Cyberattacks: Modeling, Analysis, and Mitigation

Sara Abbaspour Asadollah
School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden
sara.abbaspour@mdu.se

***Abstract*—Industrial cybersecurity has risen as an important topic of research nowadays. The heavy connectivity by the Internet of Things (IoT) and the growth of cyberattacks against industrial assets cause this risen and attract attention to the cybersecurity field. While fostering current software applications and use-cases, the ubiquitous access to the Internet has also exposed operational technologies to new and challenging security threats that need to be addressed. As the number of attacks increases, their visibility decreases. An attack can modify the Cyber-Physical Systems (CPSs) quality to avoid proper quality assessment. They can disrupt the system design process and adversely affect a product's design purpose.**

This working progress paper presents our approach to modeling, analyzing, and mitigating cyberattacks in CPS. We model the normal behavior of the application as well as cyberattacks with the help of Microsoft Security Development Lifecycle (SDL) and threat modeling approach (STRIDE). Then verify the application and attacks model using a model checking tool and propose mitigation strategies to decrease the risk of vulnerabilities. The results can be used to improve the system design to overcome the vulnerabilities.

***Index Terms*—Cyber-Physical Systems (CPSs), Cyberattacks, Formal verification, Cybersecurity, Model checking, STRIDE, SDL.**

I. Introduction

Cybersecurity is concerning as one of the highest priority targets on the global policy and national security plans with increasingly challenging policy field for governments and large companies. Threats and attacks have evolved over the past twenty years, and cybersecurity is now one of the top five humanitarian threats, according to the Global Threat Report [1]. The report shows that the impact of cyberattacks on critical infrastructure has increased in 2021, while cyberattacks have become critical in areas such as Industrials and Engineering, Manufacturing, and Cloud Environments.

We believe that cybersecurity is not only belonged to a single country, industry, or disciplinary field due to the nature and amount of an increasingly connected and sophisticated technological and user base. As reported by X-Force Threat Intelligence Index [2], more than 8.5 billion records were jeopardized by attackers in 2019, while this number is more than 200% (three times) greater than the recorded number in 2018. X-Force expects that the attacks on Industrial Control Systems (ICS) will continue to increase in 2022 and beyond. We need to prepare our organization and industrial companies for resilience against cyberattacks by encouraging the response team within the organizations to better understand threat actors and to find proper strategies for prioritizing cybersecurity resources. Runtime verification and stress tests also would be another option for resilience against cyberattacks by improving reaction time, reducing downtime, and ultimately saving money in the case of an attack. According to X-force, in 2020 credential theft or re-use was one of the most commonly observed attack methods used by threat actors, so we need proper approaches to effectively inhibit this attack before it takes hold. We believe that with cybersecurity attacks, the world is facing increasingly multiple challenges in different domains with complex and new behavior that require scientific solutions to apply changes and verify them across the entire cyber-physical systems. This proposal is an attempt to propose reliable and scientific solutions in the field of CPSs cybersecurity.

The types of attacks have changed since the late-1980s and they can be categorized into five generations: ***Generation 1***, 1980s PCs were the main subject for standalone attacks, and the Anti Virus was developed to mitigate. ***Generation 2***, in the mid-1990s, attacks from the Internet were initiated and firewalls were invented to prevent them. ***Generation 3***, in the early-2000s, vulnerabilities in applications were targeted so IPS and IDS were introduced. ***Generation 4***, in 2010 polymorphic contents have been developed to change the profile of attacks by which a bad actor could act as a legitimate one. This has been the start of complex attacks which is constantly developing ever since. To mitigate these types of attacks behavioral analysis has been a major part of the protection process by which experts try to predict attackers' moves and actions. ***Generation 5***, in the last five years, types of attacks and their complexity have been transformed profoundly and by introducing mobile devices, cloud services, and multi-vectors networks, then attackers have targeted governments and commercial entities through complex activities.

In fact, the types and volume of attacks have massively increased and companies should be very vigilant to prevent any breach in their environment. According to the reports, only less than three percent of companies have managed to get protected. Their protections have been successful in response to the 3rd generation of attacks and surprisingly

This work was supported by the Swedish Foundation for Strategic Research through the Serendipity project and the Knowledge Foundation through the SACSys project.

malicious actors are still active due to the world's negligence. This situation requires us to move from the 3rd generation of protection to the 5th one by which not only the 4th generation is covered (human behavioral analysis), but also the complexity of attacks will be molded and analyzed. This way may put us one step ahead of attackers.

We believe that with cyberattacks, the world is increasingly facing multiple challenges in different domains with complex and new behavior that require scientific solutions to apply changes and verify them across the entire CPSs. To tackle the CPSs' attacks, it is required to consider an approach customized for the CPSs which includes verification and optimization during the design to ensure that the application satisfies its security requirements. Such evolution is modeled and verified before being deployed into the executing phase at design time.

In this working progress paper, we present our planned approach to model, analyze, and mitigate cyberattacks in CPSs. In order to perform this study first, we will use the actor-based language with model checking support to model and formally verify the normal behavior of all components of CPSs. Then we will model cyberattack by using the SDL and threat model approach (STRIDE) results. After that, we will integrate the attack models and the model of the normal behavior of the system. We will analyze how potential attacks can lead the system to any security violations. Finally, we will propose mitigation strategies to remove potential attacks or reduce their effects.

II. Proposed Approach

A. The Study Core Question

Cyber-Physical Systems are complex engineering systems designed to integrate physical, computation, and communication components. CPS includes three kinds of components i.e., controllers, sensors, and actuators. Sensors are responsible for gathering the data on the state of a physical process and submitting them to the controllers [3]. The operation of this type of system requires to be controlled, coordinated, monitored, and integrated by a computing and communication core that is integrated with the physical environment. The dynamic and possibly unpredictable environments, uncertain operating conditions, and connection to the Internet call for new paradigms of software design, and runtime adaptation mechanisms in terms of security.

The main application areas need to interact and possibly collaborate with humans in a secure environment to avoid accidents or collisions, and prevent undesirable changes that may harm humans and/or machines. Some of the primary questions that crossed the mind in dealing with cybersecurity are how does the nature of cyber threats and emerging trends and challenges affect the cybersecurity in our system, and how can we measure these malicious cyber activities using scientific methods? In addition, another question would be what kind of scientific and academic theories can be used to describe and decrease malicious cyber activities and improve the environment to decline the possibilities for various types of malicious cyber activities and increase scrutiny? Thus, proposing reliable strategies, techniques, and operational practices are required to define and mitigate malicious cyber activities and improve the environment to decrease the possibilities for the different types of malicious cyber activities.

In general, the core question for this study is:

How to ensure cybersecurity for cyber-physical systems at design time?

As we mentioned, the main goal of this study is to **investigate and analyze the cyberattacks at design time and propose efficient solutions to decrease or remove the risks**. This will enable the development of applications that by design exhibits high security, reliability, availability, and integrity.

We will focus on design time verification and validation of security requirements that are assumed to change when the attacker(s) causes violation(s) in the system. We will use requirement engineering and threat analysis techniques to capture the specific properties related to the security and provide an assurance case guaranteeing that the system is sufficiently secure. We will build normal behavioral models to analyze and check the requirements at design time.

To tackle the cyberattacks, it is required to consider the security of CPS beyond the IT system's standard information security. The central element in providing a scientific answer to the core research question is provided by the architecture customized for the CPS which includes verification and optimization during the design to ensure that the system satisfies its security requirements. Such evolution is modeled and verified before being deployed into the executing system at design time. The main innovation here is the consistent and integrated actor-based framework matching the characteristics of distribution, asynchrony, and dynamic changes of the system, which makes the approach unique and highly effective and efficient. We further propose mitigation solutions to reduce risks after detecting the attacks at design time.

Common cyberattacks are defined differently depending on the target application domain. The mitigation also depends on the environmental setup. However, the faults considered so far have been benign, caused by human errors or the environment. The main reason for this is that either existing CPSs have traditionally been isolated or they are supposed to operate in a confined area and are not connected externally such as subsystems within a car or specific device, and a system-of-systems in a factory.

Attack scenario. The main results of our approach will be evaluated on CPSs. An automated train control system is a type of CPSs contains a controller module for sending control commands to the train modules, a variety of sensors such as a speed sensor, some actuators like the train brake, and physical processes such as increasing/decreasing the train speed.

As it is shown in Figure 1, we have a scenario in which the speed sensor regularly senses the speed and send the value to the controller module. If the speed is more than S km/h,

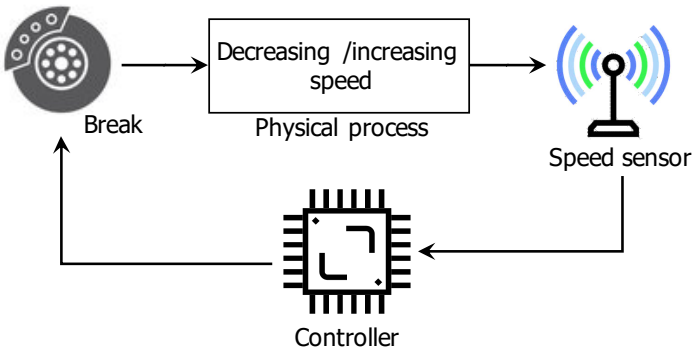

Fig. 1. A cyberattack scenario.

the controller must send the command to brake and decrease the speed or stop the train. In this scenario, if the brake does not actuate with a reasonable delay, the sensor does not send the actual speed of the train, or the controller does not send the accurate command to the brake then the train and all passengers will be in critical situations. Such a scenario could intentionally be done by an attacker while it highlights the importance of security to predict, detect and mitigate the possible attacks within a reasonable time.

We believe that the proposed approach is able to support the security and the availability as well as confidentiality and integrity of data assets and systems info. The main goal of the study is divided into the following sub-goals that answer the core research question:

- Identification of common assets, vulnerabilities, and threads for CPSs operating in open environments. Implementation of solutions and countermeasures, taking into account the requirements on timeliness and continuity of service.
- Developing compositional analysis methods and tools to address confidentiality through formal verification. The techniques consider a modeling approach that focuses on assets, threats, vulnerabilities and attacks that can capture the heterogeneity and openness of the system.

B. Approach Description and Breakdown Structure

This study is dedicated to defining a system design and analysis techniques that will allow CPSs to adapt without jeopardizing the security guarantees. To tackle the scientific challenges, we divide our approach into two phases as shown in Figure 2. Phases1 is considered for defining the needs for Phase2 and Phase2 is considered the main technical phase.

Phase1-Preparation is considered for establishing the state-of-the-art study and investigating needs, assets, and security requirements for CPSs. In this phase, we study and identify the state-of-the-art with the aim of cybersecurity guarantee in the CPSs field to classify various techniques and tools to evaluate different kinds of cyberattacks and to establish the state-of-the-art in this area for CPSs. Also, we identify the needs and requirements of cybersecurity considering the system environment, assets, and data to investigate how modeling the attack can be effective in different industrial domains. The expected result in this phase is preparation for the study and by eliciting required information for Phase2.

Phase2-Security analysis is considered for developing the analysis methods that are able to manage unexpected and unpredicted events due to sabotage by cyberattacks. We will propose methods to extract attack profiles and create attack models in the security domain based on the reference guidelines, e.g., STRIDE threat model considering the assets of the system. We also will implement an automated mapping tool to build normal behavioral models from sequence diagrams or Data-flow diagrams (DFD, from STRIDE approach). We develop methods for detecting different and dynamic attack patterns as well as building a tool for extracting attack patterns from the model checking results which are recorded in log files and to be used as the reference database. In this phase, we will build a tool for proposing suitable mitigation strategies based on the model checking results and the environmental policies to remove potential attacks or reduce their effects.

III. Related Work

To the best of our knowledge, recently several studies have been proposed to model and simulate the security of CPSs. Wasicek et al. [12] propose an aspect-oriented technique to model attacks against CPSs. They illustrate how Ptolemy [4] can be used to simulate the behavior of system components and detect anomalies. Taormina et al. [11] propose another simulation-based approach that is implemented in a MATLAB toolbox to analyze the risk of cyber-physical attacks on water distribution systems. Pedroza et al. present a UML-based method [9] for modeling and analysis of security and safety. However, this method focuses on the identification of security risks that can cause the failure of safety-critical components and does not support modeling and finding mitigation for cyberattacks. In [8] and [7], the authors rely on simulation to perform their analyses. They propose a new metric to quantify the impact of attacks on components of the target CPSs. This metric can be used to perform a cost-benefit analysis on security investments.

Furthermore, there are several formal methods examine CPSs security. In [6], Kang et al. use Alloy to model Secure Water Treatment (SWaT) behavior and potential attackers. They can discover the undetected attacks which cause safety failure (e.g., water tank overflow). The study is considered as run time monitoring, which compares the actual invariant of the SWaT system and output state in the Alloy model checker during system operation. Important attack scenarios are identified using this approach, and each run of the analysis considers only one point of the system to attack. In our study, we can analyze and detect scenarios with several threats exploiting the communication and components vulnerabilities. Rocchetto and Tippenhauer [10] present another formal method for discovering feasible attack scenarios on SWaT. ASLan++ is

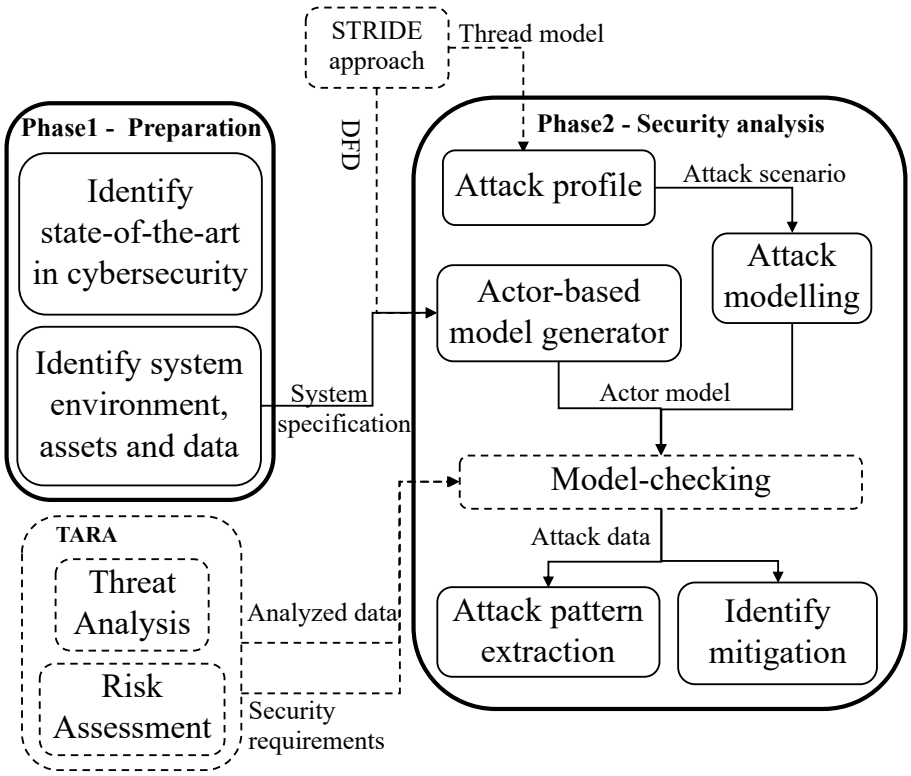

Fig. 2. Overview of our proposed approach and its breakdown structure.

the formal language used for modeling the physical layer interactions and CL-AtSe is a tool used to analyze the state space of the model and discover the potential attack scenarios. As the result, they succeed to find eight attack scenarios. They provide support for modeling different attacker profiles and only one profile can be active at each moment while in this study, we plan to do a realistic situation by having multiple threat scenarios active simultaneously. Fritz and Zhang [5] consider CPSs as discrete-event systems and model them using a variant of Petri nets. They propose a method based on permutation matrices to detect deception attacks. In particular, they can detect attacks by changing the input and output system's behavior and analyzing the attacks' impact on the system's behavior. Covert attacks and replay attacks are two kinds of attacks modeled and analyzed in their research and the combination of attacks is not considered. In this study, we will investigate and analyze the combination of covert and replay attacks.

IV. Conclusion and Future work

In this paper, we introduced an approach for modeling and analyzing the cyberattacks, as well as for finding reasonable mitigation to remove/decrease the risk of potential cyberattacks at design time. The proposed approach provides a systematic way to address and tackle such cyberattacks, which the CPSs are dealing with recently. In our proposed approach first, we use the result of SDL and STRIDE thread modeling method as input. Then we model the system by investigating the normal behavior of our system and combining it with the cyberattack model(s). Following, we simulate and verify the combined models with the cybersecurity properties using a model checking tool. After analyzing the behavior of the system while cyberattacks inject into the model, we identify and propose mitigation to tackle attacks and reduce their effect.

In future work, we plan to implement our approach and tools as well as apply the approach and use the tools on case studies in various domains in order to evaluate our approach and improve it in an iterative and incremental manner. Additionally, we plan to suggest countermeasures and/or security mechanisms according to the derived security level to fulfill the derived security requirements. As well as to establish relationship between threats and cyberattacks. Finally, we plan to provide practical guidance on how to implement penetration testing.

Acknowledgment

This work was supported by the Swedish Foundation for Strategic Research through the Serendipity project and the Knowledge Foundation through the SACSys project.

References

[1] The crowdstrike 2022 global threat report, 2022.
[2] IBM X-Force Threat Intelligence Index 2020. Library Catalog: www.ibm.com.
[3] Sara Abbaspour Asadollah, Rafia Inam, and Hans Hansson. A survey on testing for cyber physical system. In *IFIP International Conference on Testing Software and Systems*, pages 194–207. Springer, 2015.

[4] Joseph Buck, Soonhoi Ha, Edward A Lee, and David G Messerschmitt. Ptolemy: A framework for simulating and prototyping heterogeneous systems. In *Readings in hardware/software co-design*, pages 527–543. 2001.

[5] Raphael Fritz and Ping Zhang. Modeling and detection of cyber attacks on discrete event systems. *IFAC-PapersOnLine*, 51(7):285–290, 2018.

[6] Eunsuk Kang, Sridhar Adepu, Daniel Jackson, and Aditya P Mathur. Model-based security analysis of a water treatment system. In *Proceedings of Software Engineering for Smart Cyber-Physical Systems*, pages 22–28. ACM, 2016.

[7] Ruggero Lanotte, Massimo Merro, Andrei Munteanu, and Luca Viganò. A formal approach to physics-based attacks in cyber-physical systems. *ACM Transactions on Privacy and Security (TOPS)*, 23(1):1–41, 2020.

[8] Ruggero Lanotte, Massimo Merro, Riccardo Muradore, and Luca Viganò. A formal approach to cyber-physical attacks. In *IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 436–450. IEEE, 2017.

[9] Gabriel Pedroza and Guillaume Mockly. Method and framework for security risks analysis guided by safety criteria. In *Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings*, pages 1–8, 2020.

[10] Marco Rocchetto and Nils Ole Tippenhauer. Towards formal security analysis of industrial control systems. In *ACM Asia Conference on Computer and Communications Security*, pages 114–126. ACM, 2017.

[11] Riccardo Taormina, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, and Avi Ostfeld. Characterizing cyber-physical attacks on water distribution systems. *Journal of Water Resources Planning and Management*, 2017.

[12] Armin Wasicek, Patricia Derler, and Edward A Lee. Aspect-oriented modeling of attacks in automotive cyber-physical systems. In *ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014.