Modeling and Simulation of Cyberattacks for Resilient Cyber-Physical Systems*

Nafiuul Rashid¹, Jiang Wan¹, Gustavo Quirós², Arquimedes Canedo², and Mohammad Abdullah Al Faruque¹

Abstract— Securing cyber-physical systems (CPS) is an active area of research. For example, manufacturing and military CPS have been traditionally designed without an emphasis on cybersecurity. This paper presents a model-based secure-by-design approach for modeling and simulating the cybersecurity aspects of CPS. We demonstrate our systematic approach by modeling several classes of cyberattacks that may affect the normal operations of CPS, and evaluate the impact of these attacks on the system through the use of simulation. We follow a functional modeling approach that may reduce the engineering effort and increase the quality of the developed system, while also increasing the resilience of the system when exposed to cyberattacks.

I. INTRODUCTION

In state-of-the-art CPS (e.g., automated production, power generation and distribution, intelligent transportation, military vessels, smart buildings), the focus lies on the functionality of the system and on non-functional aspects such as reliability, efficiency, safety, and usability. Most of the prior research and development effort has been focused on coping with system complexity and in operation under harsh operational environments. The cybersecurity aspect is not commonly considered, as the human portion of the environment is assumed to be mostly cooperative with the system. This may be the reason why early CPS were — and many still are — particularly vulnerable to cyberattacks. However, after the occurrence of recent attacks on the cybersecurity and integrity in production systems [1], [2], [3], [4] and in critical infrastructure [5], the aspect of cybersecurity is becoming more important at design time. Military IT systems have also been targeted by cyberattacks [6], and the risk of a cyberattack on military infrastructure is increasing considerably [7]. Also, existing methods for securing embedded systems have proven not to be completely effective in the domain of CPS [8]. As a consequence, these problems are attracting more researchers to investigate the topic of cybersecurity for CPS more closely [9], [10], [11], [12], [13], [14]. Although the goals of reliability and cybersecurity are related, there is an important difference between them. Low probability risks are neglected by reliability models because their occurrence is too unlikely to justify the additional overhead that is needed to address these risks. On the other hand, even low probability risks need to be considered by cybersecurity models, because intelligent attackers may and will exploit any known vulnerability. Therefore, cybersecurity models should explicitly consider any weakness that the system may expose.

Today, it is estimated that a wide range of CPS are exposed and vulnerable to cyberattacks [9], [17]. Even when these systems comply with the general cybersecurity requirements for IT systems, the close interaction with the physical environment may potentially open new opportunities for attackers targeting CPS. These may be, for example, acoustic side-channel attacks on additive manufacturing systems [15] or the control signals in an automated production system or the sensors in a military vessel. In the case of manufacturing, the increasingly important requirements of flexible and efficient production drive the development of smart manufacturing systems — with added levels of complexity [16]. In this scenario, reliability and cybersecurity become an even bigger challenge than before. Smart manufacturing requires high levels of connectivity and open communication between hardware devices and between software components, and this may potentially introduce new cybersecurity holes and vulnerabilities in the system.

In recent years, there has been a growing use of model-based design approaches for complex CPS, e.g., in the automotive systems [17], [18]. This paper shows that smart manufacturing systems may also benefit from this approach, as a way to cope with the added complexity. Following a model-based approach may reduce the engineering effort and increase the quality of the developed system [19]. Additionally, it may also increase the resilience of the system when exposed to cyberattacks, as presented in [20].

In this paper, we present an approach for modeling and simulating the cybersecurity aspect of CPS in order to integrate this design requirement into the model-based development process. To demonstrate our approach, we model several classes of cyberattacks that may affect the normal operation of the CPS, thereby extending the original set of attack classes published in [20]. We also evaluate the impact of these attacks on the system through the use of simulation. For our studies, we consider a controlled cooling...
system as a relevant use case in many different contexts such as smart manufacturing, building automation, and military infrastructure.

This paper is structured as follows: Section II summarizes the novel contributions of this paper; Section III gives an overview of the security-aware functional modeling and its advantages in the development of secure-by-design CPS; Section IV presents the details of our extended attack model; Section V illustrates the use of the attack model by considering an engine cooling system as a use case; Section VI presents the experimental results of our simulation; and Section VII summarizes the paper and its key findings.

II. OUR NOVEL CONTRIBUTIONS

The novel contributions of this paper are the following:

1) We extend the attack models presented in [20] with a new kind of attack that manipulates the control parameters of the attacked system.

2) We introduce the concept of coordinated attack models as a way to target robust systems (i.e., those having redundant components) more effectively.

3) Using an engine cooling system control system as a use-case, we demonstrate the impact of the attack models in the system.

III. SECURITY-AWARE FUNCTIONAL MODELING

Functional modeling is a design methodology used during the concept design phase of the CPS development process. A functional model [19] defines what the system does in terms of energy, material, and signal flows. Functional models provide a high-level abstraction that may be used to perform a broad design space exploration of various concepts and narrow the design space to those designs that do satisfy the requirements. The high level of abstraction in functional models makes them a suitable formalism for CPS design. Functional models naturally express cyber-physical processes by hiding details about the continuous and discrete dynamics, and naturally allow collaboration across domains [19]. As presented in [20], existing functional models naturally “leak” information that may be used to attack the system via the signal flows in the cyber domain or energy/material flows in the physical domain. The security-aware functional modeling extends the functional modeling concept by including cybersecurity functions. The security-aware functional models provide a means to analyze the effect of cybersecurity attack functions on the system through a system-level simulation, and to refine the system’s design using cybersecurity countermeasure functions. Since the detailed design models may be directly translated to executable production code, this methodology represents a systematic approach for developing secure-by-design CPS [8].

IV. EXTENDED ATTACK MODEL

To demonstrate the modeling of cybersecurity vulnerabilities of CPS, we start by evaluating the different attack models as presented in [20]. Then, we extend the attack model to incorporate our newly proposed control parameter attack. Finally, we introduce the idea of coordinated attacks that may effectively target more robust CPS, which we will describe in Section IV-C. Thus, our newly proposed extended attack model shows how state-of-the-art CPS may be compromised by various levels of cyberattacks. All the attacks were implemented as MATLAB/Simulink functional blocks.

A. Basic Attack Models

In order to evaluate the various attack models presented in [20], we formulate the following attacks, where $u_s$ is the original signal/flow and $v_s$ is the attacked signal/flow. We assume that an attacker may employ physical techniques in order to disrupt these signals/flows, for instance by using high-energy radiation or electromagnetic beams directed to the system’s sensors or communication devices. In all cases, the attack happens during the attack period $[\tau_{\text{start}}, \tau_{\text{end}}]$.

- **Fuzzy attack model:**
  \[
  \text{Event} = f_{\text{clock}, \text{Pois}}(\lambda) \\
  \text{atk}_s = \begin{cases} 
  \text{unif}(\text{atk}_{\text{upper}}, \text{atk}_{\text{lower}}) & \text{Event} \neq 0 \\
  \text{atk}_s & \text{Event} = 0
  \end{cases}
  \]
  \[v_s = u_s + \text{atk}_s\]  \hspace{1cm} (1)

  The fuzzy attack model adds a random distribution (e.g., uniform distribution $\text{unif}(\text{atk}_{\text{upper}}, \text{atk}_{\text{lower}})$) triggered by the Poisson clock $f_{\text{clock}, \text{Pois}}(\lambda)$ to distort the original signal/flow and to destabilize the system.

- **Interruption attack model:**
  \[
  v_s = \begin{cases} 
  0 & \tau_{\text{start}} < \tau < \tau_{\text{end}} \\
  u_s & \text{else}
  \end{cases}
  \]  \hspace{1cm} (2)

  The interruption attack model, also called denial-of-service attack, stops the signal/flow during the attack period.

- **Man-in-the-middle (MIM) attack model:**
  \[
  v_s = \begin{cases} 
  u_m & \tau_{\text{start}} < \tau < \tau_{\text{end}} \\
  u_s & \text{else}
  \end{cases}
  \]  \hspace{1cm} (3)

  The man-in-the-middle attack model mimics the human attack behavior. When the attack happens, the signal/flow is changed to the manipulated signal/flow controlled by the attacker. Here, $u_m$ is the manipulated signal controlled by the attacker.

- **Overflow attack model:**
  \[
  v_s = \begin{cases} 
  u_s >> \text{Num}_{\text{bits}} << \text{Num}_{\text{bits}} & \tau_{\text{start}} < \tau < \tau_{\text{end}} \\
  u_s & \text{else}
  \end{cases}
  \]  \hspace{1cm} (4)

  The overflow attack extends the number of bits of a message in a digital signal in order to overflow the...
buffer on the receiver’s side.

- Down-sampling attack model:

\[ u_{low} = \begin{cases} u_s & \tau \text{ mod rate}_{down} = 0 \\ u_{low} & \text{else} \end{cases} \]

\[ v_s = u_{low} \]  

The down-sampling attack model reduces the sampling rate of the signal/flow. When attacked in this manner, the quality of control that the attacked system provides may be significantly reduced.

B. Control Parameter Attack

Another way to directly attack the system is to modify the vulnerable control parameters. An attacker may employ cyber techniques in order to gain access to the control system and modify control parameters to arbitrary values, thereby inducing an incorrect operation of the control system. In this paper, we do not consider the details of the cybersecurity break-in to the system (e.g., via privilege escalation, code injection, etc.). We will assume that an attacker has already managed to break into the system and is able to modify the control parameters directly. Hence, we propose a new attack called control parameter attack that allows the attackers to destabilize the system by replacing control parameters.

\[ v_{par} = \begin{cases} atk_{par} & \tau_{start} < \tau < \tau_{end} \\ u_{par} & \text{else} \end{cases} \]

Here, \( u_{par} \) and \( v_{par} \) are the original and the modified parameters, respectively. Moreover, \( atk_{par} \) represents the modified parameter value. The control parameter attack model will replace the vulnerable control parameters by the attacker’s parameters. As discussed earlier, this allows the attacker to change the quality of the control that the system can provide.

C. Coordinated Attack

The attack models discussed so far provide a basic mechanism to attack any CPS. However, many CPS are equipped with redundant components that allow the system to continue operation when individual component-level service interruptions occur, e.g., due to hardware faults or external attacks, thus making the systems more robust. Sometimes it becomes difficult to destabilize these robust systems using basic attack models. However, a well-planned coordinated attack comprising the basic attack models may effectively compromise the system. To this end, we introduce the idea of coordinated attacks targeting robust systems. Since a large number of combinations of simple attacks are possible, here we show two models of coordinated attacks as examples, where each coordinated attack combines a basic attack model on a control signal with a control parameter attack:

\[ v_s, v_{par} = \begin{cases} u_s >> \text{Num}_pits << \text{Num}_pits, & \tau_{start} < \tau < \tau_{end} \\ atk_{par}, u_{par} & \text{else} \end{cases} \]

Equation 7 shows a combination of a man-in-the-middle attack model coordinated with a control parameter attack. Furthermore, equation 8 shows the combination of overflow and control parameter attacks.

V. ENGINE COOLING SYSTEM USE CASE

For the evaluation of the attack models, we present the model of an engine cooling system as a use case. The use case exemplifies a class of systems that are relevant for a wide range of applications of CPS, where the incorrect operation of the cooling system may cause serious damage to the system components that require cooling, damage to products, and a general breakdown of the system. As an example, Figure 1 shows a production step in the manufacturing of large motors, where cooling water is applied to a milling rotary axis. Cooling systems are also an integral part of the chemical process plants dealing with exothermic processes, as well as of thermoelectric power plants such as coal, nuclear, natural gas, or oil. In the case of military critical infrastructure, the ship chilled water distribution system presented in [21] is a cooling system that is part of the fluid and electrical system of a Navy ship. Its purpose is to provide cold water from coolers to different ship components (heat loads) in order to regulate their temperature and to maintain it within suitable operating conditions.

![Fig. 1: Cooling of Large Motor Manufacturing](image)

The engine cooling system considered in this paper is a modified version of the model provided in [22]. It consists
of all the basic components of a standard cooling system like pump, hose, bypass hose, engine, thermostat, radiator, and shaft controller. Figure 2 shows the general outlook of our engine cooling system which is implemented in MATLAB/Simulink.

VI. EXPERIMENTAL RESULTS

As introduced in Section V, we consider engine cooling system as a use case for the experimental evaluation of the different attack models. Figures 3a and 3b show the results of the system without instantiating any attack models. The figures show the role of the thermostat in the engine cooling system. The piston temperature climbs steadily until the thermostat opens. At that point, the flow of coolant through the radiator climbs sharply whereas the coolant flow through the bypass hose decreases. After that, the piston temperature rises more slowly as coolant passing through the radiator releases heat to the atmosphere.

For the realistic evaluation of the attack models, we have inserted the attacks between the engine and the thermostat, as thermostat opens based on the coolant temperature once it passes through the engine. The star marked zones in Figure 2 show the places where attacks are inserted. The red star represents the basic attacks whereas the blue stars represent the control parameter attacks. Coordinated attacks are made as combinations of different basic attacks and/or control parameter attacks. For each of the attacks we have run the simulation for 300 seconds and except for the fuzzy attack, all the attacks have been inserted from 100 to 200 seconds.

The basic attacks cause the thermostat to read the incorrect fluid temperature from the control signal. Eventually, system components like the engine exceed their normal operational temperature and behave abnormally. Figure 3c shows how fuzzy attack causes the piston temperature to go beyond the maximum 373 K and reach around 410 K. Here, the maximum temperature is considered 373 K as it is the boiling temperature of the coolant. Also, the mass flow through the bypass hose and radiator changes accordingly as shown in Figure 3d. Figures 4a and 4b show the effect when control signal is interrupted out. The thermostat does not allow any coolant flow through the radiator, and the piston temperature goes above the maximum threshold. Figures 4c and 4d depict the man-in-the-middle attack, where the fluid temperature control signal is manually defined by the attackers in the attack model. Figures 5a and 5b show that the overflow attack reduces the accuracy of the temperature control signal by overflowing the buffer, thus the lower-bits of the control signals are lost. That causes the thermostat to read the incorrect fluid temperature and make wrong decisions, which will eventually lead to the unstable system state. Finally, Figures 5c and 5d show the effect of a down-sampling attack that causes an abrupt change in the control signal.

The control parameter attack is applied to the vulnerable control parameters that quickly make the system unstable. For our simulation purpose we targeted two most important control parameters: Shaft Speed of the pump and Activation Temperature of the thermostat. By changing the Shaft Speed we can regulate the coolant flow in the system, and by controlling the Activation Temperature we can control the...
coolant flow through the radiator and bypass hose. Figures 6a and 6b show the effect of changing the activation temperature. The normal activation temperature considered here is 330 K. However, in between 100th and 200th seconds, it is changed to 360 K which leads to increased piston temperature (6a). Also, it causes corresponding changes in the coolant flow through bypass hose and radiator (6b). Similarly, Figures 6c and 6d represent the impact reducing the shaft speed value from 160 rpm to 60 rpm. It reduces the speed of coolant flow through the system that results in increased piston temperature (6c) and changes in the coolant flow through the bypass hose and radiator (6d).

For the coordinated attacks, we have used combinations of one basic attack and one control parameter attack. Figures 7a and 7b show the effect of the combination of a man-in-the-middle attack and Shaft Speed tampering. In Figure 4c, we see that the temperature of the piston goes around 390 K after 150 seconds for the man-in-the-middle attack alone, but when coordinated with the shaft speed reduction then the piston temperature goes up to 400 K (7a). Similarly, Figures 7c and 7d show the corresponding effect on piston temperature and mass flow rate, respectively, when an overflow attack is coordinated with the Shaft Speed tampering.

VII. CONCLUSIONS

This paper advocates the use of model-based techniques to model cybersecurity in the early design phase of CPS in order to develop secure-by-design systems. Functional modeling provides an adequate abstraction level for incorporating models of cybersecurity risks and countermeasures into the system model, by coupling these elements with the energy, material and signal flows of the modeled system. In this paper, we have presented a modeling approach for cyberattacks, and we have shown that these models may effectively disrupt
the operation of the system. The presented methods may be employed in order to develop models of CPS with built-in resilience to cyberattacks, and to quantitatively evaluate this resilience through simulation.

REFERENCES