Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Security and Safety in Cyber-Physical System (CPS): An Inclusive Threat Model

Mardiana Mohamad Noor[1,*], Ali Selamat[1], Nurulakmar Abu Husain[1], Ondrej Krejcar[2]

[1] Malaysia-Japan Institute of Technology, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia
[2] Hradec Kralove Univesity, Rokitanského 62/26, 500 03 Hradec Králové 3, Czech Republic

ARTICLE INFO

Article history:
Received 13 October 2023
Received in revised form 19 December 2023
Accepted 25 January 2024
Available online 28 February 2024

Keywords:

Internet of Things (IoT); Cyber Physical Systems (CPS) security; Issues in the Industrial Control Systems (ICS); Attacks to ICS; CPS threat model; Security and safety risk assessment

ABSTRACT

A Cyber-Physical System (CPS) is a combination of computational algorithms and physical processes that are integrated together. Cyber-Physical Systems (CPS) integrate computer and communication capabilities with the monitoring and management of physical parts, establishing a mutually beneficial interaction between the cyber and physical components. Industrial Control System (ICS) is one example of CPS which integrates the physical (OT) and cyber domains (IT), which makes them more vulnerable to attacks. Two essential characteristics of Cyber-Physical Systems (CPS) are safety and security. Threat models are methods for identifying, analysing, and proposing security control countermeasures for threats and their capabilities. However, the threat model methods which are used for the traditional IT systems are not sufficient as they do not include the physical interactions, consequences and impacts to the safety aspects in the Operational Technology (OT). On the other hand, a risk assessment analyses attack scenario, examines cybersecurity from the attacker's point of view, and gives cost-benefit data to support the expenditure on security measures. This study proposes an inclusive attacker's centric threat model and pro-active risk assessment model for CPS using Mamdani Fuzzy Inference System (FIS). The outcomes of the threat model prove that the lateral propagation of the threat is possible and threat may also propagate from the CPS assets to the IT segment. The risk assessment by using FIS shown that the safety and security risk for the CPS is significant and calculated as medium level. Hence, the risk factors that are considered in calculating the overall risk for a CPS need to be immediately addressed and mitigated.

1. Introduction

This paper focuses on security and safety of cyber physical systems (CPS) under the current Industrial 4.0 Revolution (IR 4.0). Cyber-physical systems (CPS) mainly refers to next generation systems that integrate communication, computation, and control in order to achieve stability, high performance, robustness, and efficiency as it relates to physical systems [1]. Therefore, CPS is a

[*] *Corresponding author.*
E-mail address: mardianamnoor@gmail.com

https://doi.org/10.37934/araset.40.2.176202

physically interconnected system that can be remotely controlled, monitored, and operated with real-time perception [2].

CPS are complex systems comprising heterogeneous components from communication, control and computation, that interact with the physical environment and human life. Examples of CPS include smart grids, power grids, IoT and/or sensor networks, autonomous automobile systems, medical or healthcare monitoring, process/industrial control systems, robotics systems and automatic pilot avionics. These components function seamlessly to offer specific functionalities that help enhance human lives, physical system operations and environments.

Industrial Control System (ICS) is one example of CPS which integrates the physical and cyber domains, which makes them more vulnerable to attacks. This is because cyberattacks could target Supervisory Control and Data Acquisition System (SCADA) and render the physical domain inoperable or because physical devices could be hacked or compromised, which would have an impact on the supervisory control system.

Not only the ICS is vulnerable due to the legacy hardware and known vulnerabilities of the control system hardware and devices, the heterogeneity of the CPS has also increased attack landscapes of the CPS. In addition, the use of the IoT devices such as the IED in the CPS makes the CPS more susceptible to the cyber-attacks [3].

Babu *et al.,* [4] discovered that the increased TCP/IP connectivity to the ICS as well as the intensified research effort by experts and hackers to identify and fix potential vulnerabilities in industrial control systems may cause in increase of ICS vulnerabilities. Mashkina *et al.,* [5] have furthermore listed several factors that may add to ICS vulnerabilities such as:

i. Absence or poor protection from illegal access to access components
ii. Undeclared possibilities of SCADA systems
iii. Use of wireless communications
iv. Absence or poor monitoring of the controlling influences
v. Absence of clear boundaries between different network segments (between corporate and industrial)
vi. Untimely or incorrect updating of the software
vii. Distribution of Windows as basic operating system for workstations and servers.

Two essential characteristics of Cyber-Physical Systems (CPS) are safety and security. Their common objective is to safeguard CPS from failures [6]. According to authors in [2], security is described as ensuring the integrity, authenticity, and confidentiality of information through the prevention of intentional threats, whereas safety is defined as avoiding operational dangers by preventing these unintended threats.

Availability is one such trait that could lead to conflicts between safety and cybersecurity goals. A cyberattack might be prevented by limiting availability, communication, or both. However, constant communication and availability protection are needed when a safety function necessitates continual control. If the process is frequently stopped by a safety feature, it will cause lost in availability. Hence, the safety measure needs to be thoroughly assessed from the perspective of cybersecurity if it is thought to be a potential cybersecurity countermeasure.

Invincible CPS is possible if safety and security can work well together. Issues related to safety and security are focusing more and more on CPS, creating new circumstances in which these two intricately related problems need now be taken into consideration simultaneously rather than sequentially or separately [7]. Unexpected events in a CPS are typically caused by the excessively complicated interactions and interdependencies among its various components [8].

1.1 Challenges in Aligning Cybersecurity and Safety in CPS

Cybersecurity primarily concerns itself with safeguarding systems against deliberate cyberattacks, whereas safety is concerned with preventing unintended failures in order to avoid potential risks. Although they have different areas of emphasis, their goals are identical: to prevent the collapse of CPS. Within a Cyber-Physical System (CPS), the integration of safety and security is crucial for establishing a robust foundation that ensures the CPS is impervious to harm. However, if there is a lack of alignment between safety and security measures, it can result in ineffective development and systems that are only partially protected [6].

The majority of CPS, especially ICS, rely on legacy systems that do not take cybersecurity into account during the design stage. As a result, it is not feasible to replace or update these legacy systems to incorporate the latest and standard cybersecurity capabilities. Moreover, the constant development of cyber threats requires the continuous adaptation of cybersecurity protocols. The rapid advancements in technology may outpace the ability to effectively integrate safety and cybersecurity measures. Organizations may face constraints in terms of time, financial resources, and expertise to adequately manage safety and cybersecurity threats. Balancing the need for safety and cybersecurity alongside other operational demands can be a significant challenge. Ensuring that operators have adequate training to successfully handle both cybersecurity and safety events is crucial, but challenging. Curiously, humans have the ability to inadvertently generate vulnerabilities or imperfections, which can result in detrimental consequences for both safety and cybersecurity.

The aforementioned difficulties necessitate a comprehensive solution and may entail additional expenses for ICS operators, as safety and cybersecurity are addressed in conjunction throughout the whole lifecycle of CPS—from its inception and creation to its implementation and upkeep. Therefore, it is essential to adopt a practical strategy since the merging of safety and cybersecurity is vital for maintaining the entire integrity of CPS.

The usability features in both the IT and OT segments of the ICS can play a crucial role in aligning cybersecurity and safety in the ICS. One way to achieve this is by including human factors into the enhancement of usability aspects, in addition to designing and implementing improved usability features for all devices, machines, and controllers in the ICS. Ensuring usability is of utmost importance in the alignment process, as any compromise in usability might potentially lead to the introduction of new cybersecurity and safety issues in ICS.

This research will demonstrate the alignment of cybersecurity, safety and operational usability using a Venn Diagram approach. A Venn diagram is a visual representation that use overlapping circles to depict the relationships and common attributes among multiple groups or categories. This research will also assess an additional model that aims to demonstrate the correlation between security and safety requirements and the usability issues involved in managing physical and cyber-physical assets in the operational technology (OT) domain. This research specifically focuses on the usability element within the OT segment, with a particular emphasis on the Industrial Control System (ICS) domain.

1.2 Challenges for Inclusive and Integrated CPS Threat Modelling

Due to heavy reliance on these technological interconnections, common threat actors in an Information Technology (IT) infrastructure such as adversaries with malicious intention for example nation backed terrorists, business rivals or script kiddies is anticipated.

However, in a CPS especially in an ICS, unexpected events that may also cause the failures to the ICS might possibly cause by the users or insiders inside the Operational Technology (OT) while performing different levels of operational activities on the CPS's physical or cyber-physical assets. According to Xirong Ning *et al.,* [9], a malicious insider might be more dangerous threat to the CPS than an external adversary due to knowledge and skills an insider has about the physical and cyber system configurations, communication networks and protocols, and their vulnerabilities. Furthermore, the physical and logical access control is not applicable for an insider who already has legitimate access, and an insider is more capable to carry out attack in stealthier manner without triggering any alarm to avoid detection and delay responses.

The only approach to fully investigate potential negative effects on the ICS information environment is through threat modelling [5]. The objective of threat modelling is to give security measures an organized analysis of the likely attack pathways so that they can analyse the assets the attacker is targeting and, in turn, determine the attacker's profile [10]. However, conventional threat modelling techniques designed for Information Technology (IT) systems may not be appropriate for Cyber-Physical Systems (CPS) because of significant disparities in their structure, functionality, and the types of threats they encounter. This may be due to integration of physical components, interconnectedness and interdependencies and human machine interaction.

Even though the unification of the security and safety aspects in a CPS threat model is still lacking [7], there is a positive development in integrating both security and safety elements in the current research. However, most of the proposed models are asset-based, which are concentrating on the interdependencies and interconnectivities of the critical assets. Due to insufficient consideration to the system's dynamic and under-estimation of human error, thus may cause inefficiencies in predicting and evaluating the threat and the associated risks. Current CPS threat models also are lacking of physical to cyber-attack propagation which is due to inappropriate human-machine interaction due to the lack of good practices in the usability aspects in the physical and cyber physical assets.

This research proposes a novel threat model that focuses on the attacker. The choice to utilize an attacker-centric threat model in the analysis of threats in a Cyber-Physical System (CPS) is driven by the need to understand and mitigate potential hazards resulting from deliberate and malicious actions. An attacker-centric threat model focuses on realistic scenarios in which persons with bad intent and varied motivations may target the system with the goal of compromising it. This approach facilitates a more precise and practical understanding of potential hazards, as it considers intentional hostile actions.

In this study the link and the relationship between the security, safety and ICS's assets usability is investigated. It is hypothesized that the manipulation of an ICS physical or cyber-physical asset's operational usability not only might cause danger and hazards but may also compromise the system's security aspects. This may weaken the security measures of the CPS, which may put the CPS more vulnerable to remote cyber-attacks. Considering the relationship between the two said aspects, further, we are developing a threat model for CPS which incorporates both security and safety aspects in a CPS, particularly ICS.

1.3 Problem Statement

The adoption of emerging technologies such as the Industrial Internet of Things (IIoT) has led to a heavy reliance on technological interconnection and interconnectivity in Cyber Physical Systems (CPS) and Industrial Control Systems (ICS). As a result, these systems have experienced a significant increase in potential vulnerabilities and risks to their operations. The ICS threat landscape is dynamic and will continue to change over time. Therefore, the current guidelines and areas of focus may not be effective in dealing with future attack patterns. Moreover, the presence of ICS-targeted malicious software provides attackers with additional leverage to inflict disruptions and damage to the ICS.

The intricate nature of the interactions and interdependencies among the many components of a CPS often leads to unforeseen outcomes [31]. Due to the substantial reliance on these technological connections, it is anticipated that many threat actors, including individuals or groups with ill intentions, corporate competitors, state-sponsored terrorists, and inexperienced hackers, will be present in an IT infrastructure. Conversely, unforeseen events, especially within an ICS, can also lead to failures in a CPS. These occurrences can be attributed to either users or insiders within the Operational Technology (OT) who are engaged in different operational activities involving the actual or cyber-physical assets of the CPS. According to Xirong Ning *et al.,* [9], insiders possess extensive knowledge and skill regarding the setups of physical and cyber systems, communication networks, protocols, and other weaknesses. This makes them potentially more harmful to the CPS than external attackers. Furthermore, as insiders already possess permitted access, they are exempt from both logical and physical access control measures. Conversely, those with privileged access can carry out attacks in a more discreet manner, without arousing suspicion or triggering any warning signs, so evading detection and causing delays in reaction. Some notable gaps in the current research in addressing the problem statements are:

i. Risks connected with the user-technology interaction in terms of usability is inadequately addressed. There is a significant lack in assessing the propagation of threats from physical or cyber physical assets to digital assets. Hence, the main objective of this work is to analyse and develop a relational model that investigates the correlation between security, safety, and operational usability (SSOU) in a Cyber-Physical System (CPS).

ii. Evaluation of risks based on human-centric for an inclusive threat model for CPS is lacking. The danger posed by individuals working in the IT or OT sector of the CPS can be demonstrated by integrating human factors into the threat modelling of the CPS. This study aims to fill the current void by presenting a thorough and inclusive human-centric threat model (ITM) for security and safety. The model takes into account the spread of threats among nodes and links, the involvement of threat sources and actors, and the interaction between assets and threat actors in a Cyber-Physical System (CPS).

2. Related Work

Cyber-physical systems, in contrast to software-based ones, have a wider range of hardware, software, and communication components that perform a physical task, necessitating the involvement of a wider range of stakeholder groups, such as operators dealing with physical processes or more heterogeneous development teams with different backgrounds in addition to IT or OT system operators. Consequently, threat modelling techniques, which have primarily been created for software, should be modified to account for the stakeholder structure of CPS systems [11]. Threat models are methods or frameworks for identifying, analysing, and proposing security control countermeasures for threats and their capabilities. Threat models may be attacker-centric, focused on the opinions, objectives, motives, and behaviours of the attackers [12].

In this study, a literature review was carried out and three research questions were developed while synthetizing the current literatures of CPS threat model which are:

RQ 1: What are the threat models (TM) methods in Cyber Physical System (CPS) available currently?

RQ 2: Is the relationship between security, usability and safety in the CPS demonstrated in the TM?

RQ 3: Do these TMs show some degree of unification of safety and security assessments in the CPS?

Vasilyev *et al.,* in [13] has proposed an automated modelling of a set of prospective incidents enables information extraction regarding infrastructure flaws, the most dangerous vulnerabilities, and potential flaws in system components. It also enables identification of the most effective attack scenarios and evaluation of the enterprise impact of those scenarios. A cognitive map-based model of the risks related to information security is proposed in by Mashkina and Garipov in [5]. In this model, the potential points of attack on significant assets are identified. The vulnerabilities connected to each attack penetrating path are found, exposing the ICS system. The model is then used for a quantitative study of information security risk assessment in an ICS.

A dependency-based, domain-neutral method for assessing cybersecurity risk is proposed by Akbarzadeh and Katsikas in their paper [8]. In order to establish effective security controls, the suggested method prioritises potential attack vectors against essential components of a CPS by considering the attacker's point of view. A Bayesian network based cyber-security risk assessment model to dynamically and quantitatively assess the security risk level in SCADA networks is proposed in [14]. The main contribution of the research is to visualize the inter-dependencies between the links and assets involved in particular attack graph propagation.

By using the graphical bow-tie diagram methodology to replace the threat model, Bernsmed *et al.,* in [15] aims to close the gap between safety and security during risk assessment. In this study, a use case in the maritime business was carried out. Bow tie diagram in showing the cause and effects be combined with other existing TM methods such as attack graphs is used to visualized the threat, consequence and the assets affected. Programmable Logic Controller (PLC) is used to illustrate the specific process that users follow when doing security-related operations [16]. While also taking into account the unique process-related needs crucial to ICS utilisation, the dangers against an existing security-usability threat model for IT systems are examined.

CPS testbed equipped with actual industrial controllers and communication protocols from real-world A industries is built as part of an integrated model-based methodology for CPS security risk assessment is developed by Tantawy *et al.,* in [17]. An exothermic Continuous Stirred Tank Reactor (CSTR) is monitored and managed by the testbed in real-time simulation. The authors have considered cyber-attacks in the test bed by using a TM adapted from attack tree model. Experimental results have shown that hazard development time and its impact to the CPS cyber-security design need to be considered. The outcomes from the study have also concluded that there is a very high dependency between cyber and physical systems; which supposed to be considered in designing integrated and secure CPS.

A summary of the related research is presented in Table 1. To this date, the research of unification in the CPS’ the security and safety aspects is lacking, as presented in Table 1. And so far, there is no inclusive (considering all the RQs in this research) threat model available to assess CPS security and safety.

Table 1
Summary of the related work in the literature review

No	Publisher, year	Title	RQ 1	RQ 2	RQ 3
[14]	IEEE, 2017 Web of Science	Application of Bayesian Network to Data-Driven Cyber-Security Risk Assessment in SCADA Networks	Bayesian Network	NO	YES
[15]	Springer Link, 2018 Web of Science	Visualizing Cyber Security Risks with Bow-Tie Diagrams	Bow-Tie Diagram	NO	YES
[16]	ACM, 2021 Google Scholar	Vision: Security-Usability Threat Modelling for Industrial Control Systems	STRIDE	NO	YES
[17]	ELSEVIER, 2020 Web of Science	Model-Based Risk Assessment for Cyber Physical Systems Security	Attack Tree & Formal Model	NO	YES
[13]	IEEE, 2021 IEEE Explore	Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modelling with CVSS Score	Attack Graph	NO	YES
[5]	IEEE, 2018 IEEE Explorer	Threats Modelling and Quantitative Risk Analysis in Industrial Control Systems	Cognitive Graph	YES	YES
[8]	Springer Link, 2022 Web of Science	Dependency-based security risk assessment for cyber-physical systems	Attack Path Analysis	NO	YES

While the current studies in securing the CPS have already considering the interdependency aspects of the assets and link by realizing the tight coupling between the cyber and the physical system, a thorough investigation of the relationship between the security, safety and operational usability aspects is yet available. Even though some of the current TMs applied in CPS are adopting the models that are used in software-based system such as STRIDE and attack tree, an inclusive model which supposed to demonstrate the interactions between all the important entities in an CPS is still lacking.

The different approaches employed elucidated the adaptability to accommodate interdependencies and intricacies in CPS. In conclusion, irrespective of the approach employed to represent the threat, the authors have successfully accomplished the primary goal of integrating and consolidating safety and security elements into a single threat model, taking into account the assets and interconnections of Cyber-Physical Systems (CPS).

Nevertheless, the techniques proposed by the authors solely depict the propagation of cyberattacks to physical systems. The potential for threats originating from the operational technology (OT) segment of cyber-physical systems (CPS) is often overlooked in existing literature. Therefore, this study recognises the existing deficiency and aims to address it by introducing a threat model that demonstrates potential 'bottom-up' threat dissemination from the Operational Technology (OT) to the Information Technology (IT) segment. Hence, this study is proposing an inclusive model which includes the interaction between the insiders and the CPS assets and demonstrating the link between the safety aspect and security which may be beneficial to CPS operators while considering the digitalization of the physical assets in their respective CPS, particularly ICS.

3. Development of CPS Knowledge Base

The objective of this research is to develop a security and safety model for CPS particularly the ICS. This model is then used as underlying idea of CPS proposed threat model. At the initial stage of the study, the problem statement was developed by using systematic literature review (SLR) using keywords such as Internet of Things (IoT), Cyber Physical Systems (CPS) security, issues in the Industrial Control Systems (ICS), attacks to ICS, CPS threat model and security and safety risk assessment. Current cyber-security framework NIST, Mitre ATT&CK, CISA and SANS were also referred as part of the literature process. The problem statement and current state for the issues mentioned above were confirmed with the stake holders whom are involved in the research area. In this study, Expert Review Method was adopted in the process. Table 2 presents the respondents in the interview sessions.

Table 2
List of respondents and interviews' key takeaways

No	Industry	Key Takeaways
1	Process Engineer Chemical Plant	Negligence in performing the task is very minimal due to high awareness to the safety aspects
2	Mechanical Engineer International Port Operation	The movement of the containers going in an out of the port is closely using tight surveillance system which consist of advanced IED and security cameras. Most of these devices are installed and maintained by different vendors.
3	Automation Industry	Some operators opt not to secure the control system assets using password due to inoperable maintenance
4	PLC Operation Expert	Many ICS operators have migrated to Industrial PC (IPC) to replace the conventional PLC in the OT segment
5	Failure and Test Engineer Semiconductor Industry	The security aspect in the OT segment is quite tight and proper access control is implemented, however it is totally controlled by different party.
6	Process Engineer, Semiconductor Industry	Standard of operations and standard of conditions must be strictly followed to ensure the quality of the processes' outputs.
7	Project Engineer, Local Oil and Gas Company	Safety is the utmost importance in an OT site for oil and gas and all the workers are consistently reminded about their safety
8	Turnaround Project Engineer, Oil & Gas exploration and production / processing	There is some degree of awareness of the controllers' vulnerability and was informed that the company's cyber-security system is resilient.
9	Facilities Shutdown Manager Oil & Gas exploration and production / processing	Dealing with quite number of projects/ events in Upstream Gas; required high commitment, focus, multitask and very strong technical skills and experience.

Majority of the respondents are the experts in handling the control systems or have some degree of involvement in different fields of manufacturing industries such as automations and semiconductors and wafers, local and international oil and gas industries, established international port industry and established chemical plant in Malaysia. The questions for the interviewees were formulated by Mockel [18] and Li *et al.,* [16] and also from the input of the current research and studies and also the existing frameworks. Some significant incidents in the CPS were also considered as the input in developing the interview questions. The analysis of the interviews' data was designed based on "thematic" method which was developed by Braun *et al.,* [19]. In qualitative research, thematic analysis is common because it places a strong emphasis on spotting, deciphering, and understanding qualitative data patterns. The findings from this process are used in classifying the threat actors and threat events in a CPS. For this purpose, Threat Actor Matrix and Threat Events Matrix are developed before proceeding to the next phase which is developing the Threat Model. The flow of this process is described in Figure 1.

Some common inputs and themes from different industries:

i. All engineers are aware of the safety aspects in the OT. These safety aspects are made available, published and emphasized many the times in the OT.
ii. The engineers, technicians and operators do not receive any security alerts from the IT team.
iii. IT and OT operations are totally in the different portfolios
iv. Depending on the industry, there are understandable policies of using own devices, accessing the files and uploading and downloading documents in the company networks.
v. Remote access capabilities are essential in all industries
vi. Ineffective passwords management is deterring efficient control systems updates and maintenance

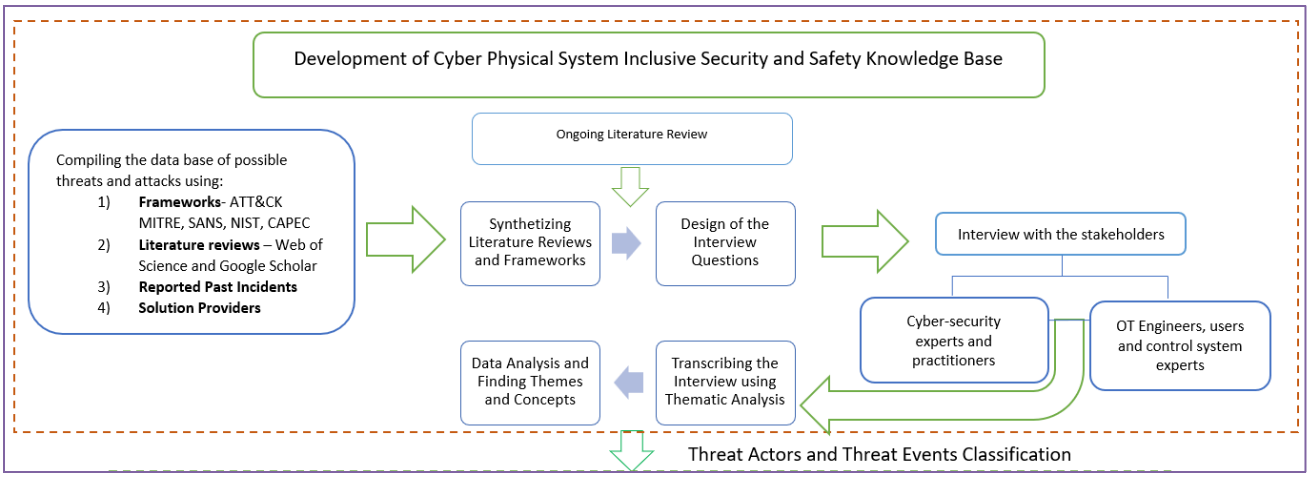

Development of Cyber Physical System Inclusive Security and Safety Knowledge Base
Compiling the data base of possible threats and attacks using:
1) Frameworks- ATT&CK MITRE, SANS, NIST, CAPEC
2) Literature reviews – Web of Science and Google Scholar
3) Reported Past Incidents
4) Solution Providers
Ongoing Literature Review
Synthetizing Literature Reviews and Frameworks
Design of the Interview Questions
Interview with the stakeholders
Cyber-security experts and practitioners
OT Engineers, users and control system experts
Transcribing the Interview using Thematic Analysis
Data Analysis and Finding Themes and Concepts
Threat Actors and Threat Events Classification

Fig. 1. Flow of the study in developing the knowledge base for CPS threats

3.1 Alignment of Security and Safety via Usability for CPS

The impacts from the past cyber-attacks on CPS especially ICS has been proven catastrophic on the physical systems. This is an evidence of the direct relationship between security and safety in an ICS [20]. The failure to properly secure the IT segments from intentional cyber-attacks has caused hazards in OT segment which will lead to loss to the availability of the process, may contaminate the environment or cause loss of human lives. A lot of security requirements have been deployed to address security issues in the cyber domain, however the applicability of the same requirements in the OT segment has demonstrates some degrees of intricacy due to the complicated cyber-physical interactions [21].

Since the processes in an ICS are heavily dependent on the automation using the controllers, the usability of the assets in the IT and OT segments should not exclude the security and safety aspects. The usability is usually important while considering the security aspects in developing a software or an IT system [16]. Meanwhile in a CPS, the usability of the OT assets is equally important as in IT segment.

However, in reality, certain procedures or standard operating flows may be bypassed or neglected by the operators such as engineers or technicians in order to expedite certain processes.

This, may cause direct or indirect effect to the system’s safety and security aspects. For example, by using default usernames and passwords to control certain processes and by giving general access privileges to the operators to operate control system such as PLC will open up the opportunity to the unauthorize personnel to change the ladder diagram or the program, thus will cause disruption to the physical processes. Other possible scenario that may cause indirect effect to safety is when the operational usability compromises the system’s security and creating an opportunity for the cyber-attacks to be carried out remotely by the adversary in order to achieve the ultimate objective, which is to cause failures to the ICS.

Gerson [22] has defined usability as “ *the ease of use and learnability of a human-made object. The object of use can be a software application, website, book, tool, machine, process, or anything a human interacts with”*. In this study, the usability aspect (in the OT segment) is studied and the safety and security risk imposed by this aspect is investigated. This will lead to the assessment of the behaviour of the users in the OT segment, which is considered as another threat actor in the CPS threat model. The relationship between these three aspects is visualized in Figure 2. The figure shows the relationship between security, safety and usability in IT and OT context. The diagram also showing the parameters which are involved in each realm.

This paper's notion of usability is derived from an examination of usability in secure software applications [18]. Since usability and security in IT systems have been shown to be closely related, the same may hold true for OT systems with a small variation in the architecture. The proposed model in Figure 2, has suggested the most important parameters in each aspect. In an IT segment, the utmost importance is to prevent cyber-attacks by strictly following the security protocols so that the confidentiality, integrity and availability of the data is guaranteed. At the same time, the users in the segment should also agree to the usability aspects of the IT assets to avoid security conflicts in the respective domain which can be achieved by series of effective trainings and clear instructions.

On the other hand, for the OT segment, safety is the key parameter to consider. Any neglect in the Standard of Procedures (SoP) and Standard of Condition (SoC) may cause loss in human lives and damage in the environment which may lead to the uncontainable impact. The said neglection may be due to the usability conflicts in the OT physical assets. In this study, manipulation of usability in the OT and its consequences to the system’s security aspects is highlighted.

Due to the interdependencies between the IT and OT segments, CPS must consider both aspects towards reliable data and physical processes. From Figure 2 it is demonstrated that the overlapping or the linkage between security and safety is possible by means of the usability aspects. By considering these three aspects in the CPS design stage, dependable and invincible CPS might be able to materialize.

The alignment of CPS safety and security requirement has been highlighted by the authors in [20]. The research has concluded that safety and security requirement may be in-line, conflicting or has no effect on each other. Thus, an integrated requirement analysis method is proposed in the research to resolve safety and security conflicts.

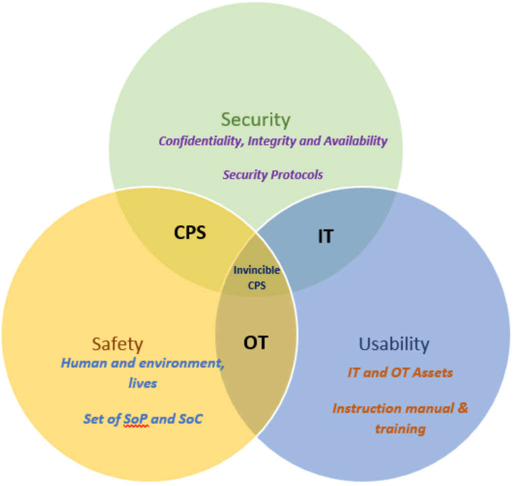

Security
Confidentiality, Integrity and Availability
Security Protocols
CPS
IT
Invincible CPS
Safety
Human and environment, lives
Set of SoP and SoC
OT
Usability
IT and OT Assets
Instruction manual & training

Fig. 2. The proposed model showing relationship in between security, safety and usability in CPS

4. Research Methodology

The work in this study has introduced security, safety and usability and proposed an inclusive threat model models in order to achieve invincible CPS, particularly ICS. The objectives of the models are to show how the security and safety in an ICS is intertwined and affecting each other by manipulation of the usability aspects in the OT segments. Based on the knowledge that have been developed in the previous section, Security, Safety and Operational Usability (SSOU) model and Inclusive Threat Model (ITM) for CPS are proposed.

The linking of the security safety and usability aspects in handling physical and cyber-physical assets in the OT and the alignment of CPS safety and security requirements are demonstrated by using Venn Diagram and a relationship model respectively. The diagram depicted in Figure 2 consists of three fundamental elements that form the basis of an invincible Cyber-Physical System (CPS).

The relationship model shown by the Venn Diagram in Figure 2 clarifies the overlapping concept between usability and security in the IT field, whereas the overlapping concept between usability and safety is noticed in the OT field. While the IT and OT segments may have slightly distinct usability objectives, it is crucial to prioritise robust usability in both. Hence, usability is a mutual objective for both categories. Usability, security, and safety are interconnected aspects of an Industrial Control System (ICS). The incorporation and execution of usability can exert a significant impact on the security and safety of an ICS. An all-encompassing strategy is required to attain a harmonious equilibrium among usability, security, and safety while creating and operating an ICS. An optimal solution takes into account the particular requirements of the industrial environment, ensuring that enhancements in usability result in a favourable effect on the overall security and safety of the system.

Aligning cybersecurity and safety concerns is crucial in guaranteeing the highest security, safety, and usability of the CPS domain. This entails safeguarding the system against any attacks that may jeopardise its security, mitigating any adverse consequences arising from security breaches, and guaranteeing efficient and secure interaction between humans and machines. Additionally, it is crucial to minimise the impact of usability manipulation on the security and safety of the CPS.

Organisations can strengthen the cohesiveness and resilience of Cyber-Physical Systems by aligning security and safety requirements through the adoption of common goals and shared principles. Considering the interaction between security and safety issues in an integrated strategy improves the overall resilience of the CPS. To achieve this integration and alignment, it is necessary to enhance the usability elements of the cyber physical and physical assets and devices in the OT segment. Usability considerations can potentially fulfil five typical security and safety needs in a CPS. The requirements include access control, authorization and authentication, physical security measures, emergency and incident response planning, monitoring, and interdisciplinary integration. Table 3 and Figure 3 provide a comprehensive summary of the standard requirements and recommended usability good practice.

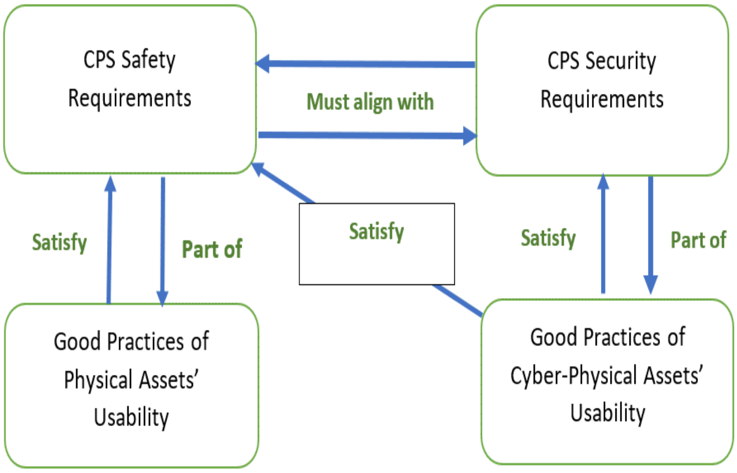

CPS Safety Requirements
Must align with
CPS Security Requirements
Satisfy
Part of
Satisfy
Satisfy
Part of
Good Practices of Physical Assets' Usability
Good Practices of Cyber-Physical Assets' Usability

Fig. 3 The relationship between usability safety and security requirements and its alignment in CPS

Table 3
Non-Conflicting Cybersecurity and Safety Requirements for CPS

CPS safety and security requirements	Good Practices of Physical Assets Usability	Good Practices of Cyber Physical Assets Usability
Access Control, Authentication and Authorization	Interoperability and Integration	Security Awareness in the design
Physical Security Measures	Clear and Intuitive Interfaces	Intuitive User Interfaces
Emergency and Incident Response Planning	Minimal Cognitive Load	Effective Data Visualization
Monitoring	N/A	Remote Monitoring and Control
Interdisciplinary Collaboration and Integration	Interoperability and Integration	Interoperability and Integration

The threat model is developed in 5 different phases (Figure 4); which are identifying the CPS domain, listing important and critical assets, evaluating potential external and internal attackers, finding possible threats events which might be triggered by the attackers and assessing the propagation path as presented in Figure 2.

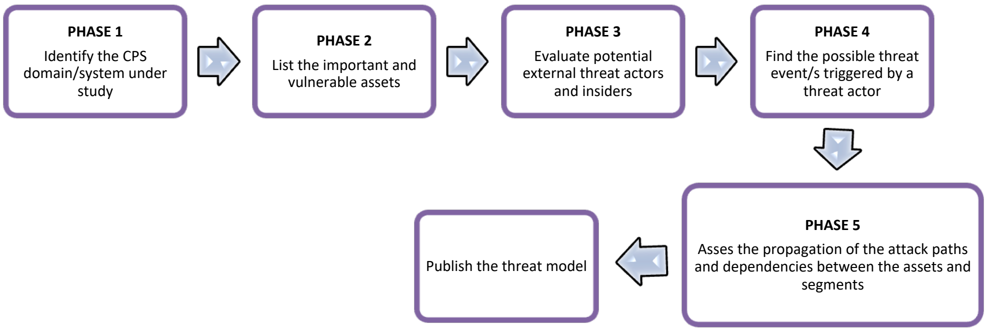

PHASE 1
Identify the CPS domain/system under study
PHASE 2
List the important and vulnerable assets
PHASE 3
Evaluate potential external threat actors and insiders
PHASE 4
Find the possible threat event/s triggered by a threat actor
PHASE 5
Asses the propagation of the attack paths and dependencies between the assets and segments
Publish the threat model

Fig. 4. Threat Modelling Process

4.1 PHASE 1 - Identification of the CPS Domain: Industrial Control System (ICS)

When it was first developed, Industrial Control Systems (ICS) resembled conventional information technology (IT) systems only slightly. Essentially, ICS were separated systems that used specialised hardware and software to execute proprietary control protocols. Numerous ICS components were installed in physically secure locations, and they weren't connected to any IT networks or systems. However, nowadays, as more remote functionalities are introduced for seamless accessibilities and control to the OT, the ICS are much more connected to the Internet. Hence, the ICS has been more exposed to cyber-attacks. Figure 5 represents a typical ICS topology proposed by Trend Micro.

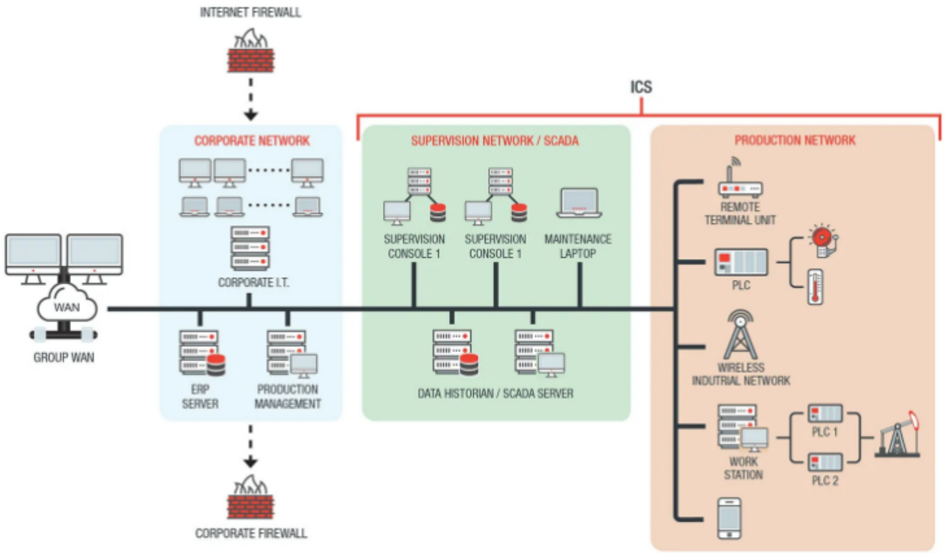


Fig. 5. A typical ICS topology as suggested by Trend Micro [23]

4.2 PHASE 2: Evaluating Typical ICS Assets

Critical infrastructure is built on top of highly specialised ICS. The physical processes that these operational technology systems regulate are directly connected to them. An ICS typically consists of:

i. A sensor: A device that generates an analogue signal in response to a physical attribute being measured.
ii. Actuator: Changes industrial control procedures based on input from controllers.
iii. Controller: Directs actuator inputs using algorithms that are informed by sensor outputs.

iv. Human Machine Interface (HMI): a hardware-and-software solution that enables operators to communicate with system controllers.

v. Programmable Logic Control (PLC): The main controller to give regulatory control and control certain applications and typically, ladder logic or ladder diagrams are used to program the PLCs.

vi. Supervisory Control and Data Acquisition (SCADA): A centralized data gathering and supervisory control to regulate the scattered assets in an ICS.

vii. Industrial Control Networks (ICN): Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP) for electronic mail, Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) for the Internet, and File Transfer Protocol (FTP) for file transfers are all commonly used by enterprise operating systems. Traffic on the control network is typically restricted to ICS command and control protocols like Modbus.

4.3 PHASE 3: Potential Threat Actors (TA)

In the proposed threat model, the potential attackers (in this paper are called as the threat actor ,TA) are divided into two categories, which are malicious external adversaries which will likely to launch cyber-attacks against the ICS and insiders in the OT segments. The profiling of the TA is very crucial to show the intention and capability of the adversaries as well as to demonstrate interaction between the stakeholders and the assets in the CPS, which might increase the security and safety risks in the ICS. The TA score is also an important element that will be considered in the risk quantification. The classification of the potential attackers (TA) is conducted through a thorough process during the systematic literature review (SLR), past incidents, existing framework such as MITRE ATT&CK [24] and National Institute of Standards and Technology, NIST [25] and series of the interviews with the stakeholders in the CPS such as cyber-security expert and analyst, and engineers in the CPS environment from various industries. According to Al Majali *et al.,* [26] the likelihood of the TA for adversaries can be profiled and quantified according to their intend, capability and targeting. Table 4 represents the metric of the potential attackers in an ICS based on the NIST framework. However, for the TA which are categorized as the ‘insiders’ no standard metric for profiling is yet available especially for CPS, hence in this research we are modifying the existing profiling metrics for the insiders based on the NIST framework as presented in Table 4. The ability of all TA to access the OT level based on the Purdue model [27] is also considered in the metrics. The metrics will be used in quantifying the Attacker’s Score as part of risk calculation.

Table 4
The Modified Threat Actor Characteristics Metric adapted from NIST [25]

Threat Actor (TA)	Intent	Capability	Targeting	Purdue OT Level Access
	High | Medium | Low	High | Medium | Low	High | Medium |Low	High | Medium | Low
Adversary with malicious intent attacking directly to the OT segment (TA 1)	The intention of the adversary is very clear which is to cause failure to the ICS HIGH	The adversary a very high-level expertise and may have some substantial experience. The adversary is also well resource and is capable to launch several successful, persistent and coordinated attack HIGH	The adversaries make use of the available information which is available publicly to persistently targeting high value information or assets HIGH	The adversaries may not have physical access to the OT level access but can initially virtually access OT L_3 L3 (MEDIUM)
Adversary with malicious intent attacking through the enterprise (TA 2)	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. HIGH	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks HIGH	The adversary gains some useful information through reconnaissance and scanning (using Shodan) and persistently target the critical OT's hardware and network vulnerabilities. The adversaries are also interested in the types (such as brands) of the assets in the OT and targeting legacy devices HIGH	The adversaries do not have physical access to the OT level access but can access the OT network at L_3 through lateral attack propagation from the enterprise network L3 (MEDIUM)
Insider with malicious intention (TA 3)	The Insider is a dissatisfied or disgruntled employee who has a very strong motive to cause ICS failure HIGH	Knowledge and skills about the physical and cyber system configurations, communication networks and protocols, and their vulnerabilities. HIGH	The insider is able to carry out attack in stealthier manner without triggering any alarm to avoid detection and delay responses. The insider is able to study the system thoroughly and decide the most critical and impactful asset to attack. HIGH	The insiders do have physical access to the OT level (0 to 3) HIGH

Negligent Insiders (TA 4)	The Insider might be an engineer/technician/ operator who have been working for many years and has been manipulating the usability of the physical or cyber-physical assets MEDIUM	TA might have high knowledge and skill MEDIUM	Due to lack of awareness or costing/budgeting, negligent insiders intentionally bypass certain SoP and SoC to expedite certain procedures or processes HIGH	The insiders do have physical access to the OT level (0 to 3) HIGH
Accidental Insiders (TA 5)	The Insider might be engineer/technician/ operator who unintentionally trigger a certain security or safety events LOW	TA might have high knowledge and skill MEDIUM	Due to certain unexpected scenario or lack concentration on a certain procedure, unwanted events may occur LOW	The insiders do have physical access to the OT level (0 to 3) HIGH

4.4 PHASE 4: Evaluating the Threat Events (TE)

Based on the study carried out by the authors in [8], the threat events will be evaluated based on Vulnerability (V) and current Control (C) available such as regulation, mitigation and solution to the threats. Vulnerabilities of the system (V) is categorized intro three different levels which are High (H), Low (L), and Medium (M). Control (C) such as mitigation, regulations or solution to the particular possible TE is also considered as one factor for the TE to materialize which can be defined as Proven to be Efficient (E), Not Efficient /Restricted(R) or Not Applicable (NA). The metric of the TE that is proposed in this work is presented in the Table 5.

Table 5
Possible Threat Events (TE) Initiated by the identified Threat Actors (TA)

TE	Factors	Vulnerability			Control		
Level & Score		High	Medium	Low	E	R	N/A
TA 1	Manipulating Remote Access to manipulate PLC settings or access confidential files which are shared in a server	High			E		
	Targeting the Windows Systems' unpatched vulnerabilities to gain access	High			R		
	Launching spear phishing attacks targeting public facing PC or staff PC in the enterprise network	High			E		
TA 2	Attacking the OT networks by using control system's hardware (e.g. SCADA) known vulnerabilities	High			R		
	Targeting the hardcoded credentials and manufacturer settings of the legacy devices	High			NA		
	Launching MiTM to the RTU (Attack to the OT network)	High			E		
	Launching attacks through the IoT devices in the OT segment	High			R		
TA 3	Disabling the safety sensor/alarm to expedite certain physical processes	Medium			E		
	Infecting the controllers/HMI with Trojans	High			R		
	Purposely changing PLC's ladder diagram to disrupt the physical process or to interrupt the safety	Medium			E		
	Putting illegitimate IoT devices physically in the CPS for example camera or CCTV for spying purpose	High			E		

	Giving information about the PLC program to an outsider with an ill-intention	Medium	R
TA 4	Do not apply a regulated access control for the control system equipment such as PLC or SCADA or HMI.	High	E
	Disabling the safety sensor/alarm to expedite certain physical processes	High	E
	Using personal USB stick (may contain virus) to retrieve work related data.	High	E
	Do not follow password requirement especially for controllers' access	Medium	E
	Not changing the default configuration settings of the devices or application	High	R
TA 5	Unintentionally using a laptop with Trojan and connect it to the controllers' interface or other types of HMI	High	E
	Using personal USB stick (may contain virus) to retrieve work related data. Since some control system has been using Industrial PC (IPC), which contains malicious code to delete or modify data	High	E
	Accidentally clicking on Phishing e mail while using the OT networks	High	E
	Accidentally putting in wrong input to the HMI or the controller	Medium	NA

Threat actor 1 (TA 1): *Adversary with malicious intent attacking directly to the OT segment,* Threat actor 2 (TA 2): *Adversary with malicious intent attacking through the enterprise,* Threat actor 3 (TA 3): *Insiders with malicious intention,* Threat actor 4 (TA 4): *Negligent Insiders,* Threat actor 5 (TA 5): *Accidental Insiders*

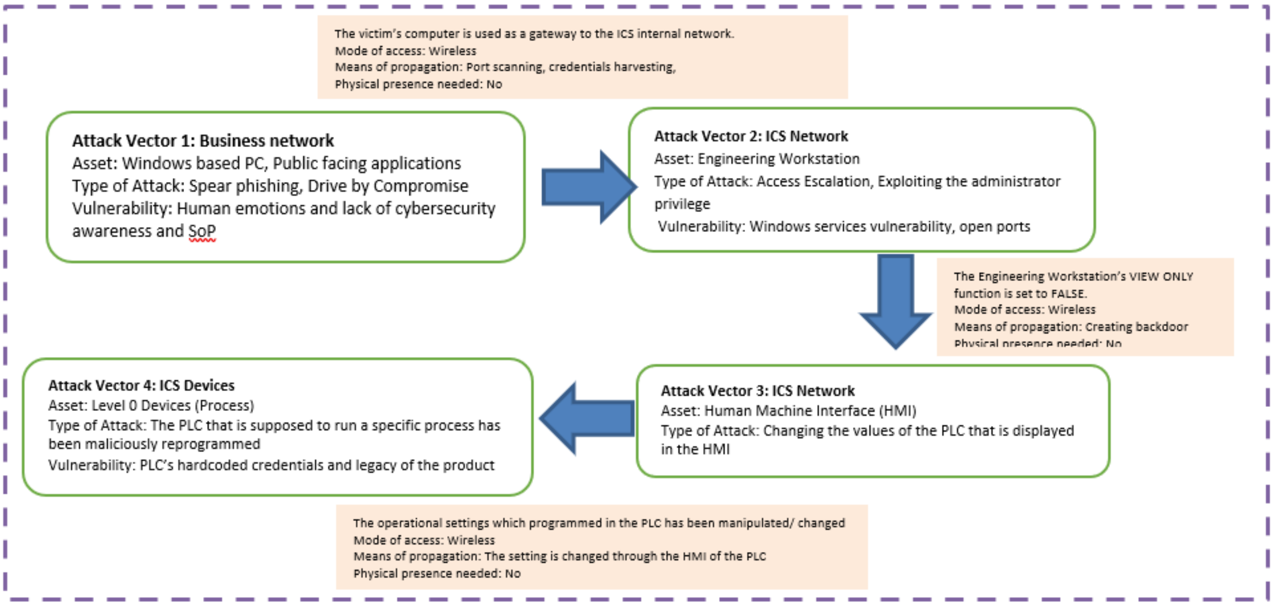
E: Exist, R: Restricted, NA: Not Available

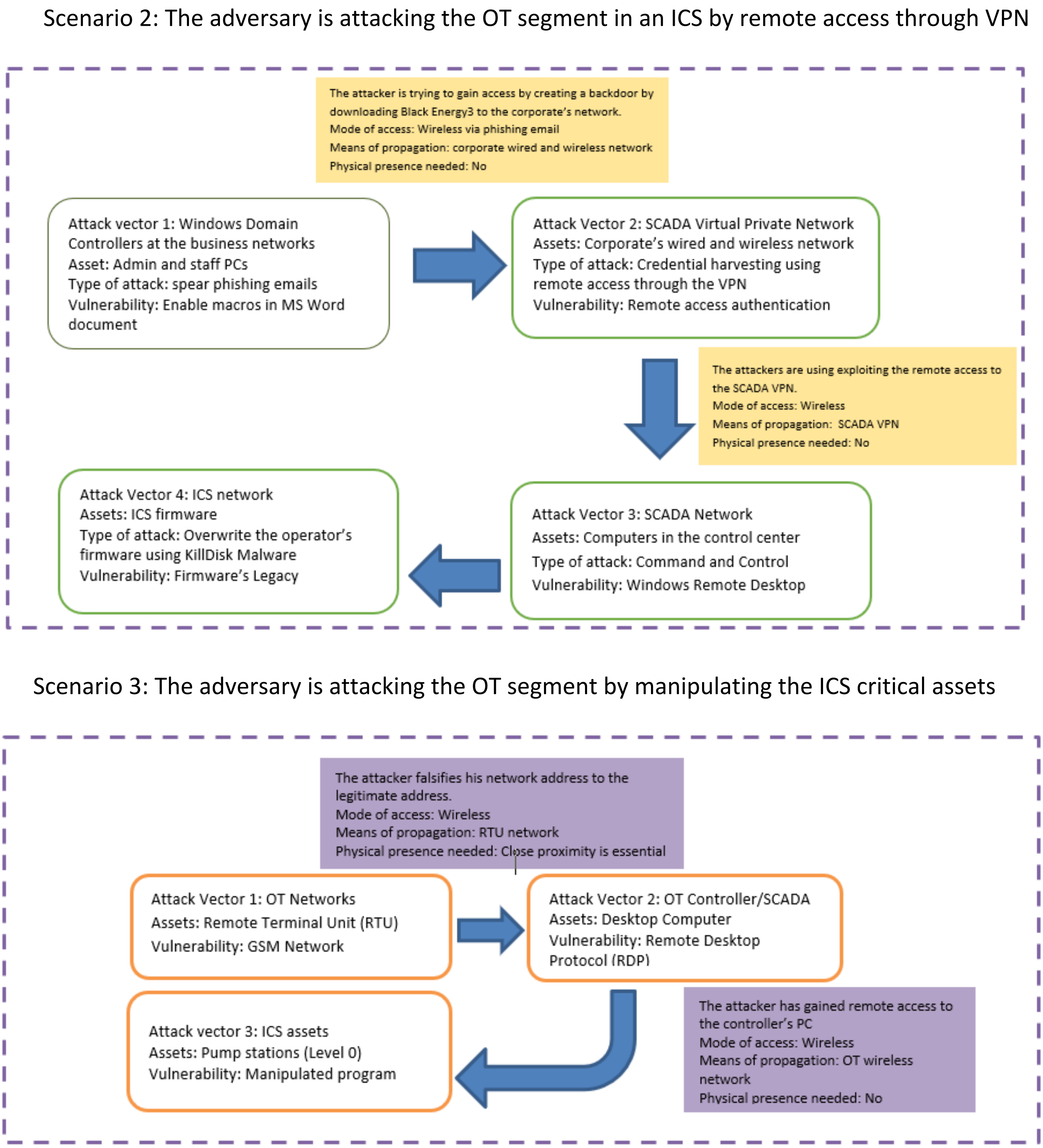
Low: 0 – 0.33, Medium: 0.34 – 0.67, High: 0.68 – 1.00)

4.5 PHASE 5: Assessing the Propagation of the Attacks and Dependencies between the ICS assets

Creating a threat model requires a critical step that involves explaining potential threats in terms of attack propagation. The attack propagation in this model is visualized using a flow chart to demonstrate an attack which possibly initiated by an adversary with malicious intention as presented in Figure 5.

Scenario 1: The adversary is attacking the OT segment in an ICS through the IT/Business Networks


The victim's computer is used as a gateway to the ICS internal network.
Mode of access: Wireless
Means of propagation: Port scanning, credentials harvesting,
Physical presence needed: No
Attack Vector 1: Business network
Asset: Windows based PC, Public facing applications
Type of Attack: Spear phishing, Drive by Compromise
Vulnerability: Human emotions and lack of cybersecurity awareness and SoP
Attack Vector 2: ICS Network
Asset: Engineering Workstation
Type of Attack: Access Escalation, Exploiting the administrator privilege
Vulnerability: Windows services vulnerability, open ports
The Engineering Workstation's VIEW ONLY function is set to FALSE.
Mode of access: Wireless
Means of propagation: Creating backdoor
Physical presence needed: No
Attack Vector 4: ICS Devices
Asset: Level 0 Devices (Process)
Type of Attack: The PLC that is supposed to run a specific process has been maliciously reprogrammed
Vulnerability: PLC's hardcoded credentials and legacy of the product
Attack Vector 3: ICS Network
Asset: Human Machine Interface (HMI)
Type of Attack: Changing the values of the PLC that is displayed in the HMI
The operational settings which programmed in the PLC has been manipulated/ changed
Mode of access: Wireless
Means of propagation: The setting is changed through the HMI of the PLC
Physical presence needed: No



Scenario 2: The adversary is attacking the OT segment in an ICS by remote access through VPN

The attacker is trying to gain access by creating a backdoor by downloading Black Energy3 to the corporate's network.
Mode of access: Wireless via phishing email
Means of propagation: corporate wired and wireless network
Physical presence needed: No
Attack vector 1: Windows Domain Controllers at the business networks
Asset: Admin and staff PCs
Type of attack: spear phishing emails
Vulnerability: Enable macros in MS Word document
Attack Vector 2: SCADA Virtual Private Network
Assets: Corporate's wired and wireless network
Type of attack: Credential harvesting using remote access through the VPN
Vulnerability: Remote access authentication
The attackers are using exploiting the remote access to the SCADA VPN.
Mode of access: Wireless
Means of propagation: SCADA VPN
Physical presence needed: No
Attack Vector 4: ICS network
Assets: ICS firmware
Type of attack: Overwrite the operator's firmware using KillDisk Malware
Vulnerability: Firmware's Legacy
Attack Vector 3: SCADA Network
Assets: Computers in the control center
Type of attack: Command and Control
Vulnerability: Windows Remote Desktop

Scenario 3: The adversary is attacking the OT segment by manipulating the ICS critical assets

The attacker falsifies his network address to the legitimate address.
Mode of access: Wireless
Means of propagation: RTU network
Physical presence needed: Close proximity is essential
Attack Vector 1: OT Networks
Assets: Remote Terminal Unit (RTU)
Vulnerability: GSM Network
Attack Vector 2: OT Controller/SCADA
Assets: Desktop Computer
Vulnerability: Remote Desktop Protocol (RDP)
Attack vector 3: ICS assets
Assets: Pump stations (Level 0)
Vulnerability: Manipulated program
The attacker has gained remote access to the controller's PC
Mode of access: Wireless
Means of propagation: OT wireless network
Physical presence needed: No

Fig. 6. Examples of the threat propagation and dependencies of the ICS assets

5. Discussion and Analysis

An inclusive threat model is achieved once all development phases have been completed. An attackers' centric threat model (TM) is constructed by visualising the propagation of the attack path. The TAs which are categorized into 'adversaries with malicious intent' and 'insiders' are chosen as the main criteria of this TM due to the complexity of the attack vectors in the ICS.

The adversaries with malicious intent can be nation-backed terrorist, business rival or even script kiddies, may be able to attack the ICS through the enterprise network or directly to the OT segment. The main objective of getting into the enterprise network is to gain access, to steal some important credentials for privilege escalation or to set ‘foot hold’ in the network for spying networks’ activities. Once the adversary has gained access in the enterprise network and gain some important credentials of the OT network, the adversaries can start attacking the OT. The lateral propagation of the attack from IT segment to the OT segment is illustrated in Figure 7.

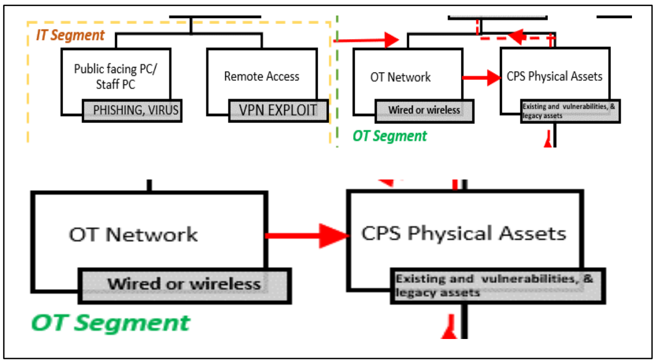


Fig. 7. Lateral threat propagation by the adversaries

Due to the convenience of the remote access features, the adversaries may also leverage this technology to gain access to important files which is stored in the enterprise servers. Furthermore, some PLCs data and information are available in the data historian, hence introducing another opportunity to the adversary to reprogram or manipulate the process flow in the PLCs. Once the PLCs been reprogrammed maliciously, the physical processes in the OT segment might be affected.

Direct attack to the OT system is usually leveraging the known vulnerabilities of the SCADA. Also, due to the heterogeneity of the ICS hardware and devices and also communication technology, such as IoT devices, the attack vector in the ICS has significantly increased. For example, vulnerabilities of the IoT devices can be exploited by the adversaries as a ‘proxy’ to attack its own OT network and may affect the physical processes. Not only that, the adversaries may also use the OT network to propagate to the physical process or change the OT’s safety requirement due to the interconnectivity technologies that are implemented in an ICS. In summary, the advantages adversaries with malicious intent have can be listed below:

i. Increased CPS attack landscapes and size of the logical and physical size of the CPS
ii. Increasing known vulnerabilities databases
iii. Increased attack sophistication with available tools online
iv. More Internet of Things (IoT) devices are used in CPS setting such as IED, smart sensors and surveillance camera.

Insiders are also considered as the TAs in the TM. Three types of insiders are considered in this study which are malicious insiders, negligent insiders and accidental or unintentional insiders. One common advantage the insiders has is physical presence and their interaction with the assets in the OT. A criterion that is discussed in this study is the operational usability aspects of the physical and cyber-physical assets in the OT. The operational usability or behaviours of the insiders may cause direct or indirect hazards to the OT system and the surrounding environment. For instance, disabling the safety alarm to expedite certain processes might compromise the OT safety aspects. On the other hand, hazard might happen indirectly if cyber-physical system such as the HMI is infected with virus, malware, spyware or Trojan. This will give the opportunity for the adversary to launch attack against the ICS remotely. Advantages a malicious insider has can be concluded as below:

i. Physical presence
ii. Wider windows of opportunity
iii. Significant and substantial amount of knowledge about the operations and process

The proposed TM is able to show the effect of operational usability manipulation to the system's security. As defined earlier, security is to protect the system from the intended malicious cyber-attack and behaviours of the insiders in the OT segment may compromised the security. Figure 8 shows how the manipulation of the cyber-physical assets in the OT can create an advantage for the adversary to launch the attack remotely. The TM has shown possible 'bottom-up' threat propagation from the OT to the IT segment.

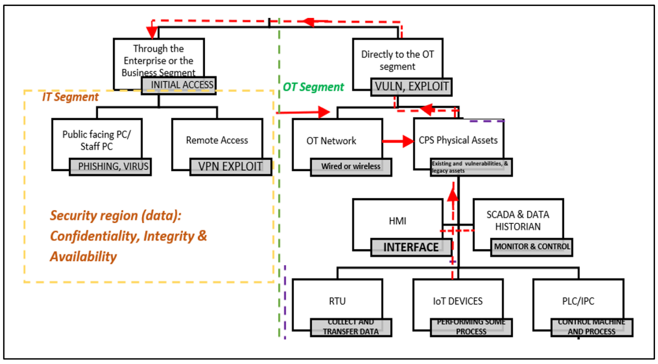

Through the Enterprise or the Business Segment
INITIAL ACCESS
Directly to the OT segment
VULN, EXPLOIT
IT Segment
OT Segment
Public facing PC/ Staff PC
PHISHING, VIRUS
Remote Access
VPN EXPLOIT
OT Network
Wired or wireless
CPS Physical Assets
Existing and vulnerabilities, & legacy assets
Security region (data): Confidentiality, Integrity & Availability
HMI
INTERFACE
SCADA & DATA HISTORIAN
MONITOR & CONTROL
RTU
COLLECT AND TRANSFER DATA
IoT DEVICES
PERFORMING SOME PROCESS
PLC/IPC
CONTROL MACHINE AND PROCESS

Fig. 8. Threats from infected cyber-physical devices to the other segment (bottom-up propagation)

The possible attack from the infected IoT devices in the OT network to its own network or to the adjacent network is also demonstrated by the TM. The proposed complete and inclusive threat model is presented in Figure 9.

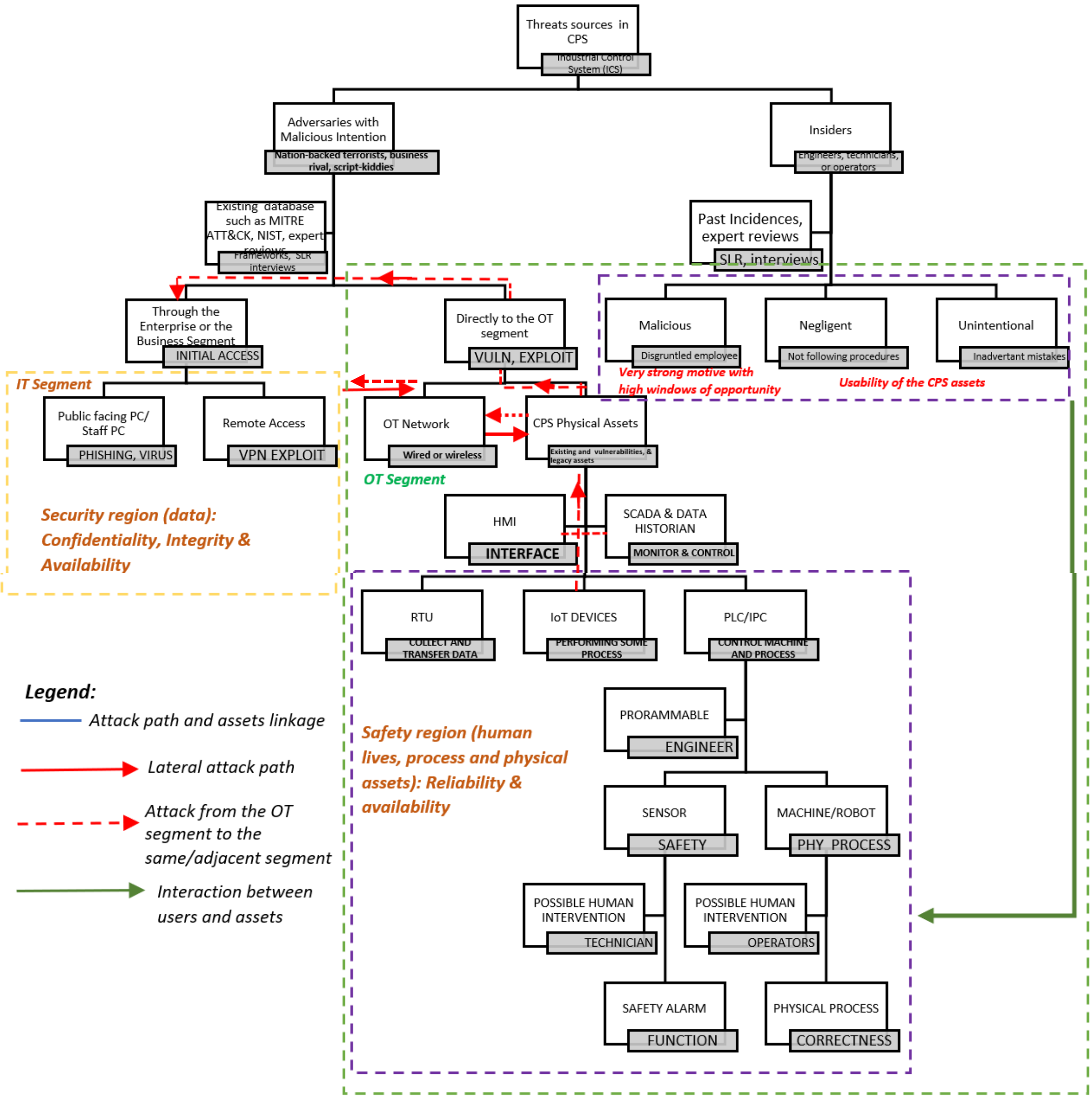

Threats sources in CPS
Industrial Control System (ICS)
Adversaries with Malicious Intention
Nation-backed terrorists, business rival, script-kiddies
Insiders
Engineers, technicians, or operators
Existing database such as MITRE ATT&CK, NIST, expert reviews
Frameworks, SLR interviews
Past Incidences, expert reviews
SLR, interviews
Through the Enterprise or the Business Segment
INITIAL ACCESS
Directly to the OT segment
VULN, EXPLOIT
Malicious
Disgruntled employee
Negligent
Not following procedures
Unintentional
Inadvertant mistakes
Very strong motive with high windows of opportunity
Usability of the CPS assets
IT Segment
Public facing PC/ Staff PC
PHISHING, VIRUS
Remote Access
VPN EXPLOIT
OT Network
Wired or wireless
CPS Physical Assets
Existing and vulnerabilities, & legacy assets
OT Segment
HMI
INTERFACE
SCADA & DATA HISTORIAN
MONITOR & CONTROL
Security region (data): Confidentiality, Integrity & Availability
RTU
COLLECT AND TRANSFER DATA
IoT DEVICES
PERFORMING SOME PROCESS
PLC/IPC
CONTROL MACHINE AND PROCESS
PRORAMMABLE
ENGINEER
Legend:
Attack path and assets linkage
Lateral attack path
Attack from the OT segment to the same/adjacent segment
Interaction between users and assets
Safety region (human lives, process and physical assets): Reliability & availability
SENSOR
SAFETY
MACHINE/ROBOT
PHY PROCESS
POSSIBLE HUMAN INTERVENTION
TECHNICIAN
POSSIBLE HUMAN INTERVENTION
OPERATORS
SAFETY ALARM
FUNCTION
PHYSICAL PROCESS
CORRECTNESS

Fig. 9. The proposed inclusive threat model for ICS

6. Using Inclusive Threat Model as a Tool for Inclusive Risk Assessment

As for the further work, the proposed threat model will be used as a model to assess security and safety risks in an ICS. A risk assessment metric which will include both security and safety aspects of an ICS will be developed as a reference for ICS stakeholders. A semi-quantitative security and safety risk assessment formula might be useful during the decision making while implementing safety and security threats counter-measures or mitigation system. In proposing an inclusive and quantitative risk assessment for ICS, certain factors need to be considered such as overall likelihood and TA score. The authors in [28] has proposed formula for Cyber-Security risk assessment as the function of overall likelihood and impact. However, the TA score as the result of interaction between the insiders and the OT assets was not considered in their study. Hence, in this study we are proposing an inclusive CPS risk assessment formula which is a function of overall likelihood, impact and attacker's score as shown in Eq. (1) until Eq. (3).

F1= Attackers Score (Intent, Capability, Targeting, Purdue Operational Level Access)

$$F1 = \sum_{1}^{\mathrm{n}} \frac{(\text{Intent+Targeting+Capabilities+Purdue Operational Level Access})}{4} \tag{1}$$

F2 = Overall Likelihood (Attacker's Score, Vulnerability of the Attack Vector, Control and Mitigation)

$$F2 = \sum_{1}^{n} \frac{(\text{Attacker's Score+Vulnerability of the Attack Vector+Control and Mitigation})}{3} \tag{2}$$

F3 = Risk (Overall Likelihood, Impact)

$$F3 = \sum_{1}^{n} \frac{(\text{Overall Likelihood+Impact})}{2} \tag{3}$$

The quantification of the risk will be realized using Mamdani Fuzzy Inference System (FIS) [29] and will be simulated using Fuzzy Logic Toolbox in Matlab which is based on fuzzy inference process as shown in Figure 10. Based on Figure 10, crisp input is in the form of intuitive inputs which is based on database, past and current incidents and expert reviews. The followings are the steps in fuzzy inference system.

a. Fuzzification: Define the membership functions for each input variable. These functions describe how inputs are mapped to fuzzy sets.
b. Rule Base: Create a set of fuzzy rules that relate the input variables to the output variable. These rules should be based on expert knowledge or data.
c. Inference Engine: Implement the Mamdani inference method, which combines the fuzzy rules to produce fuzzy output.
d. Defuzzification: Define the membership functions for the output variable and use a defuzzification method (e.g., centroid, mean of maxima) to obtain a crisp output value.

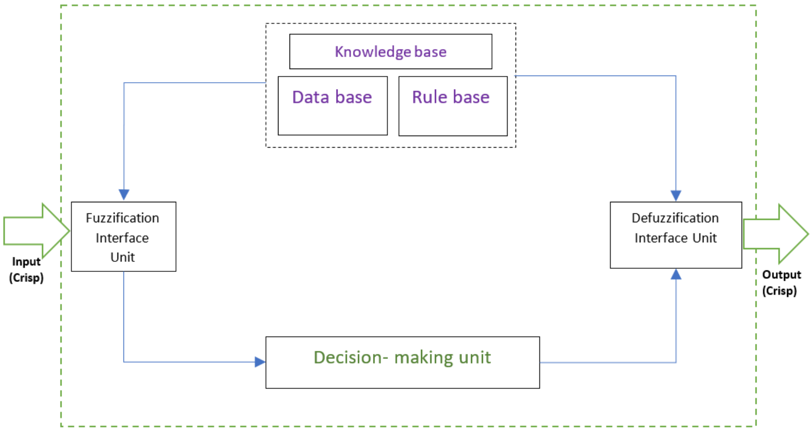


Fig. 10. Fuzzy inference process

The proposed fuzzification blocks for risk quantification which base on Eq. (1) until Eq. (3) is demonstrated in Figure 11.

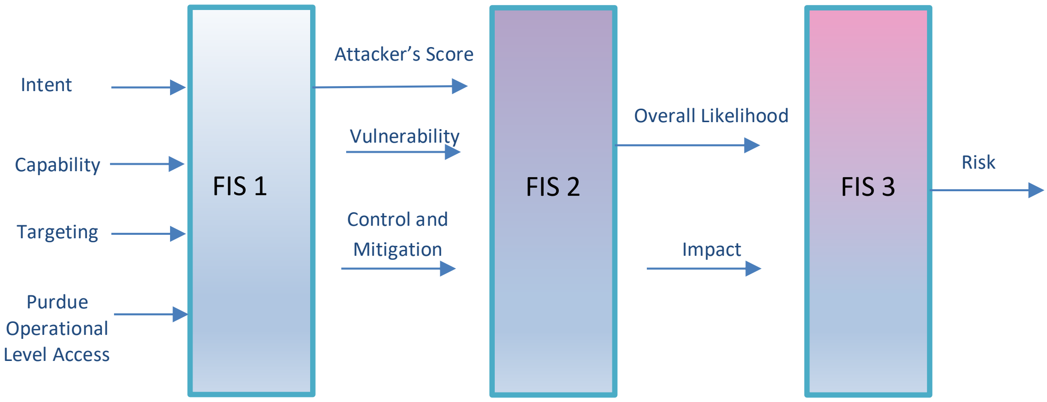


Fig. 11. Proposed Mamdani Fuzzy Interference System (FIS) for Inclusive Risk Assessment (adapted from Mansour *et al.,* [28])

The cascaded system is designed using Fuzzy Logic Designer Toolbox in Matlab software version R2023b. A cascaded Mamdani is proposed in this study to break down the complex components of the risk factors. The chosen function is FISTree (Fuzzy Inference System Tree) which comprises of three blocks which are FIS 1, FIS 2 and FIS 3. FIS 1 is a fuzzy inference block that is used to calculate the value of the attacker's score. FIS 1 is a function of Intent, Capability, Targeting and Purdue Operation Level Access. Different threat actor will be assigned different levels of Intent, which is assessed by using their motives of attack. For example, malicious external adversaries and malicious insiders will be assigned the highest level of Intent which is '1 = High', while internal negligent insiders will be assigned moderate value of Intent which is '0.5 = Medium'. On the other hand, internal accidental or unintentional insiders will be assigned a '0 = Low' value of Intent. Capability and Targeting will vary for malicious external adversaries and insiders which will be assigned different values from Low (0 to 0.33), Medium (0.34 to 0.67) and High Level (0.68 to 1.00). While for accidental or unintentional insiders, the Capability will vary from Low to High level and for the targeting '0' value will be assigned to this type of potential attackers. The highest value which is '1' is assigned for Purdue Operational Level Access to the all insiders as they have the advantage of physical presence in the OT. As for the external adversaries, the value for the access to the Purdue Operational Level is medium (0.5). This is due to the fact that these external adversaries may be able to access the OT segment virtually, hence they do not have the privilege of the physical presence as compared to the insider attackers.

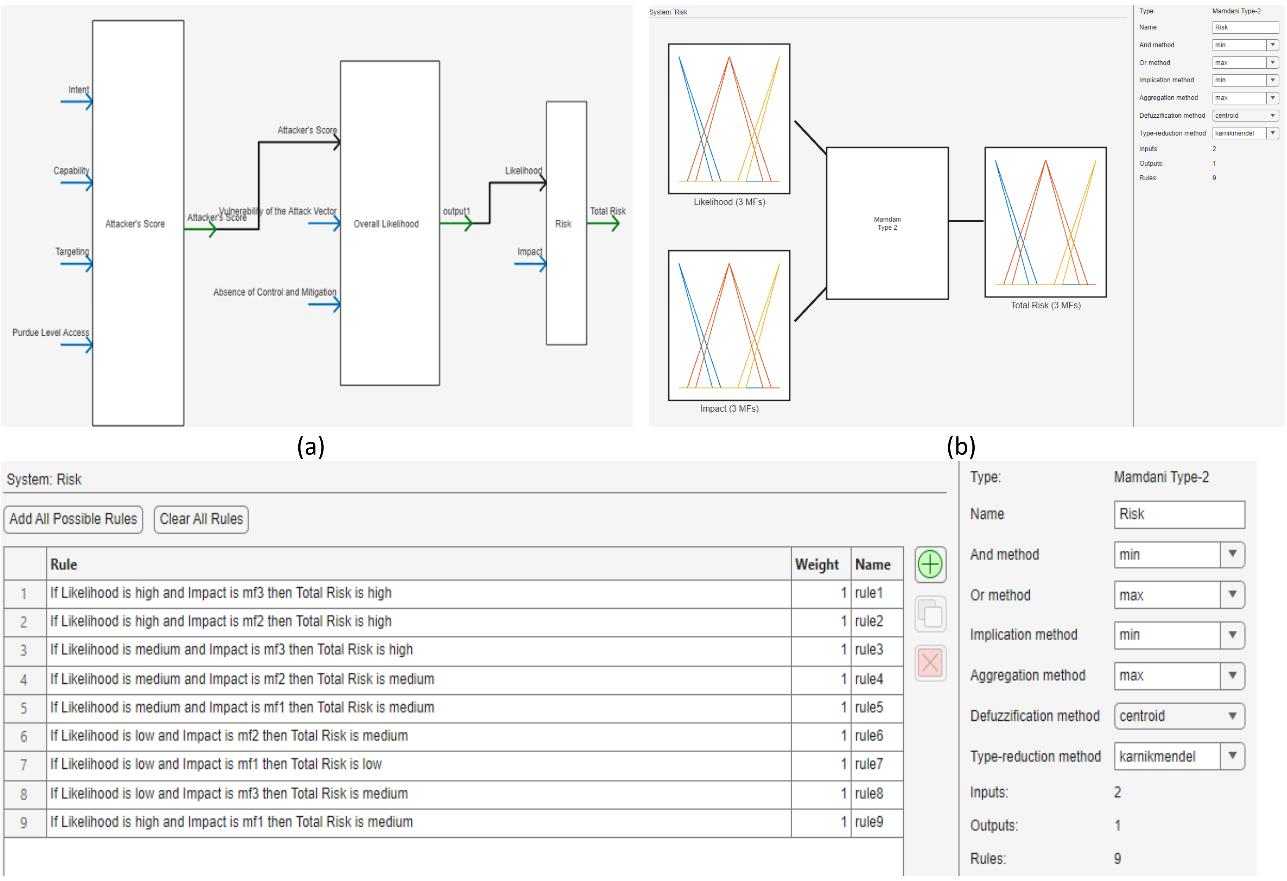
In order to calculate likelihood of the attacks, the attacker's score which is derived from FIS 1 is used as one of the inputs in the FIS 2. Other than attacker's score, vulnerability of the attack vectors and absence of control and mitigation to the threats are the other inputs to FIS2. The values of vulnerability and absence control and mitigation assigned to the different threat actors are based on Possible Threat Events (TE) Initiated by the identified Threat Actors (TA) matrix.

Finally, the overall risk is calculated in FIS3 as the function of likelihood and impact. The likelihood score is derived in FIS2 and the impact is evaluated based on the impact of attack economy, public and environmental including human loss.

6. Results and Findings

In order to calculate the total risks, the following steps are followed. The ultimate output from the risk assessment is to calculate the risk imposed by different Threat Actors, (TA) in different Threat Events (TE) scenarios. The outputs from Matlab Fuzzy Logic Designer simulations are shown in Figure 12.

i. Set input and output descriptor for each FIS block.
ii. Apply membership function for each input and output. In this case, triangle membership function (trimf) is used.
iii. Design and program the cascaded FIS using FISTree Function in MATLAB Fuzzy Logic Designer version R2023b.
iv. Tune the membership function and add/customize rules for each FIS using the Threat Actor and Threat Event Matrices.
v. Justify the risk for variations of inputs according to the TA and TE metrics table to evaluate the rules.



(a)

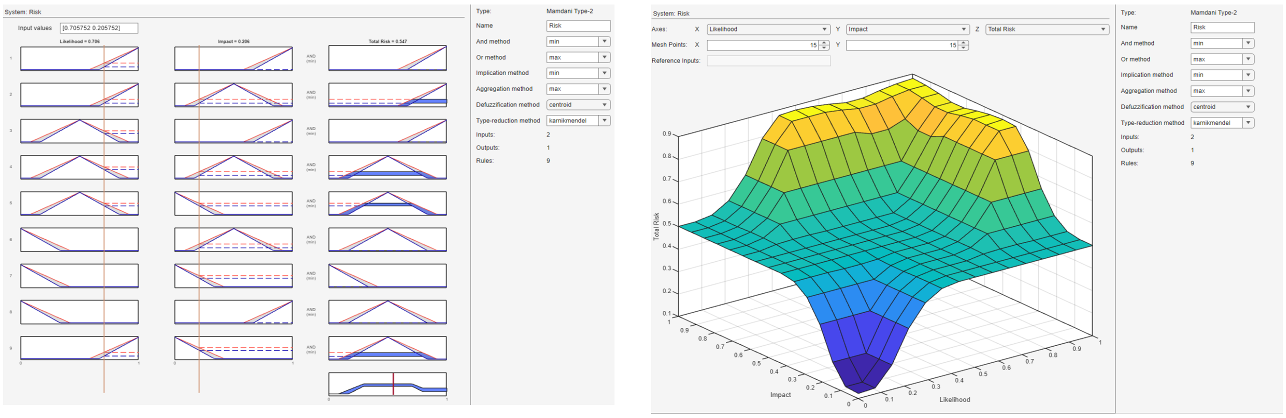
(b)

System: Risk

	Rule	Weight	Name
1	If Likelihood is high and Impact is mf3 then Total Risk is high	1	rule1
2	If Likelihood is high and Impact is mf2 then Total Risk is high	1	rule2
3	If Likelihood is medium and Impact is mf3 then Total Risk is high	1	rule3
4	If Likelihood is medium and Impact is mf2 then Total Risk is medium	1	rule4
5	If Likelihood is medium and Impact is mf1 then Total Risk is medium	1	rule5
6	If Likelihood is low and Impact is mf2 then Total Risk is medium	1	rule6
7	If Likelihood is low and Impact is mf1 then Total Risk is low	1	rule7
8	If Likelihood is low and Impact is mf3 then Total Risk is medium	1	rule8
9	If Likelihood is high and Impact is mf1 then Total Risk is medium	1	rule9

Type: Mamdani Type-2
Name: Risk
And method: min
Or method: max
Implication method: min
Aggregation method: max
Defuzzification method: centroid
Type-reduction method: karnikmendel
Inputs: 2
Outputs: 1
Rules: 9

(c)



System: Risk

Input values [0.705752 0.205752]

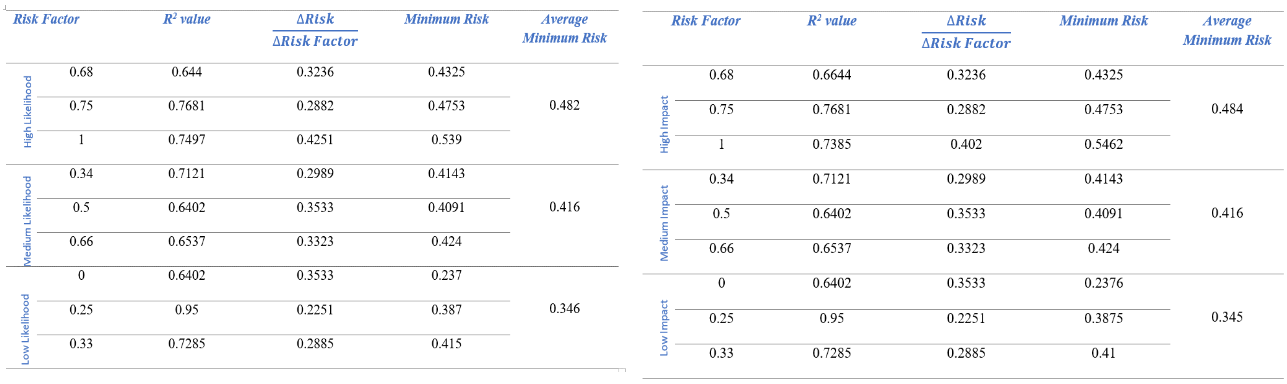
Type: Mamdani Type-2
Name: Risk
And method: min
Or method: max
Implication method: min
Aggregation method: max
Defuzzification method: centroid
Type-reduction method: karnikmendel
Inputs: 2
Outputs: 1
Rules: 9

System: Risk
Axes: X Likelihood Y Impact Z Total Risk
Mesh Points: X 15 Y 15
Reference Inputs:

(d) (e)

Fig. 12. (a) FISTree I/O descriptor (b) Membership functions for likelihood impact and total risk (c) Rules to calculate overall risk (d) FIS Rule Inference System (e) Matlab Surface plot for Risk

By using Matlab Rule Inference System, different scenarios of possible inputs were tested in FIS3 to calculate risk values. 9 possible combinations were tested for High, Medium and Low Impact and Likelihood and the outputs were analysed using Linear Regression in Microsoft Excel. From the regression test, it has been observed that for both conditions the average minimum risk is almost similar. From the results shown in Figure 13, the average minimum risks for High, Medium and Low Likelihood and Impact are 0.483, 0.416 and 0.346 respectively.



	Risk Factor	R^2 value	$\frac{\Delta Risk}{\Delta Risk\ Factor}$	Minimum Risk	Average Minimum Risk
High Likelihood	0.68	0.644	0.3236	0.4325	0.482
	0.75	0.7681	0.2882	0.4753	
	1	0.7497	0.4251	0.539	
Medium Likelihood	0.34	0.7121	0.2989	0.4143	0.416
	0.5	0.6402	0.3533	0.4091	
	0.66	0.6537	0.3323	0.424	
Low Likelihood	0	0.6402	0.3533	0.237	0.346
	0.25	0.95	0.2251	0.387	
	0.33	0.7285	0.2885	0.415	

(a)

	Risk Factor	R^2 value	$\frac{\Delta Risk}{\Delta Risk\ Factor}$	Minimum Risk	Average Minimum Risk
High Impact	0.68	0.6644	0.3236	0.4325	0.484
	0.75	0.7681	0.2882	0.4753	
	1	0.7385	0.402	0.5462	
Medium Impact	0.34	0.7121	0.2989	0.4143	0.416
	0.5	0.6402	0.3533	0.4091	
	0.66	0.6537	0.3323	0.424	
Low Impact	0	0.6402	0.3533	0.2376	0.345
	0.25	0.95	0.2251	0.3875	
	0.33	0.7285	0.2885	0.41	

(b)

Fig. 13. Average minimum risk imposed by different TA (a) Relationship between Impact and Risk (b) Relationship between Likelihood and Risk

7. Conclusion

This study has proposed models to show the relationship between usability, security and safety in a CPS. The models suggested the importance of including the safety aspect in developing the threat model in a CPS. The proposed models have shown that security and safety is strongly related by means of usability aspects. Non conflicting security and safety requirements for CPS and good practices of usability of physical and cyber-physical assets is also summarized in this study. The underlying understanding in the proposed model is used to develop an Inclusive Threat Model (ITM) that demonstrates the interaction between the threat actors and the assets and the propagation of the threats from the enterprise to the OT network and to the OT assets. The possible threat propagation from the OT assets (such as IoT devices) to the OT network and the IT segment is also shown in the proposed threat model. The assessments of the Threat Actors in the Threat Actors metrics and the evaluation of the Threat Events in the Threat Events metrics have been carried out in this study as part of the risk quantification as proposed for the further work.

Based on the proposed threat model, risk quantification is done using Fuzzy Logic inference system. Mamdani Fuzzy Logic inference is chosen as the quantification method because the method is well suited to human input. In this research, the input is elaborated using the knowledge base developed in the initial phase. Furthermore, Mamdani Fuzzy Logic Inference system represents more interpretable rule based and does have wide spread acceptance. From the first phase of the simulation using Matlab software, it has been observed that the risk values imposed by all the Threat Actors are significant (in the medium range). Hence, conducting risk assessment in a CPS, particularly ICS as part of the security and safety exercise mitigation plan is highly recommended.

Acknowledgement

This research was not funded by any grant.

References

[1] Rajkumar, Ragunathan, Insup Lee, Lui Sha, and John Stankovic. "Cyber-physical systems: the next computing revolution." In *Proceedings of the 47th design automation conference*, pp. 731-736. 2010. https://doi.org/10.1145/1837274.1837461

[2] El-Kady, Ahmed Hamdy, Syeda Halim, Mahmoud M. El-Halwagi, and Faisal Khan. "Analysis of Safety and Security Challenges and Opportunities Related to Cyber-physical Systems." *Process Safety and Environmental Protection* (2023). https://doi.org/10.1016/j.psep.2023.03.012

[3] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." *Computer networks* 148 (2019): 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

[4] Babu, Bijoy, Thafasal Ijyas, P. Muneer, and Justin Varghese. "Security issues in SCADA based industrial control systems." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 47-51. IEEE, 2017. https://doi.org/10.1109/Anti-Cybercrime.2017.7905261

[5] Mashkina, Irina, and Ildar Garipov. "Threats modeling and quantitative risk analysis in industrial control systems." In *2018 International Russian Automation Conference (RusAutoCon)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/RUSAUTOCON.2018.8501694

[6] Jin, Yunye, and Hwee Pink Tan. "UNISENSE: A Unified and Sustainable Sensing and Transport Architecture for Large Scale and Heterogeneous Sensor Networks." In *Complex Systems Design & Management Asia: Designing Smart Cities: Proceedings of the First Asia-Pacific Conference on Complex Systems Design & Management, CSD&M Asia 2014*, pp. 15-26. Springer International Publishing, 2015. https://doi.org/10.1007/978-3-319-12544-2_2

[7] Lyu, Xiaorong, Yulong Ding, and Shuang-Hua Yang. "Safety and security risk assessment in cyber-physical systems." *IET Cyber-Physical Systems: Theory & Applications* 4, no. 3 (2019): 221-232. https://doi.org/10.1049/iet-cps.2018.5068

[8] Akbarzadeh, Aida, and Sokratis K. Katsikas. "Dependency-based security risk assessment for cyber-physical systems." *International Journal of Information Security* 22, no. 3 (2023): 563-578. https://doi.org/10.1007/s10207-022-00608-4

[9] Ning, Xirong, and Jin Jiang. "Defense-in-depth against insider attacks in cyber-physical systems." *Internet of Things and Cyber-Physical Systems* 2 (2022): 203-211. https://doi.org/10.1016/j.iotcps.2022.12.001

[10] M. Kamal, "ICS Layered Threat Modeling," (2021).

[11] Khalil, Shaymaa Mamdouh, Hayretdin Bahsi, Henry Ochieng'Dola, Tarmo Korõtko, Kieran McLaughlin, and Vahur Kotkas. "Threat Modeling of Cyber-Physical Systems-A Case Study of a Microgrid System." *Computers & Security* 124 (2023): 102950. https://doi.org/10.1016/j.cose.2022.102950

[12] Jbair, Mohammad, Bilal Ahmad, Carsten Maple, and Robert Harrison. "Threat modelling for industrial cyber physical systems in the era of smart manufacturing." *Computers in Industry* 137 (2022): 103611. https://doi.org/10.1016/j.compind.2022.103611

[13] Vasilyev, Vladimir, Anastasia Kirillova, Alexey Vulfin, and Andrey Nikonov. "Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score." In *2021 International Conference on Information Technology and Nanotechnology (ITNT)*, pp. 1-6. IEEE, 2021. https://doi.org/10.1109/ITNT52450.2021.9649191

[14] Huang, Kaixing, Chunjie Zhou, Yu-Chu Tian, Weixun Tu, and Yuan Peng. "Application of Bayesian network to data-driven cyber-security risk assessment in SCADA networks." In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1-6. IEEE, 2017. https://doi.org/10.1109/ATNAC.2017.8215355

[15] Bernsmed, Karin, Christian Frøystad, Per Håkon Meland, Dag Atle Nesheim, and Ørnulf Jan Rødseth. "Visualizing cyber security risks with bow-tie diagrams." In *Graphical Models for Security: 4th International Workshop, GraMSec 2017, Santa Barbara, CA, USA, August 21, 2017, Revised Selected Papers 4*, pp. 38-56. Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-74860-3_3

[16] Li, Karen, Awais Rashid, and Anne Roudaut. "Vision: Security-Usability Threat Modeling for Industrial Control Systems." In *Proceedings of the 2021 European Symposium on Usable Security*, pp. 83-88. 2021. https://doi.org/10.1145/3481357.3481527

[17] Tantawy, Ashraf, Sherif Abdelwahed, Abdelkarim Erradi, and Khaled Shaban. "Model-based risk assessment for cyber physical systems security." *Computers & Security* 96 (2020): 101864. https://doi.org/10.1016/j.cose.2020.101864

[18] Mockel, Caroline. "Usability and security in eu e-banking systems-towards an integrated evaluation framework." In *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 230-233. IEEE, 2011. https://doi.org/10.1109/SAINT.2011.42

[19] Braun, Virginia, and Victoria Clarke. "Using thematic analysis in psychology." *Qualitative research in psychology* 3, no. 2 (2006): 77-101. https://doi.org/10.1191/1478088706qp063oa

[20] Gu, Tingyang, Minyan Lu, and Luyi Li. "Extracting interdependent requirements and resolving conflicted requirements of safety and security for industrial control systems." In *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, pp. 1-8. IEEE, 2015. https://doi.org/10.1109/ICRSE.2015.7366481

[21] Banerjee, Ayan, Krishna K. Venkatasubramanian, Tridib Mukherjee, and Sandeep Kumar S. Gupta. "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems." *Proceedings of the IEEE* 100, no. 1 (2011): 283-299. https://doi.org/10.1109/JPROC.2011.2165689

[22] Gerson, Sharon J., and Steven M. Gerson. *Technical communication: Process and product*. Vol. 83. Pearson, 2014.

[23] Trend Micro. “Industrial Control System,” (2023). https://www.trendmicro.com/vinfo/my/security/definition/industrial-control-system

[24] “MITRE ATT&CK Enterprise.” (2023). https://attack.mitre.org/tactics/enterprise

[25] Nist, and Emmanuel Aroms. "NIST Special Publication 800-18 Revision 1 Guide for Developing Security Plans for Federal Information Systems." (2012).

[26] AlMajali, Anas, Khalil M. Ahmad Yousef, Bassam J. Mohd, Waleed Dweik, and Salah Abu Ghalyon. "Semi-quantitative security risk assessment of robotic systems." *Jordanian Journal of Computers and Information Technology* 4, no. 3 (2018).

[27] Ackerman, Pascal. *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing Ltd, 2017.

[28] Alali, Mansour, Ahmad Almogren, Mohammad Mehedi Hassan, Iehab AL Rassan, and Md Zakirul Alam Bhuiyan. "Improving risk assessment model of cyber security using fuzzy logic inference system." *Computers & Security* 74 (2018): 323-339. https://doi.org/10.1016/j.cose.2017.09.011

[29] Zadeh, L. A. "Fuzzy sets. informat control." *vol* 8 (1965): 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X