie [33]	✓		✓		✓		
Stouffer et al. [23]	✓				✓	✓	
TISN [34]					✓	✓	
DHS [35]					✓	✓	
SCADA & ICS scientific research							
Nasser et al. [36]			✓	✓			
Finogeev and Finogeev [37]			✓		✓		
Eden et al. [38]			✓		✓	✓	
Woo and Kim [39]			✓		✓	✓	
Hewett et al. [22]			✓	✓	✓		
Miller et al. [24]	✓		✓	✓			
Bompard et al. [20]	✓		✓		✓	✓	
Gabriel et al. [25]	✓		✓		✓	✓	✓
Nan et al. [11]			✓			✓	✓
Guillermo et al. [40]	✓		✓		✓	✓	
Zhu et al. [21]	✓				✓	✓	
Tsang [41]	✓		✓	✓	✓	✓	
Kang et al. [42]			✓	✓	✓

FIGURE 2: Total no. of previous works stated each risk identification parameter.

mapping matrix least-mentioned, only appearing one time in a previous work. There are four mapping matrices that weren't mentioned at all in the previous works, as shown in the figure.

4. Risk Identification Problem in SCADA System

So far, many researchers have tried to study the risks in SCADA systems. Their trails are short and suffer from describing an efficient algorithm in identifying the risk class. Moreover, a correct definition for vulnerability in SCADA

is missed. This paper tries to map the relation between the effective parameters that identifying the SCADA risks and the whole scenario for specific risks. The whole scenario for risks is targeted through rebuilding a significant database collected from previous resources and then analysing the results. The problems that face other researches are assumed in the DB and summarized in the following points:

(1) Giving a detailed level of identifying the risks and classifying them based on the nature of the risk agents, their action's motivation, and the penetration tools/techniques that can be used to cause a risk on a SCADA system.

FIGURE 3: Total no. of risk identification parameters per previous work.

FIGURE 4: Total no. of risk identification parameters mapping stated per previous work.

(2) Providing all possible components that formulate a SCADA system and state all known vulnerabilities that can be used by attackers to perform the attack.

(3) Mapping between risks, vulnerabilities, and system components by linking each risk with all possible vulnerabilities of system's components that an attack agent can utilize to achieve the risk goals. A description of the estimated impact on that component as a result of an attack is also missing.

(4) Description of the interdependency among threats that can be used to present the possible attack path scenarios.

The main point in this work depends on the hierarchical-based method. The relation among related parameters is converted into matrices, which are linked synchronously to construct an augmented matrix with six dimensions, which is analyzed.

5. The Comprehensive Risk Identification Model for SCADA System

The risks that face SCADA were studied through a set of vulnerability resource databases, such as ICS-CERT [19], NVD [43], CVE [44], Bugtraq [45], OSVDB [46], Mitre [47], and exploit-DB; incidents repositories such as RISI [18]; and annual reports related to threats in the field of industrial

control systems and SCADA systems. These reports and guides were collected from NIST [28], and ENISA [29].

The collected information were organized and classified in the form of six main risk identification parameters, (What, Who, Why, How, Where, and When). Then, an analytical study that defines the relations among these parameters draws a complete view of the risk scenarios. Each scenario can define the risk affection on the SCADA system (What), the source of that risk (Who), the reasonable motivations behind performing specific actions (Why), penetration tools and methodologies that cause the risk (How), possible system components wherever an attack can be targeted (Where), and the existing vulnerabilities in components when a threat source can execute his attack (When).

The hierarchical-based methodology was used to build the proposed model. The hierarchal tree consists of four levels. The first level aims to define each parameter's values. The consequent level is constructed by mapping each parameter with the most related parameters. Seven matrices are constructed in the second level. Hence, collections of matrices are similarly constructed based on reducing the number of neighbors and augmenting the relation among parameters in the next levels. By the third level, four matrices are constructed by merging the seven matrices in the previous

FIGURE 5: The hierarchical methodology of the proposed model.

step. Finally, full-risk scenarios matrix is constructed by developing an algorithm used to relate all 3D matrices in level three and produces complete risk scenarios, as illustrated in Figure 5. The defined steps are stated as shown in the following steps:

5.1. Step 1. Define the six main parameters (risks, risk agents, agent motivation, system's components, system's vulnerabilities, risk's penetration methodologies).

Risk (What?) defines the list of initial incidents that can threaten the SCADA system. These incidents cause a negative impact on a system's availability, integrity, and/or confidentiality, which leads to defects in achieving the system's objectives and functionality. Risk agent (Who?) defines the list of the most possible risk agents [18, 23, 32] that represent the sources of any risk affecting the system either accidentally or intentionally. These agents are classified based on a set of features [14]:

- (i) *Nature*: human agent and natural agent.
- (ii) *Scope*: internal agent and external agent.
- (iii) *Intention*: agent's action that causes risk could be intentional and accidental.
- (iv) *Strength*: for human agent, the strength feature expresses the overall characteristics to successfully execute risk. This feature has been calculated based on three characteristics (capability, knowledge, and skills) of a human agent [48]. For a natural agent, the strength feature represents the power of natural phenomena. This feature has been ranked into three levels: low, medium, and high.

This classification helps us understand the risk motivations for each agent. Risks can result from these motivations, as we will illustrate in the next sections. Any risk that occurs in a SCADA system has at least one reason. This reason incites the agent to carry out his attack on the system. The risk motivations (Why?) parameter defines these reasons. The system components (Where?) parameter defines the physical devices of a SCADA system that can be targeted for an attack. The most physical components of the SCADA system are categorized into eight main categories based on technical and functional characteristics of the component. The component vulnerabilities (When?) parameter illustrates the conditions when their existence could lead to or facilitate the risk agent from initiating his attack on the system. The penetration technique (How?) parameter defines the most common penetration methodologies, techniques, and tools that risk agents can use to exploit a system's vulnerabilities and/or cause harm to one or more system components.

The six main parameters of the proposed model are listed in Table 3. This table lists 27 risks, 24 risk agents, 7 risk motivations, 14 penetration tools, 36 vulnerabilities, and 30 system components.

5.2. Step 2. In this step, the interdependency risk map, the cascading effect among all risks listed in step 1, is counted as shown in Figure 6. This map provides the common possible attack paths that can be used by risk agents to reach a specific risk. It also defines the direct and indirect effect of any risk.

For example, the data disclosure risk can conclude from this map where all possible attack paths that lead to data disclosure are declared, as shown in Figure 7. There are three paths leading to the data disclosure risk at the end. These paths are as follows:

TABLE 3: Risk Identification Six Parameters.

Risk (What?):	Risk Agents (Who?):	Risk Motivations (Why?):	System Components (Where?):	Component Vulnerabilities (When?):	Penetration technique (How?):
(1) <i>Human risks</i> (R9) Inappropriate control commands	(A1) Current Employee (A2) Former Employee (A3) Current business partner. (A4) Former business partner (A5) Customer (A6) Script Kiddies (A7) Industrial spies (A8) Online social hacker (A9) Corporate/competitors	(M1) Convenience. (M2) Monetization (M3) Revenge. (M4) Socially. (M5) Ideologically (M6) Nationally. (M7) Environmental changes.	(1) Remote station (RT1: sensor, RT2: actuator, RT3: RTU, RT4: PLC and RT5: IED). (2) Communication device (CD1: switch, CD2: router, CD3: repeater, CD4: modem, CD5: WLAN access point and CD6: Firewall). (3) Wire media (WM1: coaxial cable, WM2: twisted pair cable and WM3: Fiber optic cable). (4) Wireless media (WLM1: radio frequency, WLM2: microwave and WLM3: satellite). (5) Master station (MS1: communication server, MS2: SCADA server, MS3: historian Server and MS4: HMI) (6) Corporate network (CN1: Application server, CN2: web server, CN3: mobile server, TRI: PC/laptop and TR2: smart phone/tablet).	(1) <i>Human errors</i> (V1: display information about the system and who operate it, V2: unqualified employee, V3: Leak of skills, knowledge and training, V4: Sharing password among users, V5: password disclosure, V6: Former employees/contact expose their system knowledge to external persons, V7: Account still activated for former employee and partners, V13: Using default password, V14: No password used, V15: Using weak password policies, V27: Inappropriate or unauthorized access controls, V36: Lack of remote access control) (2) <i>Physical vulnerabilities</i> (V8: Isolated sites, V9: Poor maintenance, V10: Absence of alarm system, V11: Weak windows and doors controlling, V12: Lack of diversity in physical security tools, V24: Lack of diversity in communication paths lead to communication failure, V28: Absence of ups and power generator not exists, V29: Air-conditioning failure, V30: Lack of redundant hardware, V33: No warranty agreement, V34: No spares management) (3) <i>Software vulnerabilities</i> (V18: Critical configurations are not stored or backed up, V20: Open communication/unprotected protocols are used, V25: Poor or non-existent software updates, V21: Unsecured wireless networks, V26: Unsecured physical ports, V31: Intrusion detection/prevention software not used, not updated, or not tested, V32: Anti-virus/anti-malware not used, not updated, or not tested, V33: No warranty agreement, V35: Memory overflow)	(PT1) Social engineering/phishing. (PT2) Interception/eavesdropping/espionage. (PT3) Exploit kits. (PT4) Malicious code. (PT5) Spamming. (PT6) Web-based attacks. (PT7) Web application attacks. (PT8) Botnets. (PT9) Spoofing. (PT10) Physical attack. (PT11) Disaster (geological/hydrological/meteorological). (PT12) Human error/misuse of resources. (PT13) Malfunction of equipment. (PT14) Data manipulation or froging.
(2) <i>Physical risks</i> (R20: Site penetration, R1: Physical theft of hardware, R2: Device power failure, R3: Destruction of hardware, R6: Site- building destruction, R7: Network wires stealing, R8: Network wires damage, R15: Physical theft of data, R22: Hardware failure, R24: Disable Device, and R27: Equipment crash)	(A10) Hacktivist (A11) Cyber-criminal group (A12) Cyber terrorist (A13) National state (A14) Earthquakes (A15) Floods (A16) Tsunamis (A17) Landslides (A18) Lightning (A19) Heavy rains (A20) Heavy snowfalls (A21) Tornado (A22) Wildfire (A23) Fires (A24) Explosions		(7) People (PE1: system employees, PE2: system clients and PE3: 3rd party stuff). (8) BSI: Building & site.	(4) <i>Data vulnerabilities</i> (V16: Sensitive data unprotected with encryption and password protection, V17: Unprotected data transferred, V19: Absence or untested backup procedure, V22: System log not maintained or revised periodically, V23: Sensitive data are not encrypted in transit)	
(3) <i>Software risks</i> (R4: Device compromise, R5: Device misconfiguration, R16: Gain physical access, R17: Gain remote access, R18: Identify network devices, R21: Gain device administrator password, R23: Bypass Device admin password, R25: Network outage, R26: Software failure)					
(4) <i>Data risks</i> (R9: Network wireless signal disruption, R10: Data sniffing, R1: Data interception, R12: Data distortion, R13: Data discloser, R14: Losing data)

FIGURE 6: Interdependency risk map for the proposed model.

FIGURE 7: Interdependency risk map for data discloser risk.

- (1) Site penetration -> Gain physical access -> Data sniffing Data discloser.
- (2) Site penetration -> Gain physical access -> Physical theft of data ->Data discloser
- (3) Site penetration -> Physical theft of hardware -> Physical theft of data ->Data discloser

5.3. *Step 3.* In this step, each parameter is linked to the most related parameters of the risk identification in a 2D matrices form in which all values of one parameter are organized in horizontal direction (row headers) and all values of the related parameter are organized in the vertical direction (column headers). Each intersection between one column and one row represents the existing relation between the values of

the intersected row and column. This relation has two values, true ($\sqrt{}$) and false (null). Consequently, 2D matrices are built based on the collected information from the works in the literature review. The constructed seven 2D matrices present a complete view of the relation among all risk identification parameters.

The first 2D matrix, labeled (who/why), describes the relations between risk agents (who) and risk motivations (why). All risk agents are listed as row headers, and all risk motivations are listed in column headers, as shown in Figure 8. The risk motivation for each agent is classified based on agent intention feature. For example, the current employee agent has a convenience motivation only for accidental intention. On the other hand, the current employee has monetization and revenge motivations for intentional intention. The competitor has monetization, revenge, and social motivations.

Similarly, the other six matrices have been built. The matrix (what/who) describes the relation between risk agents (who) and risks (what) that were caused by each agent. All risk agents represent the row headers and all risks represent the column headers, as shown in Figure 9. The matrix (who/how) defines the relation between the risk agents (who) and penetration techniques (how) to illustrate the agent's penetration tools that cause system risks. In this matrix, all risk agents represent row headers and all penetration techniques represent the column headers, as shown in Figure 10. The matrix (what/how) defines the relation between risks (what), which represent the column headers, and the penetration techniques (how), which represent the row headers, as shown in Figure 11. The (what/where) matrix defines the relation between risks (what) and system components (where) in which these risks can occur. The risks list represents the column headers and all system components represent the row headers, as shown in Figure 12. The (where/when) matrix defines the relation between system components (where) and their vulnerabilities (when), in which their existence could result in a risk, as shown in Figure 13. Finally, the (when/how) matrix defines the relation between component vulnerabilities (where) and penetration techniques (how), which can cause these vulnerabilities to create risk, as shown in Figure 14.

5.4. Step 4. Another merge step is represented where both 2D matrices from step 3 are joined to form a 3D matrix to build a partial risk scenario. Each matrix is organized as two related columns and a single row. The first column represents the most significant parameter. The second column represents all correlated values of the second parameter. A many-many corresponding relationship is defined between the first parameter and the second parameter values. The other columns' headers represent the values of the third parameter. The mapping of these three parameters defines all values of the third parameter related to the other two parameters. Each intersection between each column and each row represents the relation between the values of the intersected row and column. Also, this relation has two values, true ($\sqrt{}$) and false (null).

The first 3D matrix joins the related two 2D matrices (Who/Why and What/Who), where risk agent (who) joins the two matrices. This matrix answers the question of what risk can be caused by an agent and his motivation. In this matrix, all risk agents have been listed in the first column. For each risk agent value, the risk motivations are presented using (who/why) matrix. On the other hand, all risks are represented as columns header. Using the (what/who) matrix, the first row of each risk agent displays all risks that can be caused by that agent. The following rows for that agent are constructed in conjunction with the risk motivation, where each row defines a specific agent and certain motivation. All checked risks from the first row of that agent are oriented on the agent/motivation rows based on each agent and motivation nature for that risk, as shown in Figure 15.

For example, the current employee agent has the first four rows. The first one represents all risks that can be done by the current employee. The next three rows represent all risks that can be done by the current employee for a specific risk motivation (convenience, monetization and revenge).

The second 3D matrix combined three 2D matrices from step 3 (what/who, what/how, and who/how) into one 3D matrix of (what/who/how). This 3D matrix answers the question of what risk can happen (what) from which agent (who) and which penetration tool (how). In this matrix, the first column represents all risk agents and the second column represents all penetration techniques for each agent using the (who/how) matrix. All risks are displayed from the third column up to the end of the risk. The first row of each risk agent displays all risks that can be caused by that agent using the (what/who) matrix. The following rows for that agent are made in conjunction with penetration techniques where each row defines a specific agent and certain penetration technique. All checked risks from the first row of that agent are oriented on the agent/penetration technique rows based on each agent and penetration technique he can use to cause that risk using the (who/how) matrix, as shown in Figure 16.

The third 3D matrix joined the two 2D matrices from step 3 (what/where and where/when) into one 3D matrix (what/where/when). This matrix answers the question of what risks exist (what) in what system components (where) that have specific vulnerabilities (when). In this matrix, all system components are listed in the first column. For each system component value, risks that can occur for that component are presented using the (what/where) matrix. All vulnerabilities are organized from the third column up till the end of the vulnerabilities. The first row of each component displays all vulnerabilities that can exist for that component using the (where/when) matrix. The following rows for that component are made in conjunction with risk where each row defines specific component and certain risk. All checked vulnerabilities from the first row of that component are oriented on the component/risk rows based on each component and risk that can exploit that vulnerability to successfully achieve that risk. This 3D matrix has two types of mappings between risk and vulnerabilities. The first one defines the risks directly occurring due to the existence of a specific vulnerability. This type is presented as the yellow color cells. The other type defines the risks that indirectly

Agent list	Intention		Motivation							Characterization			strength
	Intentional	Accidental	Convenience	Monetization	Revenge	Socially	Ideologically	nationally	Environmental changes	Capability	Knowledge	Skills	
current Employee	✓		✓	✓	✓					L	L	L	L
Former Employee	✓	✓	✓	✓	✓	✓				L	M	M	M
Current business partner (Contractor-provider-suppliers-3rd Party)	✓	✓	✓	✓						H	M	M	M
Former business partner (Contractor-provider-suppliers)	✓	✓	✓	✓	✓					H	M	M	M
customers	✓		✓	✓	✓	✓				L	L	L	L
Script Kiddies	✓			✓		✓				L	L	L	L
Online social hacker	✓			✓		✓				L	M	H	M
Industrial Spies	✓			✓						M	H	H	H
Corporate / Competitors	✓			✓	✓	✓				H	H	H	H
Hacktivist	✓			✓		✓	✓			H	H	H	H
Cyber Criminal group	✓			✓						H	H	H	H
Cyber Terrorist	✓						✓			H	H	H	H
National state	✓							✓		H	H	H	H
Earthquakes		✓							✓				M
Floods		✓							✓				M
Tsunamis		✓							✓				H
Landslides		✓							✓				H
Lightning		✓							✓				H
Heavy rains		✓							✓				L
Heavy snowfalls		✓							✓				L

FIGURE 8: Snapshot of who/why matrix.

Risk Agent	Incident																							
	Physical theft of hardware	Device power failure	Disruption of hardware	Device compromise	Device misconfiguration	Site building destruction	Network wire stealing	Network wire damage	Network viruses	Legal disruption	Data interception	Data disclosure	Lossing data	Physical theft of data	Gain physical access	Gain remote access	Identify network device	Inject remote control commands	Site penetration	Gain device administrator password	Hardware failure	System password validation	Device Disabled	Network outage
current Employee	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Former Employee	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Current business partner (Contractor-provider-suppliers)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Former business partner (Contractor-provider-suppliers)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Customer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Script Kiddies	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Industrial spies	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Online social hacker	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Corporate / Competitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hacktivist	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber Criminal group	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber Terrorist	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
National state	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Earthquakes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Floods	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tsunamis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Landslides	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lightning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Heavy rains	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Heavy snowfalls	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tornado	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wildfire	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fires	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Explosions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 9: Snapshot of who/what matrix.

exist due to that vulnerability. This type is presented as red color cells, as shown in Figure 17. This mapping used the interconnected risk map shown in Figure 6 to determine the indirect risks from a specific vulnerability.

The final 3D matrix merged the (what/how) matrix with the (when/how) matrix to generate a new 3D matrix of (what/how/when). This matrix defines the vulnerabilities (when) and which penetration tools (how) can use them to cause certain risks (what). In this matrix, the first column represents all risks, and the second column represents all penetration techniques for each risk using the (what/how) matrix. All vulnerabilities are displayed from the third column up to the end of the vulnerabilities, as shown in Figure 18.

5.5. *Step 5.* The consequent step aims to generate the complete scenarios by combining the four 3D matrices. The complete risk identification scenarios for SCADA systems are defined by Algorithm 1.

6. A Benchmark Database for the Proposed Model

A benchmark database was developed using the proposed model. This database uses MySQL DB version 5.7.19 MySQL [49] as the database engine. As shown in Figure 19, the Entity Relationship Diagram (ERD) of the database contains 11 tables: one table for coding each risk parameter and

Agent	Penetration Techniques													
	social engineering / phishing	interception/ eavesdropping / espionage	Exploit kits	malicious code	Spamming	Web-based attacks	Web application attacks	Botnets	spoofing	physical attack	Disaster	human error /misuse of resources	malfunction of equipment	data manipulation or froging
current Employee	✓	✓		✓	✓				✓	✓		✓	✓	✓
Former Employee	✓	✓		✓	✓				✓	✓		✓	✓	✓
Current business partner	✓	✓		✓	✓				✓	✓		✓	✓	✓
Former business partner	✓	✓		✓	✓				✓	✓		✓	✓	✓
Customer	✓			✓		✓	✓	✓	✓	✓		✓	✓	✓
Script Kiddies				✓		✓	✓	✓	✓	✓		✓	✓	✓
industrial spies	✓			✓		✓	✓	✓	✓	✓				✓
Online social hacker	✓			✓		✓	✓	✓	✓	✓				✓
Coroperate / Competitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓
Hacktivist	✓			✓		✓	✓	✓	✓	✓				✓
Cyber Criminal group	✓		✓	✓	✓	✓	✓	✓	✓	✓				✓
Cyber Terrorist				✓		✓	✓		✓	✓				✓
National state	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓
Earthquakes										✓	✓			
Floods											✓	✓		
Tsunamis										✓	✓			
Landslides										✓	✓			
Lightning										✓	✓			
Heavy rains										✓	✓			
Heavy snowfalls										✓	✓			
Tornado										✓	✓			
Wildfire										✓	✓			
Fires										✓	✓			
Explosions										✓	✓			

FIGURE 10: Snapshot of who/how matrix.

Penetration technique	Risk																														
	Physical theft of hardware	Device power failure	denial of hardware	device compromise	misconfiguration	site hijacking	network wires	stealing	network wires damage	network wireless signal disruption	data sniffing	data interception	data disruption	data disclosure	losing data	Physical theft of data	gain physical access	identity network devices	inappropriate control commands	site penetration	gain device administrator password	hardware failure	bypass password validation	Device Disabled	network outage	software failure	equipment crash				
social engineering / phishing											✓	✓								✓		✓									
interception/ eavesdropping / espionage											✓	✓	✓							✓			✓								
Exploit kits(sw / fw)				✓	✓					✓	✓	✓	✓			✓	✓					✓	✓								
malicious code										✓	✓	✓	✓	✓	✓							✓	✓		✓						
Spamming																															
Web-based attacks				✓	✓						✓	✓	✓								✓		✓	✓	✓						
Web application attacks				✓	✓						✓	✓	✓	✓	✓				✓				✓	✓	✓						
Botnets																							✓	✓	✓						
spoofing																								✓	✓						
physical attack	✓	✓	✓			✓	✓	✓							✓	✓				✓			✓								
Disaster (heat/ water / wind/ land sliding)	✓	✓	✓			✓		✓	✓													✓									
human error /misuse of resources		✓	✓			✓		✓	✓							✓	✓		✓	✓	✓	✓	✓	✓	✓						
malfunction of equipment								✓	✓										✓			✓		✓	✓	✓					
data manipulation or froging													✓						✓					✓	✓	✓	✓				

FIGURE 11: Snapshot of what/how matrix.

four tables for mapping the 3D matrices (agent_mot_risk, agent_tool_risk, comp_risk_vuln and risk_vuln_tool). The last table (Risk scenarios) contains the full risk scenarios matrix for the SCADA system, which was generated using Algorithm 1.

The risk scenario table resulting from Algorithm 1 contains 19,163 scenarios. Figures 20, 21, 22, and 23 show the total number of risk scenarios for each risk, risk agent, risk motivation, and penetration tool, respectively.

7. Case Study

In this section, a case study of the proposed model and the resulted database is presented. This case study shows a short sample of the detailed data about the possible risks scenarios that could occur in a SCADA system and that could be used further by decision makers and risk managers. This data can

help managers to determine the weak points in the system, the possible risk agents, causes that make them attack the system, and the tools and methodologies agents can use to perform these attacks. Also, the benchmark database that was produced by this model could be used to generate a SCADA risk knowledgebase for SCADA Risk Management simulation tools. To the best of our knowledge, this level of detailed information presented by the proposed model and resulted database hasn't been provided by any type of related research work or database.

7.1. Case Study 1. One of the questions that can be answered by the proposed model is what are the possible risks that risk agents can use to attack a SCADA system and what are the risk scenarios for these attacks?

To answer this question, the proposed model will be applied on Hacktivist as an example of risk agents. The

System Components	Risk																							
	Physical theft of hardware	Device power failure	destruction of hardware	device compromise	misconfiguration	site- building destruction	network wires stealing	network wires damage	network-wireless signal disruption	data sniffing	data interception	data disclosure	losing data	Physical theft of data	gain physical access	gain remote access	identify network devices	inappropriate control commands	site penetration	gain device administrator password	hardware failure	bypass admin password	Disable Device	network outage
Sensor c1	✓	✓	✓	✓																				
Actuator c2	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
RTU c3	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
PLC c4	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
IED c5	✓	✓	✓	✓						✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Switch	✓	✓	✓	✓																				
Router	✓	✓	✓	✓						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Repeater	✓	✓	✓	✓						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Modem	✓	✓	✓	✓						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
WLAN access point	✓	✓	✓	✓						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Coaxial cable							✓	✓																
Twisted pair cable							✓	✓					✓	✓										
Fiber optic cable							✓	✓					✓	✓										
Radio frequency								✓	✓	✓	✓	✓	✓	✓										
Microwave								✓	✓	✓	✓	✓	✓	✓										
satellite								✓	✓	✓	✓	✓	✓	✓										
Communication server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SCADA Server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Historian Server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HMI	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile server	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PC/ laptop	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart phone/ tablet	✓	✓	✓	✓	✓					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System employees																								
System Clients																								
3rd party stuff																								
Building & site						✓												✓						

FIGURE 12: Snapshot of what/where matrix.

Vulnerability	Remote station				Communication device							wire media			Wireless media			Master station				corporate network				People			Building & site					
	Sensor c1	Actuator c2	RTU c3	PLC c4	IED c5	Switch	Router	Repeater	Modem	WLAN access point	Firewall	Coaxial cable	Twisted pair cable	Fiber optic cable	Radio frequency	Microwave	satellite	Communication server	SCADA Server	Historian Server	HMI	Application server	Web server	Mobile server	PC/ laptop	Smart phone/ tablet	System employees	System Clients	3rd party stuff	Building & site				
display information about the system and who operate it																											✓			✓				
unqualified employee																											✓			✓				
leak of skills, knowledge and training																											✓			✓				
sharing password among users																											✓			✓				
password disclosure																											✓			✓				
former employees / contractor expose their system knowledge to external persons																											✓			✓				
account still activated for former employee and partners																			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
isolated sites																			✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓				
Poor maintenance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
absence of Alarm system																			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
weak Windows and Doors controlling																															✓	✓		
Lack or weak of Physical Security Tools	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
using default password	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
No password used	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
using weak password policies	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
sensitive data unprotected with encryption and password protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
unprotected data transferred							✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Critical configurations are not stored or backed up	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
absence or unintended backup procedure																		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Open communication / unprotected protocols are used	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Unsecured wireless networks															✓	✓	✓	✓	✓	✓	✓											✓	✓	
system log not maintained or revised periodically																		✓	✓	✓		✓	✓	✓								✓	✓	
Passwords are not encrypted in transit							✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓								✓	✓
Lack of diversity in communication paths lead to communication failure								✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓								✓	✓
Poor or non-existent software updates magement	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unsecured physical ports	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Inappropriate or unauthorized access controls	✓	✓	✓	✓	✓													✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
absence of UPS and power generator not exists	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
airconditioning failure	✓	✓	✓	✓	✓							✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
lack of redundant hardware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
intrusion detection / pervention software not used, not updated, or not tested												✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
anti-virus / anti-malware not used , not updated, or not tested												✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
no warranty agreement	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
No spares management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Memory overflow																		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
lack of remote access control																		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FIGURE 13: Snapshot of where/when matrix.

steps of the proposed model will be followed to reach the full description of risk scenarios that can exist because of the Hactivist risk agent. Given the predefined lists of six risk identification parameters, as stated in step 1 of the proposed model, in the upper level the following steps will be performed:

- (1) Build the following seven 2D matrices that define the relation between Hactivist and other risk identification parameters.

- (a) The motivation of Hactivist is ideologically and socially (Who/Why matrix).

- (b) Risks Hactivist can cause are destruction of hardware, device compromise, and device misconfiguration (What/Who matrix).

- (c) Penetration tools Hactivist can use are physical attack, malicious code, Web-based attacks and Web application attacks (Who/How matrix).

- (d) The relation between each risk Hactivist can cause and one of his penetration tools he can use is defined in the What/How matrix, such as compromising a device using malicious code or a web-based attack.

Vulnerability	social engineering / phishing	Penetration Tool											
		interception/ eavesdropping / espionage(traffic sniffing / traffic diversion/ Man in the middle)	Exploit kits (sw / fw)	malicious code(worm / trojan/ virus)	Spamming	Web-based attacks (malicious URLs/ web backdoors/ compromise web pages/ browser exploits)	Web application attacks(SQL injection / Code Injection / cross-site scripting/ DDoS attacks)	Botnets	spoofing (E-mail/ IP Address / identity)	physical attack (sabotage /vandalism/ theft /terrorism)	Disaster (heat/ water/ wind/ land sliding)	human error /misuse of resources	malfunction of equipment
sensitive data unprotected with encryption and password protection		✓	✓										
unprotected data transfered		✓	✓	✓									
Critical configurations are not stored or backed up				✓									
absence or untested backup procedure												✓	
Open communication / unprotected protocols are used		✓	✓		✓	✓	✓	✓					
Unsecured wireless networks		✓	✓		✓	✓	✓	✓					
system log not maintained or revised periodically													
Sensitive data are not encrypted in transit		✓	✓	✓									
Lack of diversity in communication paths lead to communication failure			✓										
Poor or non-existent software updates management – vulnerabilities to communications equipment routers, switches, firewalls			✓	✓	✓	✓	✓	✓	✓				✓
Unsecured physical ports		✓								✓			
Inappropriate or unauthorized access controls						✓	✓						
absence of UpS and power generator												✓	

FIGURE 14: Snapshot of when/how matrix.

Risk Agent	Risk Motivations	Risk																
		Physical theft of hardware	Device power failure	destruction of hardware	device compromise	device misconfiguration	site - building destruction	network-wires stealing	network-wires damage	network-wireless signal disruption	data sniffing	data interception	data disclosure	losing data	Physical theft of data	gain physical access	identity network devices	inappropriate control commands
Current Employee		✓	✓	✓	✓			✓	✓	✓		✓	✓	✓	✓		✓	
Current Employee	Convenience		✓	✓	✓			✓	✓	✓		✓	✓	✓	✓		✓	
Current Employee	Monetization			✓	✓							✓	✓	✓				
Current Employee	Revenge		✓	✓	✓	✓		✓				✓	✓	✓			✓	
Former Employee		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Former Employee	Convenience				✓							✓	✓	✓				
Former Employee	Monetization	✓		✓	✓		✓			✓	✓	✓	✓	✓	✓			
Former Employee	Revenge	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
Former Employee	Socially				✓					✓								
Current business partner				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Current business partner	Convenience				✓			✓	✓	✓		✓	✓	✓			✓	
Current business partner	Monetization	✓			✓			✓	✓			✓	✓	✓			✓	
Former business partner		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Former business partner	Convenience				✓						✓	✓	✓	✓			✓	
Former business partner	Monetization	✓		✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Former business partner	Revenge	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	
Customer												✓	✓					
Customer	Convenience											✓	✓					
Customer	Monetization											✓			✓			

FIGURE 15: Snapshot of what/who/why matrix.

Agent	Penetration Tools	Risk																
		Physical theft of hardware	Device power failure	destruction of hardware	device compromise	device misconfiguration	site - building destruction	network-wires stealing	network-wires damage	network-wireless signal disruption	data sniffing	data interception	data disclosure	losing data	Physical theft of data	gain physical access	identity network devices	inappropriate control commands
Cyber Criminal group	data manipulation or forging	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	social engineering / phishing										✓	✓	✓			✓		✓
	Exploit kits (sw / fw)				✓					✓	✓	✓	✓	✓				
	malicious code (worm / trojan / virus)				✓					✓	✓	✓	✓	✓				
	Spamming				✓									✓			✓	
	Web-based attacks (malicious URLs/ web backdoors/ compromise web pages/ browser exploits)				✓					✓	✓	✓					✓	
	Web application attacks (SQL injection / Code Injection / cross-site scripting/ DDoS attacks)				✓					✓	✓	✓	✓			✓		
	Botnets																	
	spoofing (E-mail/ IP Address / identity)														✓	✓		✓
	physical attack (sabotage /vandalism/ theft /terrorism)	✓	✓	✓			✓	✓	✓				✓	✓			✓	✓
Cyber Terrorist	data manipulation or forging	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	malicious code (worm / trojan / virus)				✓					✓	✓	✓	✓	✓			✓	
	Web-based attacks (malicious URLs/ web backdoors/ compromise web pages/ browser exploits)				✓					✓	✓	✓					✓	

FIGURE 16: Snapshot of what/who/how matrix.

Component	Risk	Vulnerabilities											
		Poor or non-existent software updates management – vulnerabilities to communications equipment routers, switches, firewalls	Unsecured physical ports	Inappropriate or unauthorized access controls	absence of UpS and power generator not exists	airconditioning failure	lack of redundant hardware	intrusion detection / prevention software not used, or not tested	anti-virus / anti-malware not used, or not tested	no warranty agreement	No spares management	Memory overflow	lack of remote access control
SCADA Server	software failure												
	equipment crash												
	Physical theft of hardware	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
	Device power failure												
	destruction of hardware												
	device compromise												
	device misconfiguration												
	data sniffing												
	data interception												
	data distortion												
	data discloser												
	losing data												
	Physical theft of data												
	gain physical access												
	gain remote access												
	inappropriate control commands												
	identify network devices												
	gain device administrator password												
	hardware failure												
	bypass admin password												
	Disable Device												
	network outage												
	software failure												
	equipment crash												
Historian Server	Physical theft of hardware	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
	Device power failure												
	destruction of hardware												
	device compromise												

FIGURE 17: Snapshot of what/where/when matrix.

Risk	Penetration Tool	Vulnerability											
		Unsecured wireless networks	system log not maintained or revised periodically	Sensitive data are not encrypted in transit	Lack of diversity in communication paths lead to communication failure	Poor or non-existent software updates management – vulnerabilities to communications equipment routers, switches, firewalls	Unsecured physical ports	Inappropriate or unauthorized access controls	absence of UpS and power generator not exists	airconditioning failure	lack of redundant hardware	intrusion detection / prevention software not used, or not tested	anti-virus / anti-malware not used, or not tested
Physical theft of hardware	physical attack (sabotage /vandalism/ theft /terrorism)						✓				✓		
Device power failure	physical attack (sabotage /vandalism/ theft /terrorism)						✓				✓		
Device power failure	Disaster (heat/ water/ wind/ land sliding)									✓	✓		
Device power failure	human error /misuse of resources										✓		
destruction of hardware	physical attack (sabotage/vandalism/ theft /terrorism)						✓				✓		
destruction of hardware	Disaster (heat/ water/ wind/ land sliding)									✓	✓		
destruction of hardware	human error /misuse of resources										✓		
device compromise	malicious code(worm / trojan/ virus)			✓		✓						✓	✓
device compromise	Web-based attacks (malicious URLs/ web backdoors/ compromise web pages/ browser exploits)	✓				✓		✓				✓	✓
device compromise	Web application attacks(SQL injection / Code Injection / cross-site scripting/ DDoS attacks)	✓				✓		✓				✓	✓
device misconfiguration	malicious code(worm / trojan/ virus)			✓		✓						✓	✓
device misconfiguration	Web-based attacks (malicious URLs/ web backdoors/ compromise web pages/ browser exploits)	✓				✓		✓				✓	✓
device misconfiguration	Web application attacks(SQL injection / Code Injection / cross-site scripting/ DDoS attacks)	✓				✓		✓				✓	✓
site- building destruction	physical attack (sabotage /vandalism/ theft /terrorism)						✓				✓		
site- building destruction	Disaster (heat/ water/ wind/ land sliding)									✓	✓		
site- building destruction	human error /misuse of resources									✓	✓		
network wires stealing	physical attack (sabotage /vandalism/ theft /terrorism)						✓				✓		

FIGURE 18: Snapshot of what/ when/ how matrix.

- (e) For each risk a Hactivist can cause, define all system components that can be affected by this risk in the What/Where matrix, such as device misconfiguration that can affect components like the PLC, actuator, Communication server, etc.
- (f) For each component that could be attacked by Hactivist, determine the component's vulnerabilities in the Where/When matrix, such

as open communication/unprotected protocols and poor or non-existent software updates management vulnerabilities for communication server.

- (g) The relations among system components Hactivist can attack and penetration tools he can use are defined in the How/Where matrix, such as physical attacks on a SCADA server component.

FIGURE 19: The entity relationship diagram of the proposed model's database.

FIGURE 20: Total number of risk scenarios per risk.

(2) After that, the previous 2D matrices will be combined to form four 3D matrices, which provide a description of risks caused by a Hactivist agent as follows:

(a) Who/Why and What/Who matrices will be combined to define the relation among Hactivist, his motivation, and risks he can cause (What/Who/Why matrix), such as a Hactivist can cause device compromise because of his ideological motivation.

(b) Who/How and What/How matrices are merged to show risks a Hactivist can cause and by which penetration tools (What/Who/How matrix) such as a Hactivist can cause device misconfiguration risk by using web-based attacks.

(c) What/How and How/Where matrices are combined to specify risks that can be caused by Hactivist using which tool and in what components (What/How/Where matrix), such as

FIGURE 21: Total number of risk scenarios per risk agent.

FIGURE 22: Total number of risk scenarios per risk motivation.

using a physical attack to cause destruction of hardware in HMI.

- (d) What/Where and Where/When matrices are combined to determine in what system component risks can be caused by a Hacktivist and because of what vulnerabilities (What/Where/When matrix), such as destruction of hardware to a PLC due to a lack of or weak physical security tools vulnerability.

- (3) Finally, Algorithm 1 will be used to combine the four 3D matrices of the Hacktivist agent to generate the comprehensive description of possible risk scenarios he can cause. The output of running Algorithm 1 is 306 comprehensive scenarios for risks that can be caused by a Hacktivist agent against the SCADA system.

The 306 risk scenarios the risk agent (Hacktivist) can cause are represented in a graphical representation, as shown in Figure 24. All risk identification parameters are coded to be

FIGURE 23: Total number of risk scenarios per penetration tool.

used in the graphical representation in a readable manner. All parameters' values and codes are summarized in Table 1. Every path from the Hactivist Risk agent (A10) at the most left-hand side until Risk (R3, R4, and R5) at the most right-hand side represents an individual comprehensive risk scenario caused by a Hactivist agent. The path starts from a Hactivist node (A10) passing through motivations (M), penetration tools (PT), vulnerabilities (V), and components until it reaches the Risk (R) caused by this attack scenario. In Figure 24, three examples of 306 Hactivist scenarios have been distinguished based on color into green, blue, and red as follows:

- (i) In the green scenario, Hactivist (A10), because of his social motivation (MO4), can use malicious code (PT4) to cause a device compromise (R4) to any router (CD2) when sensitive data are not encrypted in transit vulnerability (V23) occurs.
- (ii) In the red scenario, Hactivist (A10), because of his social motivation (MO4), can use Web-based attacks (PT6) to cause a device misconfiguration risk (R5) to any Communication server (MS1) in the SCADA system when the open communication/unprotected protocols vulnerability (V20) are used.
- (iii) In the blue scenario, Hactivist (A10), because of his ideological motivation (MO5), can use a physical attack (PT10) to destroy the hardware (R3) of any SCADA server (MS2) when a lack of or weak Physical Security Tools vulnerability (V12) occurs.

The other risk scenarios that affect the SCADA system by a Hactivist can be traced using the graphical representation in Figure 24 and the risk parameters value codes in Table 1. Figure 21 shows the total number of risk scenarios that can be affected in the SCADA system for each risk agent.

7.2. Case Study 2. Another question from SCADA and security managers the proposed model and benchmark DB

can answer is who are the risk agents that can cause a specific risk to the system, and what are the scenarios for that risk? To answer this type of question, the proposed model will be applied to gaining physical access as an example of a risk that can affect the system. Starting from the gaining physical access risk, the seven 2D matrices related to this risk will be built. These 2D matrices will then be combined to form the four 3D matrices for the gaining physical access risk. Finally, Algorithm 1 will be run to generate the possible scenarios for this risk. There are 387 scenarios that can result from gaining physical access to a system. These resulting scenarios for this risk are graphically represented in Figure 25, which shows that there are eight agents that can cause the gaining physical access risk on 23 system components. The total possible risk scenarios for each risk are summarized in Figure 20.

8. Conclusion and Future Work

SCADA systems are one of the most critical industrial systems because of their functionality in supervising and controlling large and worldwide industrial networks, such as electricity and gas distribution networks. Their criticality nature exposes them to a large set of risks from either natural or human sources. To manage these risks, a powerful risk management framework is needed to predict the most significant risks and handle them correctly. This framework should be based on a comprehensive risk identification step. In this paper, the most important parameters that are needed to define SCADA risks were outlined. Then, previous works in the field of risk identification phases of SCADA systems were discussed. A comparative study was provided based on a number of risk identification parameters and the level of mapping between these parameters. Then, a comprehensive model for risk identification of SCADA systems was proposed. This model used the hierarchical representation methodology to build the model, which started from defining all risk parameters and mapping them gradually into 2D

FIGURE 24: Possible Risk scenarios on SCADA system by Hactivist attacker.

FIGURE 25: Possible Risk scenarios on SCADA system cause gain physical access.

matrices and on to a 6D matrix. This 6D matrix represented the relations among six risk parameters that were defined to draw complete risk scenarios. Finally, this model was used to build a benchmark database containing 19,163 risk scenarios that could be applied to SCADA systems.

In the future, a classification model should be built using this database to generate a set of rules that could be used further in analyzing and assessing the risks affecting any SCADA system. Then, a simulation for managing SCADA system risks should be developed.

Input: amr is the agent motivation risk matrix, atr is agent tool risk matrix, rvt is the risk vulnerability tool matrix and crv is the component risk vulnerability matrix

Output: RSM is Risk Scenarios Matrix which maps (agent, motivation, risk, tool, vulnerability, component).

Begin

```

1  Fetch all data from amr.
2  for all  $amr_i \in amr$  do
3      current_agent =  $amr_i$ .agent
4      current_motivation =  $amr_i$ .motivation
5      current_risk =  $amr_i$ .risk
6      Fetch all tools from atr matrix as amr_tools where atr.agent = current_agent and atr.risk = current_risk
7      for all  $amr\_tools_j \in amr\_tools$  do
8          current_tool =  $amr\_tools_j$ .tool
9          Fetch all vulnerabilities from rvt matrix as amrt-vulnerabilities where rvt.risk = current_risk and rvt.tool =
            current_tool
10         for all  $amrt\_vulnerabilities_k \in amrt\_vulnerabilities$  do
11             current_vulnerability =  $amrt\_vulnerabilities_k$ .vulnerability
12             Fetch all components from crv matrix as amrtv-components where crv.risk = current_risk and
            crv.vulnerability = current_vulnerability
13         for all  $amrtv\_components_i \in amrtv\_components$  do
14             current_component =  $amrtv\_components_i$ .component
15             Insert into RSM ( $current\_a\_gent$ , current-motivation, current_risk, current_tool, current_vulnerability,
            current- component).
16         end for
17     end for
18 end for
19 end for
End

```

ALGORITHM 1: Generate 6-dimension SCADA risk matrix.

Data Availability

The data used to support the findings of this study are included within the supplementary information file(s) (available here).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Supplementary Materials

Supplementary material file is a compressed file that contains two files: a. The first file “SCADA Risk identification data.xlsx” is a spreadsheet file that contains the full mapping of the risk identification parameters stated in the paper as 2D and 3D matrices. The snapshots of these matrices were presented in the paper. b. The second file “scada_risk_scenarios.sql” is sql script of our proposed model database. This database contains the six tables for coding the six risk identification parameters and four tables for four 3D matrices demonstrated in the model. The last table “risk_scenarios” is the 6D matrix that was produced by Algorithm 1 to present the full mapping of risk identification scenarios. This table contains 19163 scenarios that can be used as risk scenario for using in the risk assessment purpose of SCADA systems. (*Supplementary Materials*)

References

- [1] T. Macaulay and B. L. Singer, *Cybersecurity for Industrial Control Systems*, CRC Press, Boca Raton, Fla, USA, 2012.
- [2] K. Markantonakis and K. Mayes, *Secure Smart Embedded Devices, Platforms and Applications*, Springer New York, New York, NY, USA, 2014.
- [3] J. Gao, J. Liu, B. Rajan et al., “SCADA communication and security issues,” *Security and Communication Networks*, vol. 7, no. 1, pp. 175–194, 2014.
- [4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA security in the light of cyber-warfare,” *Computers & Security*, vol. 31, no. 4, pp. 418–436, 2012.
- [5] M. Riis and T. Sjomoe, *Integration between SCADA Systems and Hydraulic Network Simulation Models*, 2016, <http://hdl.handle.net/11250/2433613>.
- [6] A. Rezai, P. Keshavarzi, and Z. Moravej, “Secure SCADA communication by using a modified key management scheme,” *ISA Transactions*, vol. 52, no. 4, pp. 517–524, 2013.
- [7] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, “Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,” *Applied Soft Computing*, vol. 71, pp. 66–77, 2018.
- [8] A. Rezai, P. Keshavarzi, and Z. Moravej, “Key management issue in SCADA networks: a review,” *Engineering Science and Technology, an International Journal*, vol. 20, no. 1, pp. 354–363, 2017.
- [9] E. Luijck, “SCADA security good practices for the drinking water sector,” 2008, http://publications.tno.nl/publication//KpvrNU/TNO-DV2008C096_web.pdf.

- [10] S. Karnouskos and A. W. Colombo, "Architecting the next generation of service-based SCADA/DCS system of systems," in *Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011.
- [11] C. Nan, I. Eusgeld, and W. Kröger, "Analyzing vulnerabilities between SCADA system and SUC due to interdependencies," *Reliability Engineering & System Safety*, vol. 113, no. 1, pp. 76–93, 2013.
- [12] A. Rezai, P. Keshavarzi, and Z. Moravej, "Advance hybrid key management architecture for SCADA network security," *Security and Communication Networks*, vol. 9, no. 17, pp. 4358–4368, 2016.
- [13] O. Andreeva, S. Gordeychik, G. Gritsai et al., "Industrial control systems and their online availability," 2016, https://kas.pr/KL_ICSAvailabilityStatistics.
- [14] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489–496, 2014.
- [15] International Organization for Standardization, "Risk management Principles and guidelines," ISO 31000, 2018, <https://www.iso.org/obp/ui/iso:std:iso:31000:ed-2:v1:en>.
- [16] D. Kasap and M. Kaymak, "Risk identification step of the project risk management," in *Proceedings of the Portland International Conference on Management of Engineering and Technology*, pp. 2116–2120, 2007.
- [17] Y. Cherdantseva, P. Burnap, and A. Blyth, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1–27, 2016.
- [18] E. Byres and M. Fabro, "RISI - The Repository of Industrial Security Incidents," 2015, <http://www.risidata.com/Database>.
- [19] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2018, <https://ics-cert.us-cert.gov/>.
- [20] E. Bompard, T. Huang, Y. Wu, and M. Cremenescu, "Classification and trend analysis of threats origins to the security of power systems," *International Journal of Electrical Power & Energy Systems*, vol. 50, no. 1, pp. 50–64, 2013.
- [21] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 380–388, Dalian, China, 2011.
- [22] R. Hewett, S. Rudrapattana, and P. Kijsanayothin, "Cyber-security analysis of smart grid SCADA systems with game models," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, pp. 109–112, Tennessee, Tenn, USA, 2014.
- [23] K. Stouffer, V. Pillitteri, S. Lightman et al., "Guide to industrial control systems security (NIST SP 80082)," 2015, <http://dx.doi.org/10.6028/NIST.SP.800-82r2>.
- [24] W. B. Miller, D. C. Rowe, R. Helps et al., "A comprehensive and open framework for classifying incidents involving cyber-physical systems," in *Proceedings of the 2014 IAJC/ISAM Joint International Conference*, 2014.
- [25] J. C. H. Gabriel, M. Y. Jose, and L. A. Roberto, "Using inter-connected risk maps to assess the threats faced by electricity infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3, pp. 197–216, 2013.
- [26] A. M. Elhady, A. Abou Elfetouh, H. M. El-bakry et al., "Generic Software risk management framework for SCADA system," *International Journal of Computer Applications*, vol. 70, no. 3, pp. 45–52, 2013.
- [27] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Information and Software Technology*, vol. 55, no. 12, pp. 2049–2075, 2013.
- [28] National Institute of Standards and Technology (NIST), 2018, <https://www.nist.gov/>.
- [29] European Union Agency for Network and Information Security (ENISA), 2019, <https://www.enisa.europa.eu/>.
- [30] United State Department of Homeland Security (US. DHS), 2018, <https://www.dhs.gov/>.
- [31] W. Schwab and M. Poujol, "The state of industrial cybersecurity 2018," 2018, <https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf>.
- [32] Communication network dependencies for ICS/SCADA Systems, 2016, <https://www.enisa.europa.eu/publications/ics-scada-dependencies>.
- [33] B. G. Brown and D. Wylie, "Securing Industrial Control Systems," 2017, <https://www.tripwire.com/solutions/industrial-control-systems/sans-state-of-ics-report-register/>.
- [34] Generic SCADA Risk Management Framework for Australian Critical Infrastructure, 2012, <https://www.tisn.gov.au/Documents/SCADA-Generic-Risk-Management-Framework.pdf>.
- [35] Common cyber security vulnerabilities in industrial control systems, 2009, <https://www.hsd.org/?view&did=7970>.
- [36] M. Nasser, R. Ahmad, W. Yassin et al., "Cyber-security incidents: a review cases in cyber-physical systems," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, 2018.
- [37] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," *Journal of Industrial Information Integration*, vol. 5, pp. 6–16, 2017.
- [38] P. Eden, P. Burnap, A. Blyth et al., "A forensic taxonomy of SCADA systems and approach to incident response," in *Proceedings of the 3rd International Symposium for ICS and SCADA Cyber Security Research*, pp. 27–39, 2015.
- [39] P. S. Woo and B. H. Kim, "A study on quantitative methodology to assess cyber security risk of SCADA systems," *Advanced Materials Research*, vol. 960-961, pp. 1602–1611, 2014.
- [40] A. F. Guillermo, T. David, and D. Joshua, "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems," in *Proceedings of the 2012 world congress in computer science, computer engineering, and applied computing*, 2012.
- [41] R. Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*, Goldman School of Public Policy. University of California, 2010.
- [42] D. Kang, J. Lee, S. Kim et al., "Analysis on cyber threats to SCADA systems," in *Proceedings of the 2009 Transmission and Distribution Conference and Exposition: Asia and Pacific*, 2009.
- [43] National Vulnerability Database (NVD), 2019, <https://nvd.nist.gov/>.
- [44] Common Vulnerabilities and Exposures (CVE), 2019, <https://cve.mitre.org/>.
- [45] Bugtraq Team, 2016, <http://bugtraq-team.com/>.
- [46] Open Sourced Vulnerability Database (OSVDB), 2017, <https://blog.osvdb.org/>.

- [47] Open Vulnerability and Assessment Language (OVAL), 2016, <http://oval.mitre.org/>.
- [48] L. Marinos, A. Belmonte, and E. Rekleitis, “enisa threat landscape 2015,” 2016, https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport.
- [49] Mysql.com, 2018, <https://www.mysql.com/>.