Threat Modeling of Cyber-Physical Systems in Practice

Ameerah-Muhsinah Jamil[1], Lotfi ben Othmane[1], and Altaz Valani[2]

[1] Iowa State University, Ames, IA
[2] Security Compass, Canada

Abstract. Traditional Cyber-physical Systems (CPSs) were not built with cybersecurity in mind. They operated on separate Operational Technology (OT) networks. As these systems now become more integrated with Information Technology (IT) networks based on IP, they expose vulnerabilities that can be exploited by the attackers through these IT networks. The attackers can control such systems and cause behavior that jeopardizes the performance and safety measures that were originally designed into the system. In this paper, we explore the approaches to identify threats to CPSs and ensure the quality of the created threat models. The study involves interviews with eleven security experts working in several different domains. We found through these interviews that the practitioners use a combination of various threat modeling methods, approaches, and standards together when they perform threat modeling of given CPSs. Key challenges practitioners face are: they cannot transfer the threat modeling knowledge that they acquire in a cyber-physical domain to other domains, threat models of modified systems are often not updated, and the reliance on mostly peer-evaluation and quality checklists to ensure the quality of threat models. The study warns about the difficulty to develop secure CPSs and calls for research on developing practical threat modeling methods for CPSs, techniques for continuous threat modeling, and techniques to ensure the quality of threat models.

1 Introduction

In the past, CPSs operated on their own networks, which were separated or air-gapped from the corporate IT networks. The OT and IT networks started converging in response to the need to provide data and insights to stakeholders on IT networks. The challenge with integrating these technologies is the velocity of change: IT technologies tend to change very frequently, and updates or patches can be readily done while OT technologies have a considerably longer shelf life. Legacy security concerns when OT technologies were initially deployed can be significantly different from the present security concerns. Trying to capture this disparity is done, in part, through threat modeling.

Until recently, attackers needed physical access to CPSs. The trend of integrating these systems to IP networks and the internet for services, such as remote car diagnostic and cooperative adaptive cruise control, has extended the attack surface. The goals of attacks on CPSs, such as Stuxnet and Triton,

are often not to breach the confidentiality, integrity, or availability of the system's data but to make the target system perform activities other than the ones planned and expected by the original designers. Hence changing the actual process and unleashing damaging consequences.

Threat modeling is a "systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service" [1]. It is an approach for identifying threats to a system and suggesting mitigations. In this paper, we will not discuss mitigations and limit the scope to threats.

There are several methods for threat modeling, including threat tree, attack tree, STRIDE, and abuse cases [2]. Xiong and Lagerstrom surveyed threat modeling literature. The authors of many of the surveyed papers validated their proposed approaches (22 out of the 54 selected papers) using, for example, case studies, and simulation while only two papers used real-word applications [3]. Most of these methods have been designed for information systems where the assets are data at rest and in-transit. The focus on data within the IT network is an important one. Threat modeling of OT components can often be physically dangerous, expensive, or even identifying the data flow before it gets to the OT but may not be sufficient to identify misuses of CPSs.

Xiong and Lagerstrom's survey of threat model literature [3] discussed above shows that there is a gap between the academic research on and the practice of threat modeling of CPSs. This paper aims to address that by answering the question: *What are the practices of threat modeling of CPSs by cyber-security experts?* To address this question, we interviewed eleven security experts who perform threat modeling of CPSs in their respective organizations. Then, we transcribed the interviews, extracted the main information, and grouped them into themes, and analyzed the findings. We found that:

1. there is a lack of effective systematic threat modeling methods for CPSs; the practitioners use a combination of threat modeling methods, approaches, and standards, together, when performing threat modeling of CPSs;
2. organizations often do not update the threat models of their modified CPSs;
3. there is no effective method for ensuring the quality of threat models besides peer-evaluation and quality checklists;
4. the practitioners face several challenges when performing threat modeling of CPSs, including the difficulty to transfer the threat modeling knowledge they acquire in a cyber-physical domain to other domains.

The results of this work could be used by organizations when performing threat modeling of CPSs and by academia to develop solutions and techniques that help practitioners perform threat modeling efficiently.

This paper is organized as follows: Section 2 discusses related works, Section 3 describes the research approach, Section 4 presents the results of the study, Section 5 summarizes the study results and discusses the impacts and limitations of the study, and Section 6 concludes the paper.

2 Related Work

This section discusses related work on the security of CPSs and threat modeling methods and standards.

Security of CPSs. Security issues of CPSs has been studied for several years. For instance, Alguliyev et al. [4] analyzed the main types of attacks and threats of CPSs and proposed a tree of attacks that includes the attacks on sensing, actuation, computing, communication, and feedback loops; Lu et al. [5] proposed a framework of CPSs security, which includes the security objectives, approaches, and applications of CPSs; and Pakizeh[6] proposed a framework that aims to understand the cyber attacks and related risk of different elements of CPSs [6]. In addition, using the expert knowledge on security aspects, such as the forms of attacks, attacker positions, operating systems, and routing permissions Klaudel and Rataj [7] proposed an attack graph that describes the software and hardware of a CPS and their mutual mapping with security artifacts and a workflow that automates the construction of a vulnerability model of a CPS that is used to quantitatively analyze the threat models of the CPSs, and estimate their exploitation costs.

The concern in security in IT is the reduction of monetary losses and is the safety of people and controllability of the systems, besides the reduction of monetary losses, in the case of CPSs [8]. Sabaliauskaite and Mathur [9] proposed the integration of safety and security life-cycle processes and a model that unifies the attack tree and the fault tree and their countermeasures. Dong et al. [10] proposed security and safety framework, and security framework that focuses on the security of information and controllability of the CPSs.

The National Institute of Standards and Technology (NIST) developed a CPS framework to assist in developing secure and safe CPSs [11]. The security concern of the framework is to protect CPSs from unauthorized accesses, change damages, and destruction in addition to the CIA triad, and the safety concern is preventing negative consequences of cyber attacks on the stakeholders, including life, health, property, data, and damage to the physical environment.

Threat Modeling methods and standards. There exist several works on threat modeling for CPSs [3]. For instance, Martins et al. [12] proposed a tool for systematic analysis of threat models that includes sketching metamodel of the system using GME, defining the data-flow and its attribute, and identifying the vulnerabilities that may exist in the data-flow connections. Also, Khan et al. [13] adapted the STRIDE method for CPSs by focusing on the data-flow between the components of the system, which demonstrated promising results when applied to a case study as it identifies the vulnerabilities at cyber subsystems and their potential consequences on the physical components of the system. In addition, Casola et al. [14] developed a threat catalog that consists of known threats affecting different components of IoT and classified them based on asset types.

Several researchers acknowledged the impact of application domains on the threat modeling of CPSs. For instance, Meyer et al. [15] proposed an attack

tree to threat model building and home automation systems in order to identify security faults either in implementation or deployment, and Suleiman et al. [16] developed a comprehensive threat modeling by integrating the results of smart grid system security threat analysis with the reference architecture of smart grid including the components and communication among them.

The International Standards Organization (ISO) and SAE International released standard ISO/SAE 21434- Road vehicles cybersecurity engineering to address the need in cybersecurity engineering of electrical and electronic systems within road vehicles. The standard provides guidelines to integrate cybersecurity concerns in product development, and perform cybersecurity assessment and monitoring, and develop policies to handle cybersecurity incidents.

This paper addresses the gap between the development of threat modeling methods, techniques, and standards and the practice of threat modeling of CPSs.

3 Research Approach

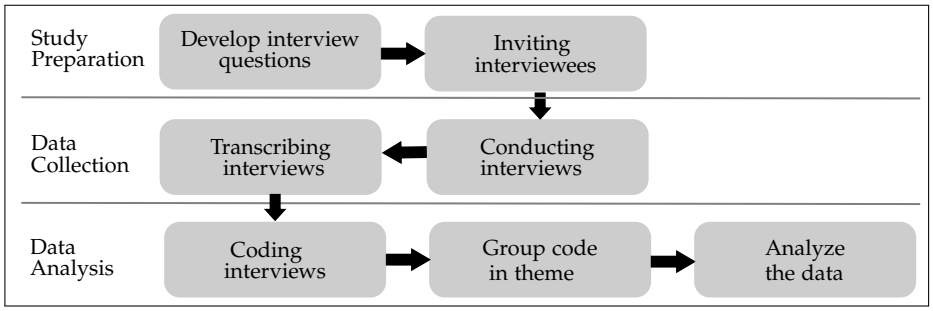

FIG. 1: Phases of the study.

This study aims to explore the practice of threat modeling of CPSs in the industry. The data source of the study comes from interviewing a set of security experts practicing threat modeling. Figure 1 illustrates the process of the study, which has three phases: study preparation, data collection, and data analysis. The descriptions of the phases follow.

3.1 Study Preparation

The description of the study preparation follows.

Interview protocol. We reviewed the literature on threat modeling of a CPS. We used the knowledge that we acquired to develop a questionnaire protocol. We specified the research goal with the project sponsor and formulated a set of open-ended interview questions. The questionnaire was tested by trial runs with team members and revised based on the feedback. The set of questions consists of eleven open-ended questions–Open-ended questions encourage the participants to provide detailed responses.

Participants selection. We invited a set of security experts working in cybersecurity companies. Eleven participants accepted our requests and participated

TABLE 1: Business of each participant.

Participant	Business
P1	Security consultation
P2	Software engineering
P3	Security consultation
P4	Areal vehicles integrator
P5	Software engineering
P6	Software engineering
P7	Security consultation
P8	Ground vehicles integrator
P9	Ground vehicles integrator
P10	Original Equipment Manufacturer (OEM)
P11	Ground vehicles integrator

in the study with the goal to contribute to science, not to represent their employers. Table 1 shows the experience of each participant on threat modeling and the business of their employers. Among the participants, three work for major software development companies and five work for major companies that develop CPSs.

TABLE 2: Threat modeling themes.

Theme	Description
Security aspects	It concerns confidentiality, integrity, and availability.
Threat business impacts	The other aspects that the participant is concerned about when performing threat modeling including users' safety and company reputation.
Threat modeling approaches	The approaches and methods that the participants use for threat modeling, e.g., asset-centric, attacker-centric, STRIDE etc.
Threat identification methods	The methods that the participants use to identify the threats which is part of the threat modeling process.
Threat modeling steps	The activities or steps performed by the experts to identify the threat model of a given system.
Continuous Threat modeling	The process used to update threat models to address system changes.
Quality assurance of threat models	The methods used to assess and evaluate the quality of the threat models.
Tools	The tools used in the threat modeling process.
Involved people	People involved in the threat modeling process.
Challenge	The challenge that experts face when performing threat modeling for CPSs.
Suggestion	Suggestions to improve the threat modeling process for CPSs.

3.2 Data Collection

The data collection consists of two sub-phases: conducting the interviews and transcribing the interviews. The descriptions of these sub-phases follow.

Conducting the interview. We scheduled a one-hour meeting with each expert. The meetings were held through Zoom and Web-ex because the interviewers and participants are located in different places. The interviews were conducted by one of the authors. The interviewer explained to each of the interviewees at the beginning of each of the meetings the goal of the project, the interview process and requested the consent of the participant to record the interview.
Transcription of the interviews. The interviews were transcribed using oTranscribe [3] and Otter.ai. [4].

3.3 Data Analysis

Interview coding. We used the thematic analysis method for the interview coding [17]. Thematic analysis is "a method for identifying, analyzing and reporting patterns within data" [18]. It allows researchers to explore phenomena through interviews, stories, and observations [19].

Interview coding uses the interview transcripts as the input and outputs codes that identify the aspects mentioned during the interviews. A code is a word or short phrase identifying the essence of a portion of text. At the end of this step, we assigned codes to each of the eleven interview transcripts. For example, we assigned code *security properties/goal* to the text *"When it comes to the CPSs, the availability of the system matters a lot"*. Codes that were semantically similar across transcripts were consolidated. We used Atlas.ti [5] tool to code the interviews.
Data extraction and classification. Similar codes are grouped into themes. A theme generalizes a set of codes belonging to a given concept. The process of assigning themes to codes was done for each transcript. For example, the code *other aspect* and *safety aspect* is grouped together as *threat business impact* theme. Table 2 lists the themes and associated categories.
Analysis of the results. From the code groups, we identified information on security properties, threat business impacts, threat modeling approaches, and method, threat modeling details activity, continuous threat modeling approach, threat identification methods, continuous threat modeling approaches, risk assessment approaches, quality assurance approaches, roles involved in threat modeling, tools, and challenges. We then modeled the relationships among these themes.

4 Data analysis

This section describes the themes that we extracted from the eleven interviews.

We used *Pi* to refer to participant *i* in the interview.

[3] oTranscribe: `https://otranscribe.com/`
[4] Otter.ai: `https://otter.ai/`
[5] ATLAS.ti: `https://atlasti.com/`

4.1 Security Properties

Security experts focus on protecting the confidentiality, integrity, and availability (CIA triad) of the data managed by their systems. Table 3 lists the number of participants that discussed each of the security properties. We observe that the participants are concerned about data integrity and availability but not about data confidentiality. They are also concerned about secure modification, availability, consistency, accuracy, and misuses of the data over their life-cycle in their system. For instance, P9 said: *"so things that are important to us are maybe not, as you said, the confidentiality of it if you're talking about a control system, but you're looking at the integrity of the messaging[...], the data is the control message."* The reason is: data is used to process the control commands of the physical components of CPSs. Modification and misuses of these data can cause damages or losses, and unavailability of data and system components could prevent real-time feedback behaviors of certain CPSs and cause losses and damages.

TABLE 3: No. of participants concerned with each of the security properties/-goal.

Security properties	# Participants
Confidentiality	1
Integrity	6
Availability	6

TABLE 4: No. of participants who used known methods for threat modeling.

Method	Ref.	# Participants
Attack tree	[20]	1
DREAD	[21]	1
EVITA or variant of	[22]	2
LINDDUN	[23]	1
PASTA	[24]	1
STRIDE	[13]	6

4.2 Threat Business Impacts

Many CPSs, including connected cars, involve human as users and are safety-critical systems. Security and safety are closely related in these systems [25]. The exploitation of systems' weaknesses and vulnerabilities could have a high impact on the safety of the users. For example, P3 said: *"..the cyber threats can actually impact the physical safety of workers,[...],cause an explosion within a plant or any number of potential outcomes"*. Besides safety, financial losses, and reputation damage are also important aspects that participants consider when performing threat modeling of CPSs. Security weaknesses in the supply chain is a typical example.

4.3 Threat Modeling Approaches

The participants in the study have either control systems or IT background. The participants with control systems background focus on the malicious controllability of the physical components of the studied system as P11 said *"All these methodologies started from this classic [Referring to ISO27005] as an approach with slight modifications. What was added by Evita is the notion of controllability"*. **P1**, for example, uses a field-tested custom engine derived from the ISA/IEC

62443 standard [26] to identify the physical/cyber threats that apply to each of the assets, zones (a group of assets), and conduits of the system under consideration, keeping in mind that a cyber threat can have a physical attack surface ,and **P2** uses the STRIDE taxonomy [13] and analyze the failure scenarios that might apply to the components considering the behavior of the physical components and the safety of the system. In general, these participants combine the use of the known approaches such as STRIDE or PASTA with the analysis of failure modes and criticality of the physical systems.

Participants with IT background apply the classic threat modeling approaches such as STRIDE [13] and DREAD [21]. They identify the assets, the components, and the data managed by the studied system and focus mostly on threats to the integrity, availability, and confidentiality of the data. For example, **P5** approach is: understand the system, identify the weaknesses, identify potential attacks and mitigations, and prioritize the identified threats. They consider that each CPS operates in a specific environment, is associated with specific weaknesses and type of attacks, which justifies the use of threats on data rather than misbehavior of the components of the studied system.

Most of the participants decompose the system being analyzed into components and analyze the threats to each of the components. Participant **P7** deviates from this approach and analyze the studied system as a whole.[6] They look at the weaknesses related to the integration of the components of the given system.

4.4 Threat Identification Methods

Threat identification, a key process in threat modeling, allows identifying the weaknesses of a given system that could cause harm and damage when exploited by attackers. Table 4 provides the frequency of using the common individual threat modeling methods by the participants. The participants use (1) Known methods, such as attack-tree and STRIDE, (2) a combination of known methods, and (3) a combination of security standards and known approaches.
Known method. Several participants reported that they use known methods such STRIDE, PASTA [24], LINDDUN [23], and attack-tree [20]. Most of the participants (6 out of 11) use STRIDE. One expert mentioned that they use the attack-tree method because of its ability to cover all entry points of the attacks. Hence, they can identify all possible threats to the system. Some participants start with a known method and then elaborate further on their threat model based on their experience and knowledge. For example, participant **P2** identify the data flow diagram and the physical locations of the components of the studied system and apply the STRIDE method to identify the initial list of threats.
Combination of known methods and approaches. Some participants reported the use of multiple approaches, such as asset-centric and attacker-centric, in the same project because they believe that each of the approaches and methods gives a different perspective of the system weaknesses and using a set

[6] This approach is similar to the approach used to improve business processes [27].

of methods, although time-consuming, helps to identify the "complete" list of threats to a given system.

Combination of threat modeling standards and known approaches. One Participant, **P1**, uses real-world experience jointly with the ISA/IEC 62443 standard [26] to identify the physical/cyber threats that apply to each of the assets or zones (a group of assets).

4.5 Continuous Threat Modeling Approaches

Developers often modify parts of their CPSs [28] to introduce new features, fix existing defects, or improve the maintainability and the performance of these systems. The evolution of a system often involves changes to its components, which could invalidate the initial threat model since the changes could modify the attack surface and introduce new threats to the system.

Some participants do not have processes and/or experience with managing the evolution of the threat models of their systems. For instance, one participant reported that they do not need to have processes for revising threat models as they are not involved in the businesses of the systems that they perform threat modeling of and another participant reported that they do not review the threat models of their systems even if these systems change. In addition, Participant **P11** reported that the manufacturers of cars cannot do a correct continuous threat modeling. They said *"..you have two updates per year for the cars...the information flow concerning various threats is not so good today because car manufacturers are not aware about all the threats related to the parts coming from their suppliers."*

The rest of the participants (eight from eleven) have processes or approaches to manage continuous threat modeling. For example, Participant **P1** identifies the changes or triggers to a system under consideration and does a thorough threat and vulnerability assessment update, re-assessing the attack surfaces/-sources and the related impacts, and adding new threats and vulnerabilities if necessary; Participant **P5** performs threat modeling as an activity of their adapted scrum [29] process; Participant **P6** uses version control on source code of the software to identify changes and periodically assess in collaboration with the architect the the potential impacts of the changes on the threat model of the given system; Participant **P7** performs a full threat modeling of new systems and partial threat modeling when new components are added to existing systems (only the new components and impacted components are considered the partial threat modeling); Participant **P8** assesses the exploitability of the threats of changed systems and updates the priority of addressing the threats accordingly; and Participant **P9** uses a questionnaire to assess the impacts of the software changes on the previous ranking of the threats to the their system. We note that some participants report that they perform continuous threat modeling only for formality: to pass their systems to the next phase of the DevOps [30].

We observe that most of the participants practice continuous threat modeling, and there is no common continuous threat modeling approach. This

mixed input shows the importance of continuous threat modeling of CPS for the industry and the lack of rigorous and efficient approaches to do so.

4.6 Risk Assessment Approaches

The participants reported the use of several risk analysis and scoring approaches, which we discuss in the following.

Using risk standard and/or regulations. P1 uses risk assessment standards ISA/IEC 62443 [26], which provides guidelines to organize and facilitate a cyber security risk assessment for industrial automation and control systems (IACS) while considering the necessary regulations and sector's security/risk specifics, and Participant **P7** considers the impacts of the threats on the compliance with the regulations that their products must adherent to. For instance, **P7** said *Regulations play a major role in telling [..] the stakeholders what's more important to sustain the [business], right. I mean, basically, the products [could] fail [because of] the regulator, and you could be out of the business."*

Known approach. Many of the participants use common risk assessment approaches, such as FAIR [31] and Bug Bar [32]. The bug bar method, for example, requires assessing the criticality and severity of the threats in collaboration with the customer (which allows considering their concerns) and prioritize the threats based on their severity levels. The FAIR method allows using FAIR data to analyze and highlight the threats of the threat model. For instance, Participant P9 said *" So we use the fair [...] threat modeling to highlight the threats and then run that in fair to actually turn that into a risk."*

In-house risk assessment methods. Three participants have their own risk assessment methods. For instance, Participant **P2** uses a risk register to report the risks of a given system and continuously monitor these risks, and Participants **P8** uses a custom formula to compute the risks of a system using the revenue generated by the system and the criticality of the threats.

4.7 Quality Assurance Approaches

Most of the participants reported that the quality of threat modeling exercises depends on the experience and skills of the experts who perform the threat modeling and the thoroughness of the assessment, including the detailed level of the used architecture and profoundness of the interviews with the stakeholders of the given system. For instance, **P1** said *"the ISA/IEC 62443 standard provides the basic framework but most of the quality of the assessments is based on real-world experience, which also helps with the quality of the specific deviations for every different sector"* and **P11** said "the expert, nothing else."

Few participants use techniques to ensure the quality of their threat models. For instance, Participant **P2** uses peer-evaluation to assess the quality of the threat models that they create. They Said *" There were certain folks that we would do peer reviews [of their] threat models."*. Participant **P3** performs review at each project milestone to ensure the work done at the given milestone is of sufficient quality. They said *"at each of the gates or milestones, you do the proper review to make sure that the work that was done up until that point is of sufficient*

TABLE 5: Roles in the threat modeling processes.

Role	Description
Security team	Initiate the threat modeling process and perform the threat modeling exercise.
Architect	Provide the documentation and artifacts about the system. The security team may interview them to get more details about the system.
Developer	The security team interviews the developers to get more details about the system.
Stakeholder	The security team interviews the other stakeholders of a system as needed to get more details.

quality." And, Participant **P6** uses a set of requirements to verify the coverage of the developed threat model of the important security aspects related to the domain of the given system.

4.8 Roles Involved in Threat Modeling

Table 5 lists the common roles that the participants work with when performing threat modeling. Some of the participants involve the CPS operators, the management staff, the subject matter experts, and the equipment suppliers in their threat modeling exercise as they need. These roles help to gain depth understanding of the system, including the different environments of running the given CPS, the operations of the system, the used equipment, and possibly other aspects. Interviewing different stockholders helps to develop a "complete" threat model.

4.9 Tool

Three participants use Microsoft Threat Modeling Tool [33] although the tool does not cover the physical components of CPSs and three participants use their own tools, including custom templates, for threat modeling. For instance, **P9** said *"Microsoft has a threat modeling tool [...], and there is actually an automotive template that we look at to plug into our system."*

4.10 Challenges

The participants reported few challenges that they face when performing threat modeling of CPSs, which we discuss in the following.

Variety of CPSs. Several of the participants had to work on threat models of CPSs for several applications domains (e.g., mining, transportation, smart grid) and use a variety of physical components that are often not familiar with at the beginning of the projects. They find it impossible to have broad knowledge about threats for CPSs and difficult to generalize expertise across CPSs's application domains.[7] Participants that have IT background find themselves

[7] This different from IT systems that use known architecture styles and follow standard components definitions, e.g., web applications.

with limited knowledge about the physical components: they are not familiar with the threats to the system that they analyze and to the mechanisms that could be utilized to mitigate the threats to these systems. Some participants proposed developing a repository of patterns and mitigation strategies since there are many threat vectors and attack agents to consider.

Limitation of current threat modeling approaches and methods. The existing threat modeling approaches, such as STRIDE and PASTA, focus on computer security. The use of these methods to perform threat modeling for CPSs may produce incomplete threat models because these methods do not cover the physical aspects of CPSs. Some participants suggest the development of a framework that allows identifying common practical attack scenarios based on the application domains of CPSs.

Limitation of tools. Microsoft Threat Modeling Tool is commonly used to generate an initial list of threats to a given system based on a default template that uses the STRIDE taxonomy. It is known that STRIDE focuses on computer security threats; hence it would produce incomplete threat models for CPSs.

Challenge in current culture. Current business culture of "publish now and fix later" has been a challenge for some participants–sometimes only the threats that are related to publicly known attacks are considered. To address this problem, Participant **P4** proposes to have the security experts develop quality threat models that use publicly available threat patterns. They said: *"I think that would be very useful for the industry at large is a set of threat model patterns."*

5 Discussion

This section summarizes the results of the study and discusses the impacts of the study and its limitations.

5.1 Summary

Figure 2 shows the themes extracted from the study and the relationships among these themes. The figure shows that CPSs have security properties requirements and other associated requirements such as safety. The goal of the threat modeling processes and the continuous threat modeling sub-processes is to identify and rank system weaknesses that violate these requirements. The participants use several threat modeling methods and approaches and involve several stakeholders of the CPSs that they perform threat models of using the existing tools such as Microsoft Threat Modeling Tool.

According to the participants, integrity and availability are the security properties the most of concern for CPSs. In addition, many participants use threat modeling method STRIDE, which is unexpected since the method focuses on the threats to IT systems, not CPSs. Also, most of the participants use a combination of known approaches, known methods, and known standards when performing threat modeling of a CPS. We note that the participants associate the quality of threat models mainly to the skills and experience of the security experts who perform the threat modeling. The two techniques that some participants use to ensure the quality of threat models developed by their subordinates are peer-evaluation and the use of the quality checklist.

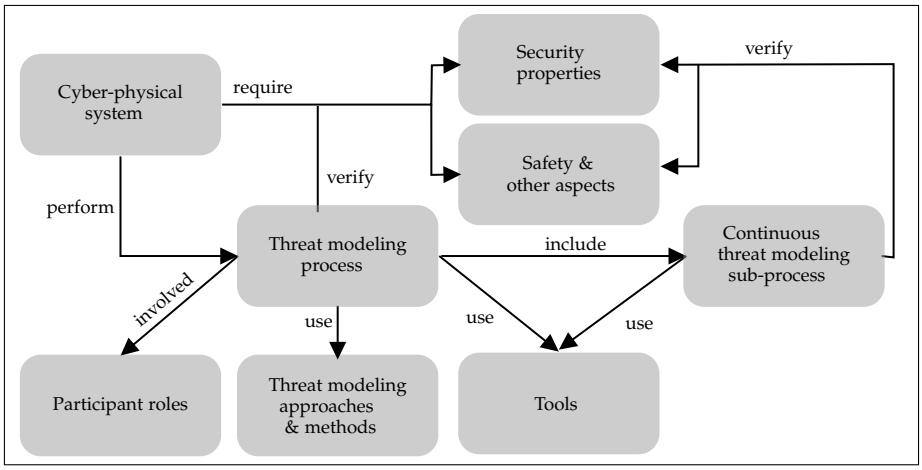

FIG. 2: Entity-relationship model of the threat modeling concepts.

5.2 Impact of the Study

Existing threat taxonomies, such as STRIDE, focus on either the CIA triad or the controllability of the physical components of a system. This study reveals that experts focus on the threats to the integrity, availability, controllability, and safety of the systems threat model a CPSs. The community should develop a knowledge base of practical threats to CPSs that consider the business impacts of failure of physical components, including safety besides the CIA triad.

We found that most of the participants use a combination of known threat modeling approaches, methods, and standards, which makes threat modeling time consuming–it is done two or more times. This calls for developing *practical* new threat modeling approaches that integrate both the IT and OT security needs of CPSs effectively. The method should be generic and flexible to fit the needs and requirements of every CPS domain, and consider the industry standards. Such methods should help security practitioners to produce quality threat models for CPS that could be trusted by the project managers.

We also observed that the participants use their own template to tie the risk to the threats of CPSs. Developing risk assessment methods for CPSs acceptable by the major actors in the industry will help the experts to communicate better and exchange information about risks of CPSs.

In addition, we found that most of the participants do not use quality assurance methods for the threat models that they produce. The managers sometimes request threat models for their CPSs from more than one experts, especially when the system gets hacked. The community should explore techniques and standards for assessing the quality of threat models.

5.3 Threats to Validity

Initially, we gave an open-source of a CPS to some of the selected participants and hoped that they provide us with their threat models, which we could use

to study the practice of threat modeling in depth. The volunteer participants did not want that given, among others, the required important time commitment to do so. Therefore, we opted for exploitative interviews for our research.

The limitations of the study are classified into construct validity, internal validity, conclusion validity, and external validity are discussed as the following [34,35].

Construct validity. To address the validity of the relations between the performed study and the goal of the study, we performed a literature review, designed an interview protocol, and tested it with some experts. We collected information from eleven participants who have different roles and are located in different cities. This gives confidence in the stability of the collected data.

Internal validity. To address the validity of the relationship between the study and its results, we tell the participants at the beginning of the interviews the goals of the interview, which should help in ensuring that the participant and the interviewer share the same goal.

Conclusion validity. To address the validity of the ability to make correct conclusions from the results of the study, the main author provided the second author their codes and the themes for each of the interview, who reviewed them, to reduce the subjectivity of the results.

External validity. To address the validity of the generalization of the study, the eleven participants in the study are selected to be security experts from nine organizations in different businesses. We believe the diverse experience of the participants supports generalizing the results.

6 Conclusion

This paper reports about the practice of threat modeling of CPSs. We conclude that (1) ensuring the integrity and availability of data and system's components in addition to controllability and safety of CPSs is the concern of threat modeling of CPSs, (2) there are differences between experts with a background in control system and experts with a background in IT regarding the approaches to perform threat modeling, (3) the experts use a combination of known approaches, methods, and standards to perform threat modeling of a given CPS, (4) most of the threat modeling participants perform continuous threat modeling, (5) the experts often use custom risk scoring methods, (6) most of the participants do not use quality assurance techniques for the threat models that they produce and rely on the experience and skills of the expert who performs the threat model, and (7) four roles are commonly involved in threat modeling, namely security team, architect, developer, and stakeholder.

The studies highlighters several future research directions to improve the practice of threat modeling of CPS. First, we need to develop a new threat modeling approach that flexible to fit the different CPSs domains, and supports for easy integration of industry standards. Second, we need to develop a threat knowledge-base that accounts for the different CPSs domains and links the threats to the target surfaces, attack means, countermeasures, and impacts. Lastly, we need to develop techniques for semi-automated threat modeling of CPSs will help experts to do incremental and effective threat models.

Acknowledgment

The author thank Simone Curzi from Microsoft, Zafar Ali from John Deere, Rohini Narasipur from Bosch, Arun Prabhakar from Security Compass, and Youssef Jad from PM SCADA Cyber Defense for participating in the study and reviewing this paper. The authors thank also the other anonymous participants in the study for their contributions. The participants were not representing their respective employers in the study.

References

1. "Definition of threat modeling." `https://pascal.computer.org/`.
2. A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014.
3. W. Xiong and R. Lagerström, "Threat modeling – a systematic literature review," *Computers & Security*, vol. 84, pp. 53 – 69, 2019.
4. R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212 – 223, 2018.
5. T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, "Towards a framework for assuring cyber physical system security," *International journal of security and its applications*, vol. 9, pp. 25–40, 2015.
6. M. Pakizeh, "Threat identifying cyber physical systems security," *International Journal of Electrical and Power Engineering*, vol. 13, pp. 5–11, 12 2019.
7. W. Klaudel and A. Rataj, "Towards a Formalisation of Expert's Knowledge for an Automatic Construction of a Vulnerability Model of a Cyberphysical System," in *ICISSP 2021 - 7th International Conference on Information Systems Security and Privacy*, (Vienne, Austria), Feb. 2021.
8. L. ben Othmane, A. Al-Fuqaha, E. ben Hamida, and M. van den Brand, "Towards extended safety in connected vehicles," in *16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013)*, pp. 652–657, 2013.
9. G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia* (M.-A. Cardin, D. Krob, P. C. Lui, Y. H. Tan, and K. Wood, eds.), (Cham), pp. 41–53, Springer International Publishing, 2015.
10. P. Dong, Y. Han, X. Guo, and F. Xie, "A systematic review of studies on cyber physical system security," *International Journal of Security and its Applications*, vol. 9, pp. 155–164, 01 2015.
11. E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: Volume 1, overview." `https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview`, Nov 2018.
12. G. Martins, S. Bhatia, X. Koutsoukos, K. Stouffer, C. Tang, and R. Candell, "Towards a systematic threat modeling approach for cyber-physical systems," *2015 Resilience Week (RWS)*, pp. 1–6, 2015.
13. R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Stride-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pp. 1–6, 2017.
14. V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in iot systems," *Internet of Things*, vol. 7, p. 100056, 2019.

15. D. Meyer, J. Haase, M. Eckert, and B. Klauer, "A threat-model for building and home automation," in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, pp. 860–866, 2016.
16. H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model," *Information Systems*, vol. 53, pp. 147 – 160, 2015.
17. J. Saldana, *The coding manual for qualitative researchers*. Sage Publications, 2015.
18. V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, p. 77–101, 2006.
19. L. M. Connelly, "What is phenomenology?," *MedSurg Nursing*, vol. 19, no. 2, p. 127–129, 2010.
20. V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *Journal of Computing Sciences in Colleges*, vol. 23, 04 2008.
21. D. Marshall and D. Coulter, "Threat modeling for drivers." `https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers`, June 2018.
22. A. Ruddle, B. Weyl, S. Idrees, Y. Roudier, T. L. Michael Friedewald and, A. Fuchs, S. Gürgens, O. Henniger, R. Rieke, M. Ritscher, H. Broberg, L. Apvrille, R. Pacalet, and G. Pedroza, "Deliverable d2.3: Security requirements for automotive on-board networks based on dark-side scenarios." `https://www.evita-project.org/deliverables.html`, December 2009.
23. "Home." `https://www.linddun.org/`.
24. T. UcedaVelez and M. M. Marona, *Intro to PASTA*. John Wiley & Sons, Inc., 2015.
25. G. abaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia*, pp. 41–53, Springer International Publishing, 2015.
26. "Isa/iec 62443 cybersecurity certificate programs- isa." `https://www.isa.org/training-and-certification/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs`, journal=isa.org.
27. E. Goldratt, *The goal: a process of ongoing improvement*. North River Press, 2004.
28. A. T. T. Ying, G. C. Murphy, R. Ng, and M. C. Chu-Carroll, "Predicting source code changes by mining change history," *IEEE Transactions on Software Engineering*, vol. 30, pp. 574–586, Sep. 2004.
29. H. Takeuchi and I. Nonaka, "The new new product development game," *Harvard Business Review*, vol. 64, Jan-Feb 1986.
30. V. Mohan and L. ben Othmane, "Secdevops: Is it a marketing buzzword? - mapping research on security in devops," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, (Salzburg, Austria), pp. 542–547, 2016.
31. F. Institute, "The importance and effectiveness of cyber risk quantification." `https://www.fairinstitute.org/what-is-fair`.
32. S. Curzi, "Bug bars and stride-based calibration." `https://simoneonsecurity.com/2020/02/20/bug-bars-and-stride-based-calibration/`, Feb. 2020.
33. Jegeib, "Microsoft threat modeling tool overview - azure." `https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool`.
34. D. S. Cruzes and L. ben Othmane, *Empirical Research for Software Security: Foundations and Experience*, ch. Threats to Validity in Software Security Empirical Research, p. 275–300. Taylor & Francis Group, LLC, 2017.
35. C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering: An Introduction*. Norwell, MA, USA: Kluwer Academic Publishers, 2000.