Received: 14 January 2019 | Revised: 27 May 2019 | Accepted: 25 June 2019

DOI: 10.1002/smr.2219

SPECIAL ISSUE - EMPIRICAL

WILEY Journal of Software: Evolution and Process

A security risk mitigation framework for cyber physical systems

Maryam Zahid[1] | Irum Inayat[2] | Maya Daneva[3] | Zahid Mehmood[4]

[1] Software Engineering and Automation Lab (SEAL), National University of Computer and Emerging Sciences, Islamabad, Pakistan

[2] Capital University of Science and Technology, Islamabad, Pakistan

[3] Services, Cybersecurity & Safety (SCS), Faculty of Electrical Engineering, Mathematics & Computer Science,, University of Twente, Enschede, The Netherlands

[4] Department of Electric Engineering, University of Lahore, Islamabad, Pakistan

Correspondence
Irum Inayat, Software Engineering and Automation lab (S.E.A.L), National University of Computer and Emerging Sciences. Islamabad, Pakistan.
Email: irum.inayat@nu.edu.pk

Abstract

Cyber physical systems (CPSs) are safety-critical, be it weapon systems, smart medical devices, or grid stations. This makes ensuring security of all the components constituting a CPS unavoidable. The rise in the demand of interconnectedness has made such systems vulnerable to attacks, ie, cyberattacks. Over 170 cases of cybersecurity breaches in CPS were reported over the past two decades. An increase in the number of cyberattack incidents on CPS makes them more exposed and less trustworthy. However, identifying the security requirements of the CPS to pinpoint the relevant risks may help to counteract the potential attacks. Literature reveals that the most targeted security requirements of CPS are authentication, integrity, and availability. However, little attention has been paid on certain crucial security attributes such as data freshness and nonrepudiation. One major reason of security breaches in CPS is the lack of custom or generalized countermeasures. Therefore, we propose a security risk mitigation framework for a CPS focused on constraints, ie, authentication, data integrity, data freshness, nonrepudiation, and confidentiality. Furthermore, we evaluate the proposed work using a case study of a safety critical system. The results show a decrease in the severity of the identified security risks, ie, man-in-the-middle attack, spoofing, and data tempering.

KEYWORDS

case study, cryptosystem, cyber physical systems (CPS), cyber security, risk assessment, risk identification, risk management, risk mitigation, security

1 | INTRODUCTION

Following the fourth industrial revolution came forward a new type of complex embeded system, namely Cyber Physical Systems (CPSs),[1] having constantly monitored, controlled, and coordinated operations integrated by a core based on Internet of Things (IoT).[2] Successful applications of such systems include communications systems, home appliances, automotive electronics, games, toys, weapons, Supervisory Control and Data Acquisition (SCADA) systems deployed in various critical infrastructures including grid stations, industrial control systems, and public transport systems, to name a few. The requirements of constant connectivity among physical objects and the user of such systems are complex in nature due to limited computation power, bandwidth, storage, and power consumption issues.

However, security is the main feature CPS relies on to gain the trust of its users. Recent cyberattacks on CPS include hacking of smart pacemaker, braking systems of Tesla S-Model autonomous vehicle, and complete blackouts in various cities across North America, Russia, China, and Ukraine.[3] Man-in-the-middle (MitM) attack, botnet attack, spoofing, and denial of service (DoS) are among the top most common cyberattacks on IoT/CPS.[4] With an enhancement in services, more security vulnerability is expected due to interaction with the external networks.[5] The recent incidents recorded on cyberattacks reveal smart grids being the most vulnerable to security risks leading to massive financial loss and damage

 © 2019 John Wiley & Sons, Ltd.

to other critical infrastructures connected to it.[6] Trust in CPS has become especially challenging in hospitals and other domains of medical sciences due to the involvement of human lives.[7] The smart transportation systems are also fighting to minimize, if not eliminate, the security risks in systems in fear of there being a possible scenario of a catastrophic event resulting from a cyberattack.[8,9] Violating the privacy policies can give rise to security concerns, which eventually results in lack of users' trust in the system.[10] For gaining the public's trust in CPS, it is of utmost importance to ensuring the system's adequate handling of privacy and security threats.[11]

Implementing complex security requirements will require the use of risk analysis and mitigation along with elicitation and modeling of the requirements to determine the importance of these requirements within the system. Over the years, many security measures have been proposed to mitigate the identified security risks in both the physical layer and the network layer of CPS but have significantly shown less interest on mitigating security risks at the application layer of CPS. The traditional information technology (IT) security measures such as firewalls, authentication, cryptosystems, and intrusion detection systems, to name a few, are limited to cyber domain only.[8] Therefore, the traditional security protocols and mechanisms may not be applied to the systems embedded with physical processes and computation.[1]

This paper discusses the development of an application layer-specific risk mitigation framework for mitigating cyber security risks targeting authentication, data freshness, data integrity, confidentiality, and nonrepudiation that contributes to reducing the impact of the security risks within CPS.

Following the introduction of this paper, we provide an overview of the related work on the security in CPS and risk management processes adopted to minimize their impact on the system. Section 3 presents our proposed solution followed by its evaluation using multiple case studies in Section 4. Before concluding the paper, we present the results and discussion in Section 5.

2 | RELATED WORK

Our related work includes two streams of literature: on security requirements and risks to CPSs and on risk management. These are presented in Section 2.1 and 2.2, respectively.

2.1 | Security in CPS

2.1.1 | Security requirements in CPS

Although the security requirements of a CPS vary from those of a traditional IT system due to the involvement of sensors and actuators working simultaneously, there is a commonality in the security attributes in both types of systems. Security attributes such as authentication confidentiality,[12] availability, reliability, trust, data integrity,[13] liability, data freshness, fault tolerance, resilience, self-healing,[14] authorization, anonymity,[15] linkability, and nonrepudiation[16] apply to both types of systems. In CPSs, the implementation of these security attributes varies according to the layer of CPS applied; for example, the perception layer responsible for data collection must ensure confidentiality, authentication, trust, and nonrepudiation, the transmission layer responsible for data transmission must ensure authentication, data integrity, confidentiality, availability, and fault tolerance, while the application layer responsible for data analysis and control decision making must ensure authentication, data freshness, authorization, confidentiality, and reliability.[17]

Every sector in the economy implementing CPS has a different set of security requirements with the highest priority and vulnerability level. These requirements can be classified as sensing, storage, communication, and actuation control and feedback security.[18] Availability, confidentiality, and integrity are considered to be the three main security objectives in a smart grid, and thus the cyberattacks on smart grids can also be classified according to the security objective targeted.[19]

2.1.2 | Security risks in CPS

The source of the security risks in CPS range from poor implementation of the design protocols, risk management principles, cyber laws, and regulations to poor maintenance of both the software and the hardware.[20] The security threats to a CPS recorded range from physical destruction, theft, inside job to cyberattacks such as privacy leakage, malicious code, spoofing, MitM attack, DoS, cache poisoning, wormhole attack, blackhole attack, unauthorized access, selective forwarding, rushing attack, data tempering, and system hijacking.[5,21] For every CPS system such as industrial control systems, smart grids, remote medical devices, and smart cars, the factors against each of the categorized threat varies, which is a result of isolation assumptions, cyber vulnerabilities, cyber-physical vulnerabilities, increase in connectivity, and heterogeneity.[13] On the other hand, some of the major cyberattacks on CPS reported are compromised-key attacks, MitM attacks, eavesdropping, DoS, and spoofing.[19]

2.2 | Risk management

Risk management involves the process of identifying risks, analyzing the impact of the identified risks, mitigating the risks to reduce their impact on the system, and monitoring the system for any risks left unattended.[22]

2.2.1 | Risk identification

Risk identification being the first step to manage risks for the software to be developed involves identifying the ways in which a misuser, ie, a hacker can pose a threat to the system, or an undesired event such as a natural disaster or an accident can cause a system or a subsystem to fail or show abnormal behavior.[23,24]

Source, target, motive, attack vector, and potential consequences are the five common factors identified against every threat to CPS security categorized as physical threats, political threats, criminal threats, and privacy threats. Presence of defects in the software development life cycle contributes to the origin of security vulnerabilities in software systems and thus requires an improvement in the general quality of the product development.[25] Risk identification is the starting point of risk management identifying any possible risks from both the requirements and the architecture of the software system. A study[26] conducted on risk identification categorized instruction detection techniques into four types, ie, anomaly-based, specification-based, signature-based, and reputation-based instruction detection techniques. According to this study, behavior- and traffic-based collection in various wireless systems is important for detecting attacks in such systems The ability of misuse cases to depict the possible ways in which a hacker can affect the original functionalities of the system or manipulate the data processed by the system allows us to not only identify the security requirements necessary to implement, but also represents the possible risks that the software system needs mitigation measures for.[20,27] On the basis of this knowledge, the existing attack detection methods can be classified in four schemes namely signal-based, packet-based, proactive, and hybrid schemes, while the mitigation techniques can be classified on the basis of the layer applied on, ie, network layer mitigation and physical layer mitigation.[28]

2.2.2 | Risk assessment

This step of risk management involves analyzing the identified risks for the level of impact which they can have on the behavior of the system and their probability of occurrence. The differences between the traditional IT security systems and CPS are based on the identification, assignment and calculation of assets, threats, and vulnerabilities,[14] and thus it is necessary to take fully into consideration the CPS characteristics in order to find a suitable and specific risk assessment method.[15] Simulations and model representing the attack designs can help in the better assessment of risks related to the security of CPS[29] providing theoretical guidelines detecting attacks and resilience controls. Risk strategies are effective when the risks are timely identified. A study conducted on risk assessment approaches divided them into two main categories, namely qualitative and the quantitative approaches depending upon the conditions applied under.[25] The contexts in which qualitative risk assessment techniques are best suitable are those characterized by relatively short amount of time available, small budgets, unavailability of relative data, or insufficient expertise in quantitative analysis on the side of the agents conducting the process of risk assessment .[30] Furthermore, the quantitative risk assessment techniques are best applied when more detailed and accurate risk values are required, and the process involves the participation of a domain expert. Another review conducted on risk assessment techniques classifies them based on the level of detail covered by the technique, the type of risk values assigned to a particular requirement, and the type of method adopted, ie, a formal method or a model based technique.[31] Modeling of attacks involves generation of attack trees and fault trees that can be used to map the identified risks for assessment. Attack trees, although are considered to be self-documenting, are difficult when enumerating concurrent actions and all the actions of an attacker. Fault trees on the other hand are good at explicitly visualizing the relationship between the events and the causes leading to the system failure but become complex when expressing all possible sequences of a large system and, in turn, often fail to visualize the interdependencies between them.[32] Game theoretic approaches have become a commonly used way to identify and analyze the risks related to the security requirements of a system. Although helpful in the identification and analysis of risk severity, these approaches are known to be unreliable due to the factor of biasness resulting from an analyzers' lack of domain knowledge and lack of motivation. Even with such drawbacks, these approaches are known to be a versatile instrument in analyzing the complex systems.[10]

2.2.3 | Risk mitigation

Flaws in the architecture of SCADA systems give away the opportunity to the hackers in exploiting the system's services introducing a risk of brand damage, share price reduction, loss of revenue, and in worst case scenario, a loss of life. To mitigate these risks, various standards and a set of best practices have been established over the years.[30] According to Yan et al,[33] the mitigation measures proposed vary according to the layer applicable at and, in turn, can be categorized as a physical layer mitigation measure,[34] application layer mitigation measure, and network layer mitigation measure. Enforcing security measures at the design phase alone is not enough as it may involve implementing security architecture related constraints that are actually not necessary. Converting security requirements and their associated threats into design decisions throughout

the software development life cycle is another way to mitigate the identified security threats.[35] Encryption, defined authentication principles, access control, digital forensics,[36] remote attestation of embedded devices,[37] management of security incident and events, and intrusion detection can be used to develop a secure supporting infrastructure necessary to accurately store and transmit information to the appropriate application.[38] One of the ways to mitigate the risks related to these security requirements is to implement a cryptographic mechanism that ensures the transmission of secure messages between the sensors and the actuators of the CPS. Over the years, two main types of cryptographic algorithms have been proposed and made practical for use of in the industry, namely symmetric encryption algorithms[39] and asymmetric encryption algorithms.[38] An adaptive framework involving the process of adjusting internal working parameters, eg, encryption algorithms, security protocols, improving quality of service available to applications, and automating reconfigurations of the protection mechanisms while making dynamic changes to the overall security structure of the system can help ensure authentication, confidentiality, nonrepudiation, data freshness, and data integrity.[40] Encryption, defined authentication principles, access control, digital forensics, [36] remote attestation of embedded devices,[37] management of security incident and events, and intrusion detection can be used to develop a secure supporting infrastructure necessary to accurately store and transmit information to the appropriate application.[38] In what follows, we provide some examples of these techniques in specific application domains.

To reduce the impact of cyber threats to an autonomous vehicle while maintaining the performance of the system, a hybrid cryptosystem was introduced consisting of a combination of hashing algorithm for data integrity and data confidentiality checks and advanced encryption scheme (AES)–ECB (Electronic Codebook) for data authentication.[41] Automotive and edge computing systems require complex data processing while ensuring time consistency and memory efficiency. A real-time middleware for cyber-physical event processing embedded with AES-ECB cryptosystem was introduced to help not only keep data transactions secure but also ensure real-time data processing in smart grid systems.[42] To ensure the confidentiality, integrity, and authentication of the data, an advance encryption scheme – Galois/Counter Mode (AES-GCM) was precomputed into the system Graphic Processing Unit (GPU) while reducing the time complexity of the cryptosystem.[43] Another study proposed the application AES-CCM (Counter with Cipher Block Chaining Mode) encryption scheme taking into consideration the SCADA system's limitations related to computation power and real-time requirements.[44] To counter the challenges related to efficient file storage and sharing via authenticated physical devices in a cyber-physical cloud environment, a lightweight identity-based authenticated data sharing protocol using AES-CBC (Cipher Block Chaining Mode) encryption scheme was proposed.[45] Converting security requirements (such as data integrity, data confidentiality, authentication, confidentiality, nonrepudiation, and data freshness) and their associated threats into design decisions throughout the software development life cycle is one way to mitigate the identified security threats.[35] The integration of physical and cyber layer in transportation cyber physical systems (TCPs such as autonomous trains) have made it difficult to implement existing mitigation measures specific only individual layers of CPS.[46] Due to such heterogeneous nature of CPSs (such as the smart grids) communication networks, it is impractical to design a single key management scheme for all the networks in a CPS,[28] and thus have moved toward hybrid cryptosystems involving both symmetric and asymmetric cryptosystems to achieve security objectives. Some of the countermeasures involve the process of adjusting internal working parameters, eg, encryption algorithms (symmetric[39] and asymmetric encryption algorithms[38] or hybrid cryptosystems), security protocols, improving quality of service available to applications, defined authentication principles, access control, digital forensics,[36] remote attestation of embedded devices,[37] management of security incident and events, intrusion detection,[38] and automating reconfigurations of the protection mechanisms while making dynamic changes to the overall security structure of the system.[40] Hybrid cryptosystems have been gaining popularity among the various automotive, medical and industrial systems developed to reduce the impact of cyber threats while maintaining the performance of the system such as combination of hashing and AES-ECB[41] and a combination of ECC with AES-ECB for secure data transaction within the system.[47]

Since CPS includes security critical and safety critical infrastructures,[48] implementation of data freshness and nonrepudiation is of crucial importance to keep the involved human lives protected from possible imminent danger. The risk management techniques proposed in the literature sources in this section are less focused on mitigating risks related to data freshness, nonrepudiation, and data integrity at an application layer of CPS. In most cases, the risk mitigation techniques proposed are applicable either at the physical layer or the network layer of CPS. They lack the focus on trying to mitigate the security requirements at an application layer. Most of the proposed risk mitigation techniques also lack validation.[24,49,50]

3 | PROPOSED SOLUTION

Implementation of appropriate security mechanisms at an application layer of CPS is necessary due to its accessibility to the data transmitted by the nodes and its ability to process that data accordingly. Our proposed risk mitigation framework consists of four steps, as show in Figure 1:

3.1 | Steps 1 and 2: Extraction of security requirements and risk identification

During Steps 1 and 2, a modeling technique known as “Misuse Cases” is used to not only extract security requirements against the software system but also identify the possible security risks associated with those requirements. Misuse cases allow us to depict the possible ways the original functionalities of the system and the data processed by the system can be manipulated. These can easily be constructed alongside use cases during the designing of the software system under development.[20]

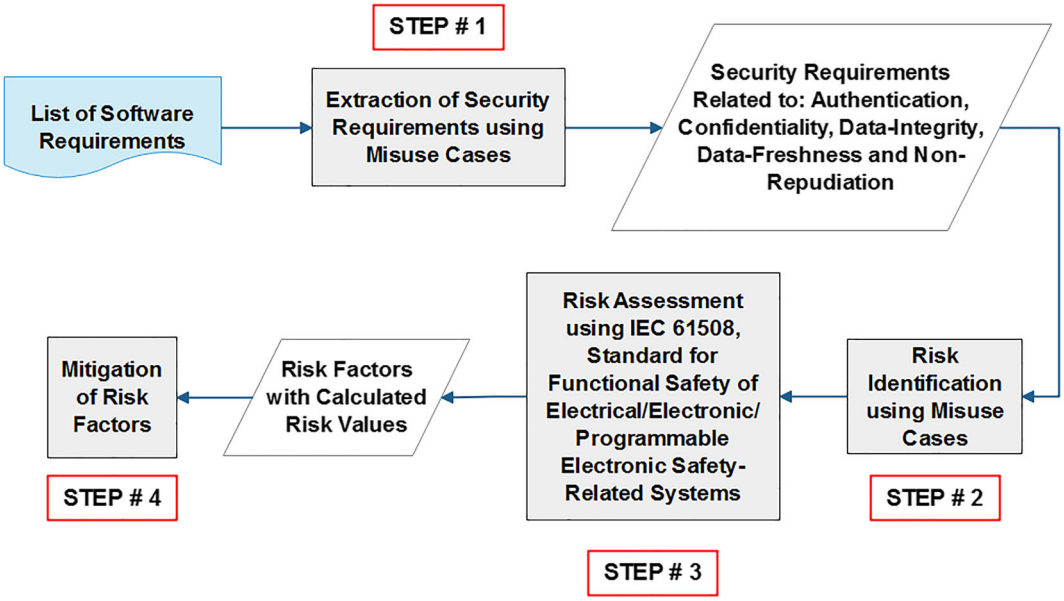

FIGURE 1 Abstract model of the proposed mitigation framework

3.2 | Step 3: Risk assessment

The risk assessment in Step 3 of our framework (see Table 1) involves the use of fault tree analysis for detailed quantitative assessment[51] along with the safety integrity levels (SILs) defined in standards: EN-50128 (for railway software),[52] which are based on a common standard defined by IEC (International Electrotechnical Commission), IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems[52,53] standard), used during the development of a safety critical system from any field of application.

The safety integrity levels used can be seen in the Table 2 below:

The SILs 1 to 4 represent the severity of the risk; in this case, level 1 represents a risk of low severity level while level 4 represents the risk of the highest severity level. The risk values (probability of failure) calculated is based on the formula as follows:

$$\text{Risk} = \text{Likelihood of occurrence} \times \text{Severity of Risk} \tag{1}$$

Equation 1, used as a part of our framework, combines the qualitative or semiquantitative severity level ratings and the probability of occurrence to evaluate risk values. This provides a greater differentiation of risks evaluated based on the actual data recorded over the years, which is crucial for developing any safety critical system. The SILs (see the first column of Table 2) assigned to each of the system's components are based on both their usage and the possible type of threat it poses toward the system and its users. Since the evaluated fault tree provides us with a quantitative analysis of the risks identified, it is considered to be more accurate. This in turn will help us understand more clearly the severity of the analyzed risk in safety-critical and security-critical systems and plan its mitigation and system design accordingly. The involvement of IEC 61508 as the basis of the risk management standard EN 50129 for railway makes our framework generalizable not only for the development of the software related to railway but also to the software of other domains such as avionics.

TABLE 1 Risk assessment steps

Steps to Calculating Risk Values
1: Select a possible risk identified using Misuse Cases
2: Draw a fault tree based on risk in focus
3: Identify all possible cut-sets
4: Apply Boolean algebra to identify minimum cut-sets
5: Using existing literature and recorded incidents, extract the frequency of that base event to occur
6: Based on the component's mode of operation, extracted frequency, and possible level of damage it can cause, select SIL
7: Using the selected SIL and extracted frequency value, calculate the risk value (probability of failure) for each base event
8: Substituting the calculated risk values for each base event into the equation for minimal cut-set, calculate the risk value (probability of failure) of the risk factor being analyzed

Abbreviation: SIL, safety integrity level.

TABLE 2 Safety integrity levels from IEC 61508 standard

SIL	Continuous and High Demand Rate (Dangerous Failures/Hr)	Low Demand Rate (Probability of Failure on Demand)
4	$\geq 10^{-9}$ to 10^{-8}	$\geq 10^{-5}$ to 10^{-4}
3	$\geq 10^{-8}$ to 10^{-7}	$\geq 10^{-4}$ to 10^{-3}
2	$\geq 10^{-7}$ to 10^{-6}	$\geq 10^{-3}$ to 10^{-2}
1	$\geq 10^{-6}$ to 10^{-5}	$\geq 10^{-2}$ to 10^{-1}

Abbreviation: SIL, safety integrity level.

3.3 | Step 4: Risk mitigation

Over the years, the mitigation measures proposed for the application layer of CPS ranged from application of coding standards, intrusion detection, and trust management, to end-to-end encryption and authentication and authorization. Implementing a cryptographic mechanism ensures the transmission of secure messages between the sensors and the actuators of the CPSs while checking for authenticity of the data and the nodes in the CPS. For mitigating the risks related to confidentiality, authentication, nonrepudiation, and data integrity, we will be using a hybrid cryptosystem[17] based on the combination of RSA (River-Shamir-Adleman) and Triple Data-Encryption Standard (DES) (3DES) eliminating the process of key management to reduce the time complexity of the encryption/decryption mechanism and making it memory efficient, and CMCIAA (Combined Method for Confidentiality, Integrity, Availability, and Authentication) encryption method.[54] The freshness of the data will be checked for at the receiver's end based on the appended date and time of encryption to the message at the beginning of the encryption process. As far as nonrepudiation is concerned, the signature generated by the RSA encryption scheme allows the system to check for nonrepudiation. This also in turn allows the system to check for data integrity and reliability. On the other hand, the 3DES encryption scheme combined with the RSA and the CMCIAA encryption schemes checks for authentication of the data transmitted between sensors and actuators.

4 | EVALUATION

For evaluating our proposed framework, we simulated both active and passive cyberattacks, namely MitM attack and spoofing, on fire alarm system simulation for railway cabin. Fire alarm system simulation is an open-source software developed in JAVA programming language.[55] The fire alarm system simulates a situation where a fire breaks out inside a train cabin and allows the user to simulate the actions that are required to be performed for containing the fire. To reduce the impact of the incident, the system allows the operator to (a) open any closed doors, (b) activate fire alarms and water sprinkler, (c) shut down power equipment operating at locations under fire, and (d) contact emergency services. The system simultaneously records the total time taken to contain the situation and presents the user with the summary of the damage done by the fire. The system is presented in Figure 2. Therein, the symbols S (colored yellow), S (colored blue), A, E, exit, purple line, and brown lines represent fire detection sensors, water sprinklers, fire alarms, power equipment, exit points, doors, and walls of the train cabin, respectively. The grid containing fire and the grids to which the fire has spread turn red in color represent areas with fire breakout.

Based on the software system requirements provided for the system, a list of security requirements along with related security risks were identified using the misuse cases drawn. The identified risks were further analyzed with the help of fault tree analysis. Existing literature and incidents recorded on security breach were used to calculate the likelihood of the risks identified. Using the data collected on the likelihood of the component's mode of operation and estimated level of damage, the risk in focus can cause a SIL was selected. Once we obtained the likelihood of occurrence and the SIL, we calculated the risk values for each of risks identified and analyzed.

During mitigation phase of the framework, the software system selected for this evaluation was first subjected to the selected active and passive attacks, using which we captured the ways a hacker can access and manipulate the captured data. We implemented our encryption scheme at the fire detection nodes and the central agent, which was responsible for establishing a secure communication channel for the sensor data and the commands to travel between the sensor nodes and central agent of the system. The performance measures used to evaluate the framework consisted of not only both the encryption and decryption times recorded but also the resources used by the cryptosystems compared with.

5 | RESULTS

5.1 | Execution of framework

5.1.1 | Steps 1 and 2: Extraction of security requirements and risks identification

Misuse cases not only helped identify the security requirements of this system but also helped identify the risks associated with the extracted set of security requirements. According to the misuse case (see Figure 3), the system continuously detected the location of a fire breakout inside a

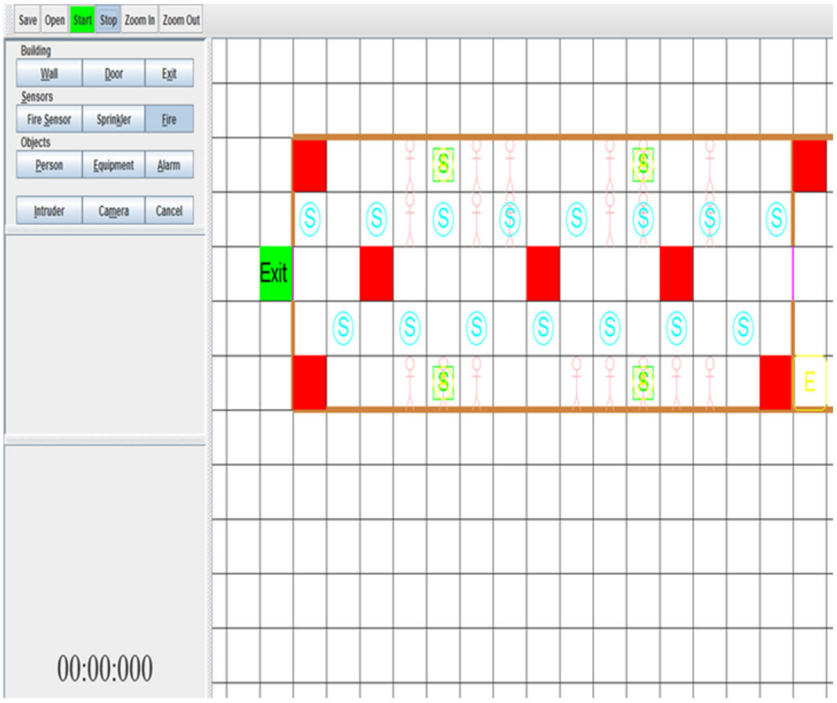

FIGURE 2 Fire alarm system simulation for railway cabin (Graphical User Interface)

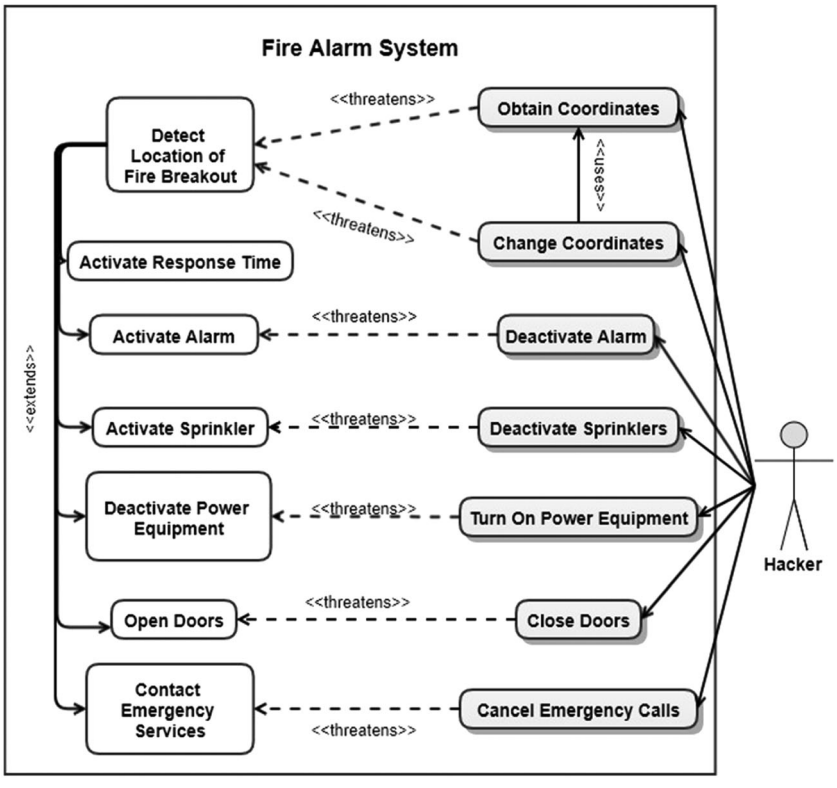

FIGURE 3 Miuse Case Fire alarm system

train cabin. Upon detecting fire, the coordinates of the location compromised are identified by the system using which the system automatically activates fire alarm, sprinklers, opens closed doors, and shuts down any active power equipment. The coordinates of the location compromised by fire and captured by the system if hacked, can use it to control and manipulate the countermeasures set by the system in order to contain the fire avoiding casualties, major injuries or heavy damages to the assets. The possible operations a hacker can perform using the accessed data consist of remotely controlling access to emergency exits, sprinklers, fire alarms, power equipment, and emergency message transmission to the relevant authorities. Thus, the security requirements extracted from the above misuse case in general consist of ensuring authentication and confidentiality

of the data transmitted between the sensors and the actuators, check for the freshness of the data received before further processing, check for nonrepudiation, and ensure a secure communicational channel for sending emergency messages to relevant authorities, to name a few.

5.1.2 | Step 3: Risk assessment

The fault tree drawn for this system is based on the failure of a fire alarm system, which in turn can be a result of failure to activate fire alarms, sprinklers, emergency service communication channel, or fire detection mechanism, as shown in the misuse case shown in Figure 1. The fault tree drawn below (see Figure 4) represents the risks analyzed during this phase of the risk management process. The evaluation of the risk[56,57] was conducted by identifying all the minimal cut-sets using the fault tree above marked with all the events and gates linking the events together.

The highlighted events in the fault tree above represent the events that are connected to the risks we have focused on in this thesis, ie, cyberattack, in particular the MitM attack and spoofing. Applying Boolean algebra, Equation 2 represents the set of minimal cut-sets obtained as follows:

$$G1 = (E8.E9) + E10 + E11 + E12 + E19 + E20 + E21 + E22 + E23 + E24 + E25 + E26 + E27 + E30 + E31 + E32 + E33 + E34 + E35 + E36 + E37 + E14 + E15 + E16 + E17 + ((E38 + E39).(E41.E42)) \quad (2)$$

Since we are focusing only on the security requirements and risks associated with them at an application layer, ie, authentication, nonrepudiation, data integrity, data freshness, and confidentiality, we selected spoofing, data tempering, and unauthorized access as the basic events to mitigate. Table 3 below summarizes the risks identified along with their risk values obtained from the existing literature. The repeated set of risks identified in the fault tree are grouped together as "a," "b," "c," and "d" to minimize the complexity of the fault tree.

The listed set of risks in Table 3 were identified using either misuse cases from Steps 1 and 2 or from the fault tree generated during the implementation of Step 3 of our framework. The probability of their occurrence was determined based on the security and privacy violation incidents reported over the past several years. To further calculate the risk values in the third column of Table 3, SILs were assigned to each of the identified risks based on their mode of operations. In case of a system being continuously operated throughout the life cycle of the software execution, the SILs assigned were based on continuous and higher demand rates. Whereas, in case of a system belonging to the category of operating only on

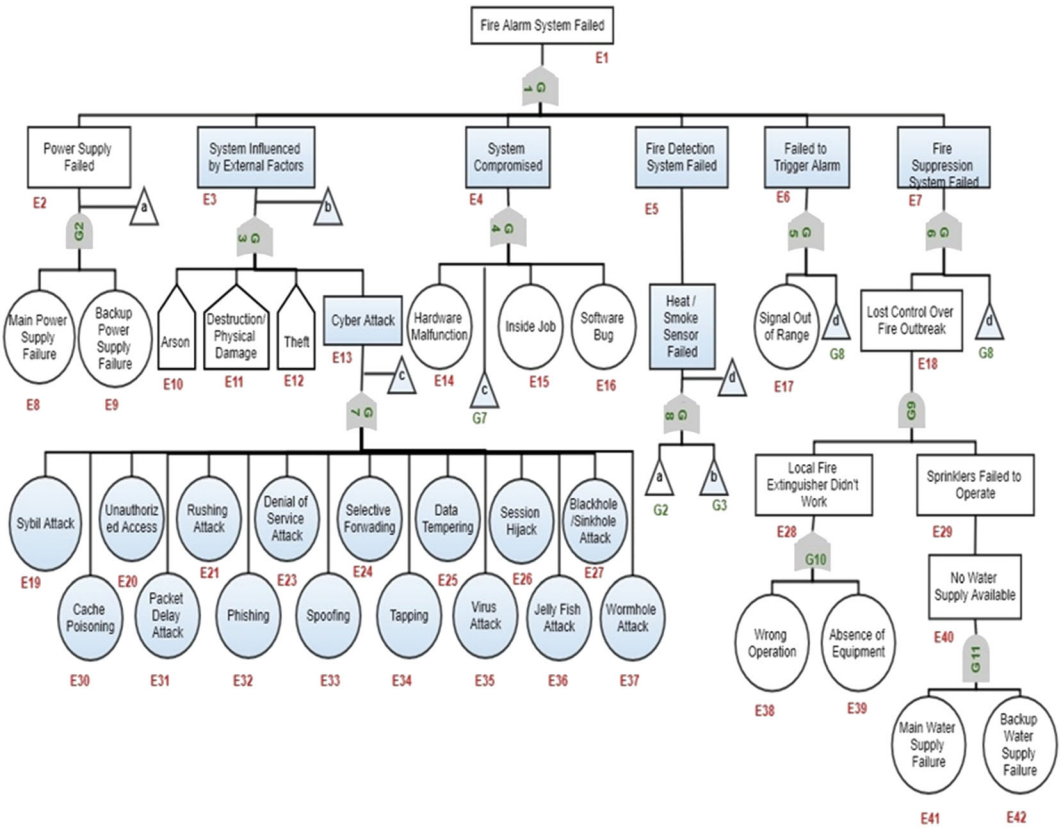

FIGURE 4 Fault tree for fire alarm system

TABLE 3 Risk values before mitigation fire alarm system

Risk Factor	SIL	Likelihood	Risk Value	Grouped
Power supply failed		1.1E-12	1.13E-12	a
Main power supply failure		1.13E-1	1.13E-1	
Backup power supply failure		1E-3	1E-3	
System influenced by external factors			7.2E-2	b
Arson	1	5.96E-2	5.96E-2	
Destruction/physical damage	2	2.79E-3	5.58E-3	
Theft	2	3.37E-3	6.74E-3	
Cyber attack			2.159E-5	c
Sybil attack	3	4.23E-2	1.27E-6	
Unauthorized access	3	4.23E-2	1.27E-6	
Rushing attack	3	4.23E-2	1.27E-6	
Packet delay attack	3	4.23E-2	1.27E-6	
Selective forwarding	3	4.23E-2	1.27E-6	
Data tempering	3	4.23E-2	1.27E-6	
Cache poisoning	3	4.23E-2	1.27E-6	
Phishing	3	4.23E-2	1.27E-6	
Spoofing	3	4.23E-2	1.27E-6	
Tapping	3	4.23E-2	1.27E-6	
Virus attack	3	4.23E-2	1.27E-6	
Session hijacking	3	4.23E-2	1.27E-6	
Denial-of-service attack	3	4.23E-2	1.27E-6	
Jelly fish attack	3	4.23E-2	1.27E-6	
Black hole/sinkhole attack	3	4.23E-2	1.27E-6	
Wormhole attack	3	4.23E-2	1.27E-6	
System compromised	3	4.23E-2	1.48E-2	
Hardware malfunction		9.12E-3	9.12E-3	
Inside job	2	2.83E-3	5.66E-3	
Software bugs	3	2.93E-3	8.8E-6	
c			2.159E-5	
Fire detection system failed			7.2E-2	
Heat/smoke sensor failed			7.2E-2	d
a			1.13E-12	
b			7.2E-2	
Failed to trigger fire alarm			7.2E-2	
Signal out-of-range	3	2.83E-8	7.14E-8	
d			7.2E-2	
Fire suppression system failed			7.2E-2	
d			7.2E-2	
Lost control over fire outbreak			2.73E-6	
Local fire extinguisher did not work			7.12E-3	
Wrong operation performed		5.12E-3	5.12E-3	
Absence of equipment	2	1E-3	2E-3	
Sprinkler failed to operate			3.84E-4	
No water supply available			3.84E-4	

(Continues)

TABLE 3 (Continued)

Risk Factor	SIL	Likelihood	Risk Value	Grouped
Main water supply failure		1.4E-1	1.4E-1	
Backup water supply failure		2.74E-3	2.74E-3	

Abbreviation: SIL, safety integrity level.

demand, the SIL assigned were based on low demand rates. The final risk values calculated were based on the product of the assigned SIL and the probability of occurrence of that particular risk.

Using the fault tree diagram of Fire Alarm System Failure in Figure 2 and inserting the corresponding risk values on the minimal cut-sets obtained during the fault tree analysis from Equation 1, resulted in Fire Alarm System Failure having an overall risk value of 0.17353312 before mitigating the identified risks.

5.1.3 | Step 4: Risk mitigation

The attacks simulated on the case studies violate some security requirements, namely authentication, nonrepudiation, confidentiality, data integrity, and data freshness.

5.1.4 | Before mitigation

MiTM and spoofing attack simulated on the software system revealed the information shared among the various functions of the software (see Figure 5), which are then further used for implementing countermeasures to reduce the impact of fire on both the train and the passengers.

MiTM attack simulated on the software system allows the hacker to tamper with data related to the titles containing fire, misleading the system regarding which titles contain fire and which do not. This can lead to risks of SIL 4 (highest severity), as it can result in causalities, heavy damage, and major injuries, as shown in Figure 6 as follows:

```
Sprinkler Activated at position 41, 54
Sprinkler Activated at position 42, 52
Sprinkler Activated at position 43, 54
Sprinkler Activated at position 44, 52
Alarm Activated at Position 45, 51
Sprinkler Activated at position 47, 54
```

FIGURE 5 Simulated passive attack on fire alarm system

```
Sprinkler Activated at position 53, 54
Sprinkler Activated at position 54, 52
Sprinkler Activated at position 55, 54
Fire Spreading to Coordinates58 55
Fire Spreading to Coordinates57 52
Fire Spreading to Coordinates58 51
Fire Spreading to Coordinates58 51
Fire Spreading to Coordinates57 52
Someone died (x_x)
Fire Spreading to Coordinates58 53
```

FIGURE 6 Active attack simulated on fire alarm system

```
Captured Data = KQx5lm8vpl08xAY26rZM7UbFjdb57nnp6loxbX7epo5Qn69fuC7xN1RuKxeicV4fvoJLiLCtG7suxEqpFzGN/jFZTArkOvT91S/
```

FIGURE 7 After applying hybrid cryptosystem

TABLE 4 Risk values after mitigation fire alarm system

Risk Factor	SIL	Likelihood	Risk Value	Grouped
Power supply failed		1.1E-12	1.13E-12	a
Main power supply failure		1.13E-1	1.13E-1	
Backup power supply failure		1E-3	1E-3	
System influenced by external factors			7.2E-2	b
Arson	1	5.96E-2	5.96E-2	
Destruction/physical damage	2	2.79E-3	5.58E-3	
Theft	2	3.37E-3	6.74E-3	
Cyber attack			2.159E-5	c
Sybil attack	3	4.23E-2	1.27E-6	
Unauthorized access	2	4.23E-2	8.46E−7	
Rushing attack	3	4.23E-2	1.27E-6	
Packet delay attack	3	4.23E-2	1.27E-6	
Selective forwarding	3	4.23E-2	1.27E-6	
Data tempering	2	4.23E-2	8.46E−7	
Cache poisoning	3	4.23E-2	1.27E-6	
Phishing	2	4.23E-2	8.46E−7	
Spoofing	2	4.23E-2	8.46E−7	
Tapping	3	4.23E-2	1.27E-6	
Virus attack	3	4.23E-2	1.27E-6	
Session hijacking	3	4.23E-2	1.27E-6	
Denial-of-service attack	3	4.23E-2	1.27E-6	
Jelly fish attack	3	4.23E-2	1.27E-6	
Black hole/sinkhole attack	3	4.23E-2	1.27E-6	
Wormhole attack	3	4.23E-2	1.27E-6	
System compromised	3	4.23E-2	1.48E-2	
Hardware malfunction		9.12E-3	9.12E-3	
Inside job	2	2.83E-3	5.66E-3	
Software bugs	3	2.93E-3	8.8E-6	
c			2.159E-5	
Fire detection system failed			7.2E-2	
Heat/smoke sensor failed			7.2E-2	d
a			1.13E-12	
b			7.2E-2	
Failed to trigger fire alarm			7.2E-2	
Signal out-of-range	3	2.83E-8	7.14E-8	
d			7.2E-2	
Fire suppression system failed			7.2E-2	
d			7.2E-2	
Lost control over fire outbreak			2.73E-6	
Local fire extinguisher did not work			7.12E-3	
Wrong operation performed		5.12E-3	5.12E-3	
Absence of equipment	2	1E-3	2E-3	
Sprinkler failed to operate			3.84E-4	
No water supply available			3.84E-4	

(Continues)

TABLE 4 (Continued)

Risk Factor	SIL	Likelihood	Risk Value	Grouped
Main water supply failure		1.4E-1	1.4E-1	
Backup water supply failure		2.74E-3	2.74E-3	

Abbreviation: SIL, safety integrity level.

According to the above displayed picture, the active attack simulated onto the software system not only violated the authentication, confidentiality, and integrity of data but has also affected the freshness of data crucial to dealing with such situations.

5.1.5 | After mitigation

After implementing our hybrid cryptosystem, the data sniffed out by the MiTM is in the form of a ciphertext (see Figure 7) rather than the actual data being transferred between the various functions of the software system.

The table below represents the risk values obtained after mitigating the identified risks in fire alarm system simulation:

Table 4 above summarizes the risk values evaluated using the same procedure adopted before merging the proposed mitigation measures into the system under observation. The above table represents the reduced severity levels against the security risks targeted and mitigated through our proposed framework. The updated SILs listed against each of targeted risks listed in the table above were then reused to evaluate the risk values for these risks. These updated risk values determined were then used to calculate the overall risk value of the fire alarm system failure risk in order to measure the effectiveness of our proposed framework. A risk value calculated after mitigation, ie, 0.17353142, shows a reduction in the severity of the risk of a fire alarm system failure for railway cabins from SIL 3 to SIL 2 reducing the overall risk of fire alarm system failure.

5.2 | Comparison of cryptosystems

For evaluation purposes, our hybrid cryptosystem was compared against some of the most recently proposed or suggested cryptosystems based on not only the overall execution time but also on the memory consumed by each of the studied cryptosystems. For comparing the cryptosystems[41–45,47] with our proposed hybrid cryptosystem as a mitigation measure, we integrated the selected cryptosystems into the fire alarm system simulation one at a time and recorded both the encryption and decryption time multiple times along with this the resources used, ie, memory consumption against each of the studied cryptosystems was measured. Once the data was collected, an average of these values was calculated and compared, based on which we drew our conclusions. The results show better performance of our cryptosystem in terms of both the encryption and decryption time of the compared cryptosystems. Figure 8 shows the worst performance mainly of the AES encryption shemes based on their memory consumption which should be taken into consideration as a memory effeciency problem especially during the development of safety-critical CPS systems having limited memory and larger reponsibilities.

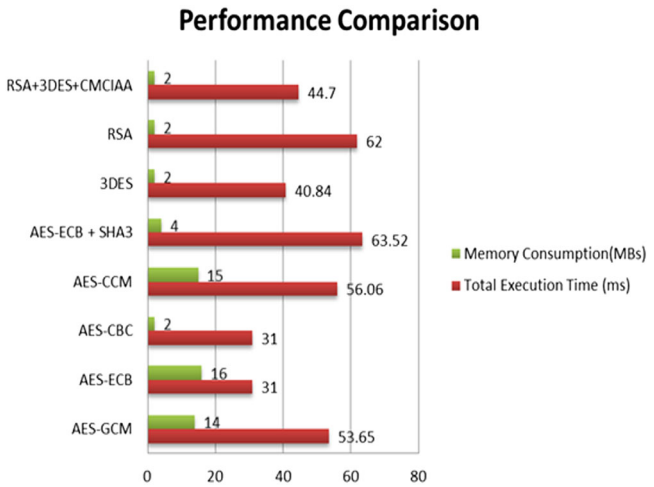

FIGURE 8 Comparison of encryption schemes

6 | DISCUSSION

During the execution of the framework on both case studies, Steps 1 and 2 (ie, extraction of security requirements and risk identification) yielded risks related to a system or a subsystem being compromised, which in turn could lead to the failure of the fire alarm system. During the risk identification phase, not all the risks could be identified using misuse cases. However, those risks that could not be identified by using the misuse cases did become visible through the fault tree constructed during the risk assessment phase of the mitigation framework. The fault tree generated during Step 3 (ie, risk assessment) was mainly mapped to the risks identified during the second step of the framework. The risk values calculated before and after risk mitigation were of a little difference since we focused only on a subset of the risks identified. In order to further reduce the overall risk of the system failure, there is a need to implement other mitigation measures for all the layers of CPS. The hybrid cryptosystem from Step 4 (ie, risk mitigation) integrated with the software system, reduced the severity of the cyberattack from SIL 3 to Severity of SIL 2, thus reducing the overall risk value of the external factors affecting the systems operation and other risks linked to cyberattacks. As compared with 3DES and RSA, the hybrid cryptosystem not only checked for data freshness but was also faster. Key management factor not being a part of the hybrid cryptosystem makes it memory-efficient. Among the various tested encryption schemes, AES-ECB combined with SHA-3 (Secure Hash Algorithm - 3)[47] showed the worst performance in terms of time consumed for data encryption and decryption along with overall memory consumption, followed by RSA and AES-CCM[44] encryption schemes. The hybrid cryptosystem suggested by our framework performed better than the tested encryption schemes, as it does not require key management.

7 | CONCLUSION

The requirement of constant connectivity in CPS invites hackers to gain unauthorized access and manipulate the operations to be performed by the system either for personal gain or just for amusement. A mitigation framework was developed focusing on mitigating risks related to authentication, confidentiality, data integrity, data freshness, and nonrepudiation at the application layer. Since the risk assessment process of our framework also involves SIL assignment taken from IEC 61508 standard, we think that it could be possible for the framework to be generalizable[58,59] to other application domains and organizations which undergo risk management processes compliant with the IEC 61508 standard, for example, the companies that are members of the 61508 Association (see www.61508.org), a cross-industry group of organizations with a common interest in functional safety, particularly in applying IEC 61508. As the association's website indicates, IEC 61508 is a standard applicable to all kinds of industry sectors. Plus, all member organizations of the association recognize IEC 61508 and related standards as the benchmark for achieving functional safety and managing risks in a proportionate way. Following Seddon and Scheepers[58] and Wieringa and Daneva,[59] if these organizations share similar values, have similar conformity assessment processes, organizational roles (eg, safety analysts and dedicated safety and security requirements specification staff), and CPS development approaches compliant to IEC61508, we could assume that our framework would be a good fit for them. Of course, more empirical research is needed to evaluate this in practice. Moreover, upon applying the proposed hybrid cryptosystem as a mitigation measure, the results not only showed a reduction in calculated risk values related to the system's security requirements but also performed relatively faster as compared with some of the most recent and most used cryptosystems. The hybrid cryptosystem since is independent of the hardware- and software-specific constraints, can thus be applied to mitigate security issues in applications of other domains. The common risk management standard IEC 61508[60] being the basis of the risk assessment phase of our framework and the cryptosystems being independent of the software's structure strengthen the generalizability of the applicability of our framework to the development of software in other from domains, other than the railway.

8 | FUTURE WORK

Other than the proposed mitigation measure, we will be further looking into other possible application layer mitigation measures as well as the measures applicable at both the network layer and physical layers for further improving the overall security of the CPS. We also plan to implement the proposed mitigation framework on case studies from other domains, namely industrial control systems, avionics, and medical applications, to assess the performance and the level of generalizability the framework provides. Only then, we could improve the generalizability[59] of our framework and possibly improve it based on the lessons learned through the case study research.

ORCID

Irum Inayat https://orcid.org/0000-0001-5576-6212
Maya Daneva https://orcid.org/0000-0001-7359-8013

REFERENCES

1. Lee EA., "Cyber Physical Systems: Design Challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363–369.

2. Carruthers K., "Internet of Things and Beyond: Cyber-Physical Systems," *IEEE Newsl*., no. May 2016, pp. 2016–2018.
3. Ciapessoni E, Cirio D, Kjølle G, Massucco S, Pitto A, Sforna M. Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. *IEEE Trans Smart Grid*. 2016;7(6):2890-2903.
4. Toms L., "GlobalSign Blog 5 Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale," *GlobalSign Blog*, 2016. [Online]. Available: https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/.
5. Ashibani Y, Mahmoud QH. Cyber physical systems security: analysis, challenges and solutions. *Comput Secur*. 2017;68:81-97.
6. Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electr Pow Syst Res*. 2017;149:156-168.
7. Sahinoglu M. and Wool K., *Risk Assessment and Management to Estimate and Improve Hospital Credibility Score of Patient Health Care Quality*. USA: Springer; 2014.
8. Guo H. and Wong JW., "Cyber-Physical Authentication for Metro Systems," in *IEEE 23rd Asia-Pacific Conference on Communications (APCC)*, 2017, pp. 1–6.
9. Li W., Song H., Wei Y., and Zeng F., Toward more secure and trustworthy transportation cyber-physical systems, no. 9789811038914. 2017.
10. Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of cyber-warfare. *Comput Secur*. 2012;31(4):418-436.
11. Santini R. and Panzieri S., "A graph-based evidence theory for assessing risk," *18th Int. Conf. Inf. Fusion*, pp. 1467–1474, 2015.
12. Jaiswal S. and Gupta D., "Security requirements for Internet of Things (IOT)," in *Proceedings of the 6th International Conference on Communication Systems and Networks*, 2014, pp. 419–427.
13. Ralston PAS, Graham JH, Hieb JL. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans*. 2007;46(4):583-594.
14. Peng Y., Lu T., Liu J., Gao Y., Guo X., and Xie F., "Cyber-physical system risk assessment," in 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.
15. Cárenas AA., Amin S., Sinopoli B., Giani A., Perrig A., and Sastry S., "Challenges for securing cyber physical systems," in Workshop on future directions in cyber-physical systems security, 2009.
16. Chan ACF, Zhou J. On smart grid cybersecurity standardization: issues of designing with NISTIR 7628. *IEEE Commun Mag*. 2013;51(1):58-65.
17. Gong L, Zhang L, Zhang W, Li X, Wang X, Pan W. *The application of data encryption technology in computer network communication security*. 1305 Walt Whitman RdMelville, New York: American Institute of Physics; 2017;1834.
18. Hartmann K. and Steup C., "The vulnerability of UAVs to cyber attacks—an approach to the risk assessment," in *Cyber Conflict (CyCon), 2013 5th International Conference on*, 2013, pp. 1–23.
19. Humayed A, Lin J, Li F, Luo B. Cyber-physical systems security—a survey. *IEEE Internet Things J*. 2017;4(6):1802-1831.
20. Ab Rahman NH, Glisson WB, Yang Y, Choo KKR. Forensic-by-design framework for cyber- physical cloud systems. *IEEE Cloud Comput*. 2016;3(1):50-59.
21. Saleem K., Tan Z., and Buchanan W., "Security for cyber-physical systems in healthcare," *Heal. 4.0 How Virtualization Big Data are Revolutionizing Healthc*., pp. 233–251, 2017.
22. I. S. T. Institute, "What is software risk and software risk management?," *International Software Test Institute*, 2018. [Online]. Available: https://www.test-institute.org/What_Is_Software_Risk_And_Software_Risk_Management.php.
23. Best J., "'Wake up baby': man HACKS into 10-month-old's baby monitor to watch sleeping infant," *Mirror Online*, Apr-2014.
24. Fletcher KK. and Liu X., "Security requirements analysis, specification, prioritization and policy development in cyber-physical systems," in 2011 *5th International Conference on Secure Software Integration and Reliability Improvement - Companion*, SSIRI-c 2011, 2011, pp. 106–113.
25. Polemi N. and Papastergiou S., "Current efforts in ports and supply chains risk assessment," in 2015 *10th International Conference for Internet Technology and Secured Transactions*, ICITST 2015, 2015, pp. 349–354.
26. Anne Tøndel I, Foros J, Skaufel Kilskar S, Hokstad P, Gilje Jaatun M. Interdependencies and reliability in the combined ICT and power system: an overview of current research. *Appl Comput Informatics*. 2018;14(1):17-27.
27. Mellado D, Fernández-Medina E, Piattini M. A common criteria based security requirements engineering process for the development of secure information systems. *Comput Stand Interfaces*. 2007;29(2):244-253.
28. Manshaei MH, Zhu Q, Alpcan T, Bacşar T, Hubaux J-P. Game theory meets network security and privacy. *ACM Computing Surveys*. 2013;45(3):1-39.
29. Wu G, Sun J, Chen J. A survey on the security of cyber-physical systems. *Control Theory Technol*. 2016;14(1):2-10.
30. Datta Ray P., Harnoor R., and Hentea M., "Smart power grid security: a unified risk management approach," in *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 2010, pp. 276–285.
31. Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. *Comput Networks*. 2013;57(5):1344-1371.
32. Nazir S, Patel S, Patel D. Assessing and augmenting SCADA cyber security: a survey of techniques. *Comput Secur*. 2017;70:436-454.
33. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. *J Netw Comput Appl*. 2014;42:120-134.
34. Xu Q, Ren P, Song H, Du Q. Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions. *IEEE Internet Things J*. 2017;4(6):1924-1933.
35. Axelrod CW., "Managing the risks of cyber-physical systems," in *2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2013, pp. 1–6.
36. Markantonakis K. and Mayes K., "SCADA System Cyber Security," *Secur. Smart Embed. Devices, Platforms Appl*., pp. 1–568, 2013.
37. Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. *Proc IEEE*. 2012;100(1):210-224.
38. Chatterjee K, Gupta D, De A. A framework for development of secure software. *CSI Trans ICT*. 2013;1(2):143-157.

39. Yao J., Venkitasubramaniam P., Kishore S., Snyder LV., and Blum RS., "Network topology risk assessment of stealthy cyber attacks on advanced metering infrastructure networks," in *Proceedings - 51st Annual Conference on Information Science and Systems (CISS)*, 2017.
40. Zhang L, Wang Q, Tian B. Security threats and measures for the cyber-physical systems. *J China Univ Posts Telecommun*. 2013;20(SUPPL. 1):25-29.
41. Munir A., Member S., Koushanfar F., and Member S., "Design and analysis of secure and dependable automotive CPS: a steer-by-wire case study," *IEEE Transactions on Dependable Secure Computing*, 2018.
42. Wang C. and Gill C., "Real-time middleware for cyber-physical event processing," in *IEEE/ACM 25th International Symposium on Quality of Service (IWQoS)*, 2017, pp. 1–6.
43. Rajbhandari L. and Snekkenes EA., "Mapping between classical risk management and game theoratical approaches," in *IFIP International Conference on Communications and Multimedia Security*, 2011, pp. 147–154.
44. Zhou L., Guo H., Li D., Zhou J., and Wong J., "A scheme for lightweight SCADA packet authentication," in 23rd Asia-Pacific Conference on Communications (APCC), 2017.
45. Karati A., Amin R., Islam SKH., Choo KR., and Member S., "Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment," *IEEE Trans Cloud Comput*, vol. 7161, no. c, pp. 1–14, 2018.
46. Flink GA, Edgar TW, Rice TR, MacDonald DG, Crawford CE. Overview of security and privacy in cyber-physical systems. *IEEE Des Test*. 2017;34(4):4.
47. Kim Y, Kolesnikov V, Thottan M. Resilient end-to-end message protection for cyber-physical system communications. *IEEE Trans Smart Grid*. 2016;3053(c):1-1.
48. Biro M, Mashkoor A, Sametinger J, Seker R. Software safety and security risk mitigation in cyber-physical systems. *IEEE Softw*. 2017;35(1):24-29.
49. Saripalli P. and Walters B., "QUIRC: a quantitative impact and risk assessment framework for cloud security," in *2010 IEEE 3rd International Conference on Cloud Computing*, 2010, pp. 280–288.
50. Anwar A. and Mahmood A., "Cyber Security of Smart Grid Infrastructure," *State Art Intrusion Prev. Detect.*, vol. January, no. January, pp. 139–154, 2014.
51. Nagaraju V., Fiondella L., and Wandji T., "A survey of fault and attack tree modeling and analysis for cyber risk management," in *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2017, pp. 1–6.
52. Boulanger J. *Control, Systems And Industrial Engineering Series CENELEC 50128 and IEC 62279 Standards*. British Library Cataloguing-in-Publication Data. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2015.
53. Rierson L. *Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance*, 1st ed. Boca Raton London New York: CRC Press Taylor and Francis Group; 2013.
54. Wadhwa N., Hussain SZ., and Rizvi SAM., "A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA)," in *World Congress on Engineering*, 2013, vol. II, pp. 6–9.
55. "Fire and security alarm monitoring simulation system," 2015. [Online]. Available: https://github.com/jnhankins/FSAMS.
56. Gerstle D., "*Power Supply Reliability*," Understanding Power Supply Reliability:: Radio-Electronics.com, 2012. [Online]. Available: http://www.radio-electronics.com/articles/power-management/understanding-power-supply-reliability-56.
57. Sumner M. Information security threats: a comparative analysis of impact, probability, and preparedness. *Inf Syst Manag*. 2009;26(1):2-12.
58. Seddon PB, Scheepers R. Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples. *Eur J Inf Syst*. 2012;21(1):6-21.
59. Wieringa R, Daneva M. Six strategies for generalizing software engineering theories. *Sci Comput Program*. 2015;101:136-152.
60. Oz MA, Kaymakci OT, Koyun A. A safety related perspective for the power supply systems in railway industry. *Oper Reliab*. 2017;19(1):114-120.

How to cite this article: Zahid M, Inayat I, Daneva M, Mehmood Z. A security risk mitigation framework for cyber physical systems. *J Softw Evol Proc*. 2019;e2219. https://doi.org/10.1002/smr.2219