IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 April 2023, accepted 5 May 2023, date of publication 9 May 2023, date of current version 15 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3274691

RESEARCH ARTICLE

Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption

MASAKI MIYAMOTO[1], (Graduate Student Member, IEEE), KAORU TERANISHI[1,2], (Graduate Student Member, IEEE), KEITA EMURA[3], AND KIMINAO KOGISO[1], (Member, IEEE)

[1]Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications (UEC), Chofu, Tokyo 1828585, Japan
[2]Japan Society for the Promotion of Science (JSPS), Chiyoda-ku, Tokyo 1020083, Japan
[3]Cybersecurity Research Institute, National Institute of Information and Communications Technology (NICT), Koganei, Tokyo 1848795, Japan

Corresponding author: Kiminao Kogiso (kogiso@uec.ac.jp)

This work was supported by the Japan Society for the Promotion of Science KAKENHI under Grant JP22H01509 and Grant JP21K11897.

ABSTRACT Encrypted control systems are secure control methods that use the cryptographic properties of a specific homomorphic encryption scheme. This study proposes a cyberattack-detectable encrypted control system and validates its effectiveness using a proportional integration derivative (PID) position-control system for an industrial motor. The proposed encrypted control system uses a keyed-homomorphic public-key encryption scheme for real-time detection of cyberattacks, such as signal and control parameter falsification. Additionally, a novel quantizer is presented to reduce the computation cost and quantization-error effects on control performance. The quantizer demonstrated a significant improvement, reducing the computation time by 47.3 % compared to using our previous quantizer, and decreasing the quantization-error effect by 30.6 % compared to a widely-used gain-multiplying quantizer. Moreover, this study establishes conditions through a theorem to avoid an overflow in the proposed control system. Experimental validation confirms that the proposed control system effectively conceals the control operation, and the presented theorem aids in designing the quantization gains to prevent overflows. Notably, the results of falsification attack tests highlight that the proposed control system enables real-time detection of attacked components within control parameters and signals, representing a significant advantage of this study.

INDEX TERMS Cybersecurity, encrypted control, keyed-homomorphic public key encryption, quantization, experimental validation.

I. INTRODUCTION

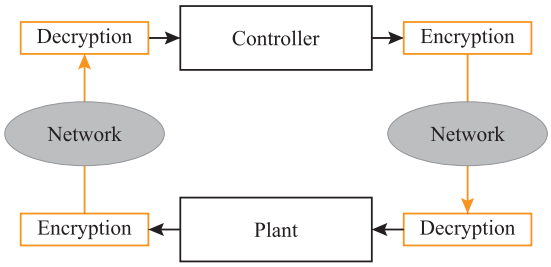
Cybersecurity is important in networked control systems. Networked control systems are connected to information networks used in factory automation and power grids for supporting modern life. However, being connected to an information network entails the risk of a cyberattack on the control system. Furthermore, unlike in the case of conventional information technology systems, cyberattacks on control systems can cause physical damage. Stuxnet destroyed centrifuges at an Iranian nuclear facility [1], and Industroyer caused massive power outages in Ukraine [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Hosam El-Ocla.

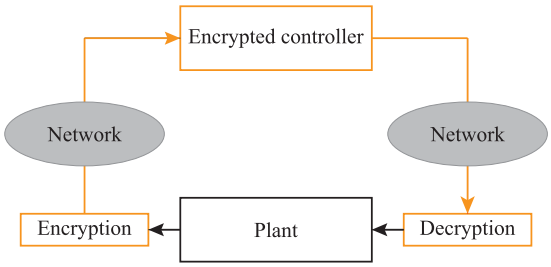
Various techniques that are used to attack control systems and several main attacks [3], [4], [5], [6] are classified based on the impact and adversary's knowledge of the control system [7]. Eavesdropping attacks are the easiest to execute because they do not require any model knowledge of the target control system, but they lead to more sophisticated attacks [8]. However, cryptography can prevent eavesdropping attacks; thus, it increases the security of control systems.

From both control-theoretic and cryptographic viewpoints, a multidisciplinary method can develop a cyber-secure automatic control technology. Homomorphic encryption (HE) [9] enables arithmetic operations on encrypted data. The method of incorporating homomorphic encryption into a control system is known as encrypted control [10], [11],

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/



(a) Traditional (unencrypted) control system.



(b) Encrypted control system.

FIGURE 1. Conceptual configuration of encrypted control systems.

[12], [13]. As shown in Fig. 1(a), networked control systems communicate control-system signals over a network. For cloud-based control systems, which have attracted attention in recent years, computations of the controller are performed in the cloud. In contrast, as shown in Fig. 1(b), an encrypted control system directly determines the control inputs in ciphertext without decrypting the signals. Hence, it has attracted considerable attention because it can reduce the risk of raw data leakage even if an attacker accesses the control network through cyberspace.

A. OUR CONTRIBUTIONS

The objective of this study is to propose an encrypted control system based on a keyed-homomorphic public-key encryption (KH-PKE) scheme that enables the detection of the malleability-based falsification of signals and control parameters. To enhance security, this study considers controller encryption using the KH-PKE scheme [14]. The falsification attack detection is inherited from the feature that allows the decryption and evaluation algorithms of the underlying KH-PKE scheme to output an error symbol when tampering occurs. The proposed encrypted control system benefits from the feature that enables the identification of attacked components within signals and control parameters, which constitutes a significant advantage over the conventional studies [10], [11], [12], [13], [15], [16], [17], [18], [19], [20], [21]. Moreover, a novel efficient quantizer is presented for constructing the encrypted control system, which is developed by modifying a conventional quantizer [16]. The efficient quantizer introduced in this study significantly improves the performance by reducing computation time, as compared to conventional quantizers [16]. Furthermore, this study investigates the conditions for avoiding overflows caused by quantization processes, which is summarized in a theorem. In addition, an experimental validation was conducted to confirm the effectiveness of the proposed encrypted control system using an industrial linear stage. First, this study evaluates three encrypted control systems with a modified quantizer and two conventional quantizers [10], [16] in terms of computation time and quantization-error effects on control performance, and the encryption scheme used is KH-PKE and common. Subsequently, this study verifies the theorem that provides a design policy for quantization gains, compared with the situation where quantization gains do not hold for the theorem. The final validation demonstrates that the proposed encrypted control system enables the real-time detection of falsification attacks. These experimental results indicate that the proposed encrypted control system is adequate and appropriate for developing secure control technologies.

The contributions of this study are threefold. i) This study developed a more secure encrypted control system that enables the real-time detection of cyberattacks compared with conventional encrypted control systems. This implies that there is expertise and knowledge in cryptography that helps enhance the security of control systems. ii) The developed linear-stage control system is a secure automatic control technology, and the proposed method can be implemented and can run in real-time with a certain key length. iii) This study provides the possibility and relevance of appropriate security concepts for real-time control systems in terms of provable and computational security. The findings of this study will lead to the creation of a new fusion area for cryptography and control engineering.

B. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows: Section II introduces the notations and syntax of the KH-PKE scheme. Section III presents the proposed encrypted control system that involves a novel quantizer. Section IV introduces a practical testbed control system and determines the parameters for implementing an encrypted controller. Section V validates the proposed encrypted control system in terms of the control performance effect, overflow avoidance, and cyberattack detection. Section VI discusses the security of the proposed encrypted control system. Finally, Section VII concludes the paper.

C. RELATED WORK

Encrypted control systems using Paillier encryption [22], which is an additive homomorphic encryption (AHE) that enables the addition of encrypted data, have been studied [11], [17], [18], [19]. Encrypted control systems using ElGamal encryption [23], which is a multiplicative homomorphic encryption (MHE) that enables the multiplication of encrypted data, have also been studied [10], [15], [16]. Furthermore, encrypted control systems using fully homomorphic encryption (FHE) [24], which can perform both addition and multiplication, have been proposed [12]. Some recent studies have considered encrypted control systems using AHE or leveled FHE based on learning with errors [20], [21]. Only the signal of the control system is encrypted when using AHE, whereas MHE and FHE enable the encryption of signals and controller parameters.

Countermeasures against cyberattacks such as tampering, are necessary to secure control systems. Although eavesdropping attacks can be prevented, the direct manipulation of signals or controller parameters enables the degradation of control performance or compromises it to break in the worst case. Encrypted control systems are vulnerable to attacks that use the malleability of the homomorphic encryption scheme [25], which means an attacker can manipulate encrypted signals and parameters to adjust controlled outputs without decrypting them. To reduce the vulnerability to attacks, there are related studies that consider countermeasures such as homomorphic authentication [26], obfuscation of controller parameters [25], and cancellation and detection by a modified somewhat homomorphic encryption [27], [28], which uses the malleability of a homomorphic encryption scheme. However, these studies could hardly identify an attacked component within signals and control parameters. The enhancement of cyberattack detection motivated us to develop a secure control technology for a quick response to cyberattack incidents.

The concept of KH-PKE, as proposed in [14] and [29], introduces another private key specifically dedicated to performing homomorphic operations. This approach aims to achieve indistinguishability under an adaptive chosen ciphertext attack (IND-CCA2) against adversaries who do not possess a homomorphic operation key. The IND-CCA2 security property enables the detection of attacks based on malleability, and various configurations of KH-PKE have been proposed in [14], [29], [30], [31], [32], [33], and [34]. Furthermore, a study has also proposed a KH-PKE scheme that supports multiplicative homomorphic operations [14]. Notably, the KH-PKE scheme is secure under the decisional Diffie-Hellman (DDH) assumption, which is commonly used to prove the security of ElGamal encryption. As a result, the use of DDH-based KH-PKE scheme is expected to enhance the security of encrypted control systems, making them more resillient against potentail cyberattacks.

II. PRELIMINARIES

This section provides notations of variables and functions and introduces the KH-PKE as preliminaries for constructing encrypted control systems.

A. NOTATIONS

Sets of real numbers, integers, plaintext spaces, and ciphertext spaces are denoted by $\mathbb{R}$, $\mathbb{Z}$, $\mathcal{M}$, $\mathcal{C}$, respectively. We define $\mathbb{R}^+ := \{x \in \mathbb{R} \mid 0 < x\}$, $\mathbb{Z}^+ := \{z \in \mathbb{Z} \mid 0 < z\}$, $\mathbb{Z}_n := \{z \in \mathbb{Z} \mid 0 \leq z < n\}$, $\mathbb{Z}_n^+ := \{z \in \mathbb{Z} \mid 0 < z < n\}$, and $\mathfrak{P}_a^b := \{a^i \bmod b \mid i \in \mathbb{Z}_b\}$. A set of vectors of size n is denoted by $\mathbb{R}^n$. The jth element of vector v is denoted by v_j. ℓ_2 norm and infinity norm v are denoted by $||v||$ and $||v||_\infty$, respectively. The set of matrices of size $m \times n$ is denoted by $\mathbb{R}^{m\times n}$. (i, j) entry of matrix M is denoted by M_{ij}. The induced 2-norm and maximum norm of M are denoted by $||M||$ and $||M||_{\max}$, respectively. The greatest common divisor of the two positive integers $a, b \in \mathbb{Z}^+$ is denoted by $\gcd(a, b)$.

Definition 2.1: The minimal residue of integer $a \in \mathbb{Z}$ modulo $m \in \mathbb{Z}^+$ is defined as

$$a \operatorname{Mod} m := \begin{cases} b & \text{if } b < |b - m|, \\ b - m & \text{otherwise,} \end{cases}$$

where $b = a \bmod m$. For example, let $m = 10$, $a_1 = 3$, and $a_2 = 7$, then $a_1 \operatorname{Mod} m = 3$ and $a_2 \operatorname{Mod} m = -3$, where $a_1 \bmod m = 3$ and $a_2 \bmod m = 7$.

Definition 2.2: Let p be an odd prime number and z be an integer satisfying $\gcd(z, p) = 1$. If there exists integer b such that $b^2 = z \bmod p$, then integer z is the quadratic residue of modulo p. If integer b does not exist, then integer z is a quadratic nonresidue of modulo p. This can be expressed using the Legendre symbol $(\cdot/\cdot)_L$ as follows:

$$\left(\frac{z}{p}\right)_L := z^{\frac{p-1}{2}} \operatorname{Mod} p = \begin{cases} 1 & \text{if } z \text{ is a quadratic residue,} \\ -1 & \text{if } z \text{ is a quadratic nonresidue.} \end{cases}$$

Definition 2.3: The rounding function $\lceil \cdot \rfloor$ of $\sigma \in \mathbb{R}^+$ to the nearest positive integer is defined as

$$\lceil \sigma \rfloor = \begin{cases} \lfloor \sigma + 0.5 \rfloor & \text{if } \sigma \geq 0.5, \\ 1 & \text{otherwise,} \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

B. KEYED-HOMOMORPHIC PUBLIC KEY ENCRYPTION

The syntax of KH-PKE for homomorphic operations [14] is introduced as follows:

Definition 2.4 (KH-PKE): Let $\odot$ be a binary operation over $\mathcal{M}$. The KH-PKE scheme $\mathcal{E} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}, \mathbf{Eval})$ for homomorphic operation $\odot$ consists of the following four algorithms:

- **Gen**: This key-generation algorithm takes a security parameter $\kappa \in \mathbb{R}^+$ as the input and returns public key $\mathbf{pk}$, private key $\mathbf{sk_d}$, and homomorphic operation key $\mathbf{sk_h}$;
- **Enc**: This encryption algorithm takes $\mathbf{pk}$ and plaintext $m \in \mathcal{M}$ as the input and returns ciphertext $c \in \mathcal{C}$;
- **Dec**: This decryption algorithm takes $\mathbf{sk_d}$ and c as inputs and returns m or $\perp$.
- **Eval**: This evaluation algorithm takes $\mathbf{sk_h}$, two ciphertexts c_1 and c_2 as inputs and returns ciphertexts c or $\perp$,

where $\perp$ denotes the error symbol.

Definition 2.5 (Correctness): A KH-PKE scheme for homomorphic operation $\odot$ is correct if, for all $(\mathbf{pk}, \mathbf{sk_d}, \mathbf{sk_h}) \leftarrow \mathbf{Gen}(\mathbf{1}^\kappa)$, the following two conditions are satisfied:

1) For all $m \in \mathcal{M}$ and $c \in \mathcal{C}_{\mathbf{pk},m}$, it holds that $\mathbf{Dec}(\mathbf{sk_d}, c) = m$;
2) For all $m_1, m_2 \in \mathcal{M}$, $c_1 \in \mathcal{C}_{\mathbf{pk},m_1}$, and $c_2 \in \mathcal{C}_{\mathbf{pk},m_2}$, it holds that $\mathbf{Eval}(\mathbf{sk_h}, c_1, c_2) \in \mathcal{C}_{\mathbf{pk},m_1 \odot m_2}$,

where $\mathcal{C}_{\mathbf{pk},m}$ denotes the set of all ciphertexts of $m \in \mathcal{M}$ under the public key $\mathbf{pk}$. For simplicity, the arguments $\mathbf{pk}$, $\mathbf{sk_d}$, and $\mathbf{sk_h}$ will be omitted henceforth.

In this study, the multiplicative KH-PKE scheme proposed in [14] is used to encrypt communication signals and

control parameters. This security is provided by the DDH assumption. In the case of multiplicative DDH-based KH-PKE, $\odot$ is replaced with a multiplicative homomorphic operation, and the plaintext space is a multiplicative cyclic group, defined as $\mathbb{G} := \{g^i \bmod p \mid i \in \mathbb{Z}_q\}$ such that $g^q \bmod p = 1$ and $p-1 \bmod q = 0$ with generator g of cyclic group $\mathbb{G}$, which is a set of positive integers with discrete values. The four algorithms can be specified as **Appendix A**. Moreover, the DDH-based KH-PKE scheme enables the error symbol to be returned when processing ill-formed ciphertexts in the **Dec** and **Eval** algorithms. Therefore, the DDH-based KH-PKE scheme helps us realize encrypted control systems with real-time detection of tampered communication signals and/or control parameters.

Remark 2.6: The original definition of the KH-PKE scheme states that if tampering occurs, then the error symbol is output to terminate the algorithm. However, because control systems require availability, this study modifies the algorithm such that it outputs the corresponding signals and never terminates them even if tampering occurs.

III. ENCRYPTED CONTROL SYSTEM

This section presents an appropriate quantizer for the proposed encrypted control systems, introduces the controller encryption technique, and explains the quantizer design policy to avoid overflows.

A. QUANTIZER

A quantizer is required to construct the encryption control system because the plaintexts and ciphertexts in the encryption scheme are integers, and the processes at the controller are reconstructed using the encryption scheme. Hence, this study presents a novel quantizer that maps $x \in \mathbb{R}$ onto $\bar{x} := (\bar{x}^1, \bar{x}^2) \in \mathbb{G}^2$, an encoding map $\mathsf{Ecd}_\gamma := \mathscr{C} \circ \mathscr{A}_\gamma$, and a decoding map $\mathsf{Dcd}_\gamma := \mathscr{B}_\gamma \circ \mathscr{D}$ with

$$
\begin{aligned}
\mathscr{A}_\gamma &: \mathbb{R} \to \mathfrak{P}_2^q \times \mathbb{Z}_q^+, \\
&: x \mapsto \begin{cases} (1, \lceil \gamma |x| \rfloor \bmod q) & \text{if } x \geq 0, \\ (2, \lceil \gamma |x| \rfloor \bmod q) & \text{if } x < 0, \end{cases} \\
\mathscr{B}_\gamma &: \mathfrak{P}_2^q \times \mathbb{Z}_q^+ \to \mathbb{R}, \\
&: (\zeta, z) \mapsto \left(\frac{\zeta}{3}\right)_L \frac{z}{\gamma} := \check{x}, \\
\mathscr{C} &: \mathfrak{P}_2^q \times \mathbb{Z}_q^+ \to \mathbb{G}^2, \\
&: (\zeta, z) \mapsto \left(\left(\frac{\zeta}{p}\right)_L \zeta, \left(\frac{z}{p}\right)_L z\right) \bmod p := (\bar{x}^1, \bar{x}^2), \\
\mathscr{D} &: \mathbb{G}^2 \to \mathfrak{P}_2^q \times \mathbb{Z}_q^+, \\
&: (\bar{x}^1, \bar{x}^2) \mapsto (|\bar{x}^1 \operatorname{Mod} p|, |\bar{x}^2 \operatorname{Mod} p|),
\end{aligned}
$$

where $\gamma \in \mathbb{R}^+$ is the quantization gain, $\zeta \in \{1, 2\}$, and $z := \lceil \gamma |x| \rfloor \bmod q$. The relationship between the maps is shown in Fig. 2.

The presented quantizer comprising Ecd_γ and Dec_γ is a modified version of the conventional quantizer [16] and has the advantage of reducing computation time and resource consumption compared to the conventional quantizer. The conventional quantizer uses plaintext space $\mathbb{G}^3$ that assigns

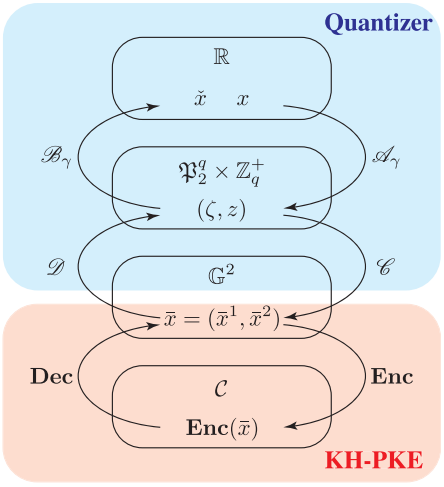


FIGURE 2. Relationship of the maps between the real and ciphertext spaces, realized by the presented $\mathbb{G}^2$-based quantizer.

$\mathbb{G}$ to a zero component. The assignment is inefficient in computing; therefore, the presented quantizer removes the zero component to obtain the plaintext space $\mathbb{G}^2$. In this study, the conventional quantizer is called a $\mathbb{G}^3$-based quantizer. In addition, the effects of the presented quantizer on the computation time are presented in Section IV-B. The proposed encrypted control system requires the plaintext space $\mathbb{G}^2$; therefore, the KH-PKE scheme must be conducted twice to encrypt data, as indicated in Fig. 2.

Remark 3.1: IND-CCA2 security holds against a KH-PKE ciphertext, and it does not imply IND-CCA2 security against two ciphertexts in a strict manner. In other words, the ciphertexts of $\bar{x}^1$ and $\bar{x}^2$ are non-malleable. However, if we consider that $(\mathbf{Enc}(\bar{x}^1), \mathbf{Enc}(\bar{x}^2))$ is a ciphertext, then it is malleable; for example, one can replace a component $\mathbf{Enc}(\bar{x}^1)$ (or $\mathbf{Enc}(\bar{x}^2)$) with other KH-PKE ciphertexts. In our system, this study does not consider such a replacement as tampering but considers element-wise tampering.

B. CONTROLLER ENCRYPTION

Let us consider a linear controller in a discrete-time state-space representation $f : \mathbb{R}^n \times \mathbb{R}^l \to \mathbb{R}^n \times \mathbb{R}^m$,

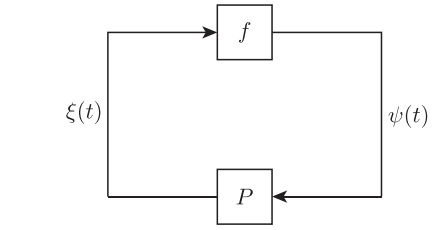
$$
f : \begin{cases} x_c(t+1) = A_c x_c(t) + B_c v_c(t), \\ u(t) = C_c x_c(t) + D_c v_c(t), \end{cases} \tag{1}
$$

where $t \in \mathbb{Z}^+$ is the time step, $u \in \mathbb{R}^m$ is the control input, $v_c \in \mathbb{R}^l$ is the measured output, $x_c \in \mathbb{R}^n$ is a controller state, and A_c, B_c, C_c, and D_c are controller parameters. Controller (1) can be rewritten as follows:

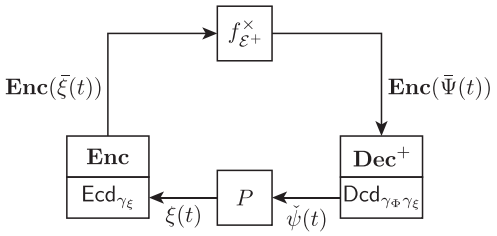
$$
\psi(t) = \Phi \xi(t) =: f(\Phi, \xi(t)), \tag{2}
$$

where $\Phi \in \mathbb{R}^{\alpha \times \beta}$ denotes a matrix that collects the control parameters, and $\psi \in \mathbb{R}^\alpha$ and $\xi \in \mathbb{R}^\beta$ denote a vector gathering the arguments and computed variables in the controller, respectively, which are written as follows:

$$
\Phi := \begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix}, \psi(t) := \begin{bmatrix} x_c(t+1) \\ u(t) \end{bmatrix}, \xi(t) := \begin{bmatrix} x_c(t) \\ v_c(t) \end{bmatrix}, \tag{3}
$$



(a) Unencrypted control system.



(b) Encrypted control system using the KH-PKE scheme.

FIGURE 3. Block diagrams of feedback control systems before and after the controller encryption.

where $\alpha = n+m$ and $\beta = n+l$. The control system is shown in Fig. 3(a).

Because f is a composition product of multiplication $f^{\times}$ and addition f^{+}, the decryption algorithm is modified to yield $\mathbf{Dec}^{+} = f^{+} \circ \mathbf{Dec}$ [10]. Using the modified homomorphic encryption scheme $\mathcal{E}^{+} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}^{+}, \mathbf{Eval})$, the linear controller (1) can be encrypted, that is, it can be reconstructed into a different representation consisting of only encrypted parameters and signals. Then, the resulting encrypted controller when using $\mathcal{E}^{+}$ forms, $\forall t \in \mathbb{Z}^{+}$,

$$f^{\times}_{\mathcal{E}^+} : (\mathbf{Enc}(\bar{\Phi}), \mathbf{Enc}(\bar{\xi}(t))) \mapsto \mathbf{Enc}(\bar{\Psi}(t)), \tag{4}$$

where $\bar{\Phi} = \mathsf{Ecd}_{\gamma_\Phi}(\Phi)$, $\bar{\xi} = \mathsf{Ecd}_{\gamma_\xi}(\xi)$, $\bar{\Psi} = \mathsf{Ecd}_{\gamma_\Phi\gamma_\xi}(f^{\times}(\Phi, \xi))$, γ_Φ and γ_ξ are quantization gains regarding Φ and ξ, respectively, and $\mathbf{Enc}(\bar{\Psi}(t))$ is calculated using **Eval** as follows, $\forall t \in \mathbb{Z}^{+}$,

$$\mathbf{Enc}(\bar{\Psi}^{\theta}_{ij}(t)) = \mathbf{Eval}(\mathbf{Enc}(\bar{\Phi}^{\theta}_{ij}), \mathbf{Enc}(\bar{\xi}^{\theta}_{j}(t)), \\ \forall \theta \in \{1, 2\}, \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}.$$

The process (4) is a ciphertext version of (1); therefore, function f running in the controller is replaced by $f^{\times}_{\mathcal{E}^+}$, and the controller output $\mathbf{Enc}(\bar{\Psi}(t))$ is decrypted and decoded at the plant side to extract control input u via a signal $\check{\psi} = \mathsf{Dcd}_{\gamma_\Phi\gamma_\xi}(\mathbf{Dec}^{+}(\mathbf{Enc}(\bar{\Psi}(t))))$. The resulting encrypted control system is illustrated in Fig. 3(b).

The merits of using the KH-PKE scheme are as follows. The proposed encrypted control system can operate using encrypted Φ, ξ, and ψ. An index of vectors or matrices falsified by attackers can be identified because **Eval** and **Dec** are performed element-wise. Thus, controller encryption can protect the controller device and communication from cyberattacks, such as eavesdropping, and can also detect the falsification of signals and control parameters.

C. DESIGN POLICY OF QUANTIZATION GAIN

The plaintext space is finite; thus, overflows may occur with inappropriate gains. This study then provides the design policy of quantization gain as a theorem.

Definition 3.2: An overflow occurs when quantizing Φ, ξ, and a homomorphic operation if $\lceil \gamma_\Phi |\Phi_{ij}| \rfloor \geq q$, $\lceil \gamma_\xi |\xi_j| \rfloor \geq q$, and $\lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\Phi |\xi_j| \rfloor \geq q$ hold, respectively.

Theorem 3.3: Consider a discrete-time linear controller with input $\xi \in \mathbb{R}^{\beta}$ and coefficient matrix $\Phi \in \mathbb{R}^{\alpha \times \beta}$, where $\Phi_{\max} := ||\Phi||_{\max}$ is nonzero. For a given positive integer q, if there exists a quantization gain $\gamma_\Phi \in \mathbb{R}^{+}$ such that the following inequality condition:

$$\gamma_\Phi < \frac{1}{\Phi_{\max}} \left(q - \frac{1}{2} \right), \tag{5}$$

holds, and if there exists a quantization gain $\gamma_\xi \in \mathbb{R}^{+}$ and $||\xi(t)||_\infty < \infty, \forall t \in \mathbb{Z}^{+}$, such that the following inequality condition:

$$\gamma_\xi < \frac{1}{\gamma_\Phi \Phi_{\max} ||\xi(t)||_\infty} \left(q - \frac{1}{2} \right) \ \forall t \in \mathbb{Z}^{+}, \tag{6}$$

holds, then an overflow never occurs in the control operation using quantization gains γ_Φ and γ_ξ.

Proof: The inequality (5) is transformed into

$$q - \frac{1}{2} > \gamma_\Phi \Phi_{\max} \geq \gamma_\Phi |\Phi_{ij}|, \ \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}, \\ \Rightarrow \left\lceil q - \frac{1}{2} \right\rfloor = q > \lfloor \gamma_\Phi |\Phi_{ij}| \rfloor = \lceil \gamma_\Phi |\Phi_{ij}| \rfloor, \forall i, j, \tag{7}$$

which is the condition in which an overflow never occurs when quantizing Φ. Next, we define $\xi_{\max} := ||\xi(t)||_\infty$, $\forall t \in \mathbb{Z}^{+}$. The inequality (6) is transformed into

$$\begin{aligned} q - \frac{1}{2} &> \gamma_\Phi \Phi_{\max} \gamma_\xi \xi_{\max} \\ &\geq \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max}, \ \forall i \in \mathbb{Z}^{+}_{\alpha+1}, \forall j \in \mathbb{Z}^{+}_{\beta+1}, \\ &\Rightarrow \left\lceil q - \frac{1}{2} \right\rfloor = q > \lfloor \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor \\ &= \lceil \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor, \forall i, j. \end{aligned} \tag{8}$$

When we choose $\xi_{\max}$ such that the following inequality $\lceil \gamma_\Phi |\Phi_{ij}| \gamma_\xi \xi_{\max} \rfloor \geq \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor$ is satisfied, the following inequality holds,

$$\begin{aligned} q &> \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor, \forall i, j, \\ &\Rightarrow q > \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi \xi_{\max} \rfloor \geq \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi |\xi_j| \rfloor, \forall i, j, \\ &\Rightarrow q > \lceil \gamma_\Phi |\Phi_{ij}| \rfloor \lceil \gamma_\xi |\xi_j| \rfloor, \forall i, j, \end{aligned} \tag{9}$$

which implies that an overflow never occurs when quantizing the homomorphic operation. Furthermore, the inequalities (7) and (9) imply that an overflow never occurs when quantizing ξ. Therefore, the overflow avoidance conditions shown in **Definition 3.2** are derived. ■

Remark 3.4: The systematic computation of $\xi_{\max}$, which is needed to confirm the overflow avoidance conditions, is difficult. However, there is a situation where we can estimate it to some extent using the specifications of

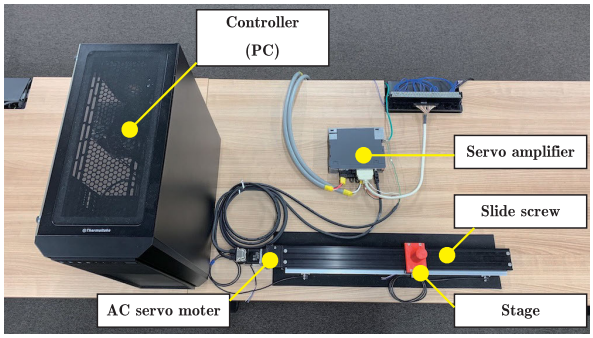


FIGURE 4. Experimental equipment.

TABLE 1. Experimental apparatus.

Servo amplifier	MITSUBISHI MR-J5-10A
Main circuit power supply	1/3-phase 200-240 VAC 50/60 Hz
AC servo motor	MITSUBISHI HK-KT13W
Rated power	0.1 kW
Rated torque	0.32 Nm
Rated speed	3000 rpm
Rated current	1.2 A
Pulse per rotation	67108864 ppr
Slide screw	MiSUMi LX3010CP-MX
Length	1250 mm
Lend	10 mm
PC	
CPU	Intel Core i7-10700K 3.80 GHz
Memory	64 GB
OS	CentOS Linux 8
Language	C++17
DA/AD board	Interface PEX-340216 (16-bit resolution)
Counter board	Interface PEX-632104 (32-bit resolution)

the control systems, such as the allowable position range of a linear stage. Section IV-B explains a method for estimating $\xi_{\max}$.

IV. IMPLEMENTATION

This section introduces a practical testbed control system and determines the parameters for implementing an encrypted controller in the control system.

A. PID POSITION CONTROL SYSTEM

We constructed a position-control system for the linear stage. Fig. 4 presents an overview of the stage position-control system. The actuator used to drive the stage via a slide screw (MiSUMi LX3010CP-MX) is an industrial AC servo motor (MITSUBISHI HK-KT13W) with a servo amplifier (MITSUBISHI MR-J5-10A). The controller device is a PC (Intel Core i7 and CentOS Linux 8), where a robot-control development tool, Advanced Robot Control System V6 (ARCS6) [35], was used for real-time control. The PC outputs a control input to the servo amplifier to actuate the AC servomotor. The position of the stage is measured by a rotary encoder installed in the motor unit and fed back to the PC via a counter board to update the control input. The processes run in the control algorithm are written as C++17. The apparatus and their specifications are listed in TABLE 1.

Throughout the experiments of the position control, we used a PID controller with proportional, integral, and derivative gains, K_p, K_i, and K_d, respectively. Defining the state and input of the controller as $x_c := \begin{bmatrix} e & w \end{bmatrix}^{\mathrm{T}}$ and $v_c := \begin{bmatrix} r & y \end{bmatrix}^{\mathrm{T}}$, respectively, the discrete-time state-space representation of the PID controller in (1) has the following matrices:

$$A_c = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, B_c = \begin{bmatrix} 1 & -1 \\ T_s & -T_s \end{bmatrix}, C_c = \begin{bmatrix} -\frac{K_d}{T_s} & K_i \end{bmatrix},$$
$$D_c = \begin{bmatrix} K_p + K_i T_s + \frac{K_d}{T_s} & -(K_p + K_i T_s + \frac{K_d}{T_s}) \end{bmatrix}, \quad (10)$$

where $r \in \mathbb{R}$ is a reference for the stage position, $y \in \mathbb{R}$ is the measured stage position, $e := r - y$ is the tracking error, and w is an integrated value defined as $w(t+1) := \sum_{\tau=0}^{t} e(\tau) T_s = w(t) + e(t) T_s$ with sampling period T_s. In this experiment, $K_p = 1.465 \times 10^{-2}$, $K_i = 6.000 \times 10^{-3}$, $K_d = 1.500 \times 10^{-4}$, and $T_s = 20$ ms. In this case, Φ is given as follows:

$$\Phi = \begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & 1 & 0.02 & -0.02 \\ -0.0075 & 0.006 & 0.0223 & -0.0223 \end{bmatrix},$$

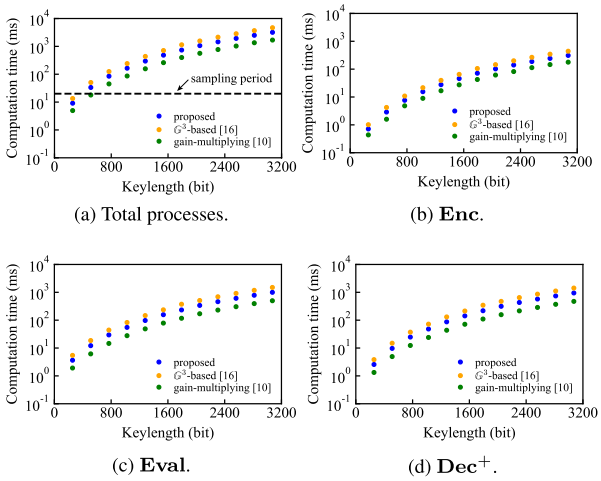
and ξ is defined by $\xi := \begin{bmatrix} e & w & r & y \end{bmatrix}^{\mathrm{T}}$, where $\alpha = 3$ and $\beta = 4$.

B. SECURE IMPLEMENTATION OF THE PID CONTROLLER

To encrypt the PID controller, we set the key length to 256 bits, which was determined by evaluating the computation time of the encrypted control processes, including **Enc**, **Eval**, and **Dec**$^+$ over key lengths. The averages of 100 computation times from 256 to 3072 bits for every 256 bits are shown in Fig. 5. Fig. 5(a) shows the total computation time of **Enc**, **Eval**, and **Dec**$^+$ of the encrypted controls using the proposed $\mathbb{G}^2$-based, $\mathbb{G}^3$-based [16], and gain-multiplying [10] quantizers, as shown in Figs. 5(b), (c), and (d), respectively. Table 2 presents the total computation time and its comparison to the proposed quantizer. The two conventional methods employed the DDH-based KH-PKE scheme, which is common in the method proposed in this study. The figure and table confirm that the computation time of the proposed encrypted control is 47.3 % lower than that of the control system with the $\mathbb{G}^3$-based quantizer, as mentioned in Section III-A. Although processing the control computation with the gain-multiplying quantizer is 45.6 % faster than with the proposed control, it tends to degrade the control performance, as shown in Section V-A. Furthermore, the computation at key length $\ell = 256$ must be completed within a sampling period of 20 ms; therefore, the presented faster quantizer is preferred to the $\mathbb{G}^3$-based quantizer.

We determine γ_Φ and γ_ξ using **Theorem 3.3**. First, we set γ_Φ to 1.0×10^{20} from the inequality (5) of $\gamma_\Phi < 4.3 \times 10^{76}$, with $||\Phi||_{\max} = 1$ and

$$q = 436330242283591462479179208760550548662 \times 291077161756781216195899944211526105 93,$$
$$\approx 4.3 \times 10^{76}.$$



(a) Total processes. (b) **Enc**. (c) **Eval**. (d) $\mathbf{Dec}^+$.

FIGURE 5. Computation time of each process over the key length.

Next, we estimate $||\xi(t)||_\infty$ over a step; that is, we estimate the maximum error e, state w, reference r, and output y. When the length of the linear stage is 1250 mm, the maximum error is 1250 mm because of $e = r - y = 625 - (-625)$. w is given by $w(t+1) := \sum_{\tau=0}^{t} e(\tau)T_s = w(t) + e(t)T_s$. If $T_s = 0.02$ and the duration of this experiment is 10 s, then the maximum state is 1250. Subsequently, $||\xi(t)||_\infty$ can be set to 1250. Therefore, we set γ_ξ to 1.0×10^{53} from inequality (6) of $\gamma_\xi < 3.44 \times 10^{53}$.

Using KH-PKE with the parameters above, the controller gains Φ are encrypted and implemented on the PC. For example, $\mathbf{Enc}(\bar{\Phi}^1_{11})$, $\mathbf{Enc}(\bar{\Phi}^2_{31})$, and $\mathbf{Enc}(\bar{\Phi}^2_{32})$ are (11), as shown at the bottom of the page.

V. EXPERIMENTAL VALIDATION

This section validates the three attributes of the proposed encrypted control system, namely, the control-performance effect, overflow avoidance, and cyberattack detection, compared with the unencrypted control (10) and the two conventional encrypted controls with a $\mathbb{G}^3$-based quantizer [16] and gain-multiplying quantizer [10]. The used encryption scheme, which is a DDH-based PH-PKE, is the same for the three encrypted control methods. In addition, the used control parameters are common, and the other parameters such as γ_Φ, γ_ξ, and ℓ are the same.

A. CONTROL RESULTS

We present the experimental results of position control using the proposed, conventional, and unencrypted controls with a step-like reference, which is given as follows:

$$\begin{cases} 0 & \text{if } 0 \le T_s t < 2 \text{ or } 8 \le T_s t < 10, \\ 50 & \text{if } 2 \le T_s t < 4 \text{ or } 6 \le T_s t < 8, \\ 100 & \text{if } 4 \le T_s t < 6, \end{cases} \tag{12}$$

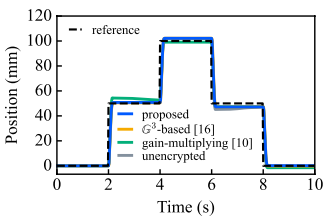
to examine the effects of the proposed secure implementation on a control system.

The control results are presented in Fig. 6. Figs. 6(a) and (b) show the time responses of the stage position and control input, respectively. In the figures, the blue, green, yellow, and gray lines represent the proposed, conventional [10], [16], and unencrypted control methods, respectively, where the broken line represents the reference. Fig. 6(c) shows three stage-position errors between each of the three encrypted controls and the unencrypted control, respectively, and Fig. 6(d) shows the three control input errors between the encrypted control and the unencrypted control. In Figs. 6(c) and (d), the blue line represents the proposed method, and green and yellow lines represent the two conventional methods. Figs. 6(e), (f), and (g) show the quantization error between the quantized and unquantized control inputs, that is, $|\check{u}(t) - u(t)|$, for the proposed method and the two conventional methods, respectively. Table 2 presents ℓ_1-norm values of the quantization-error signals for each quantizer up to 10 s. Figs. 6(h) and (i) show the time responses of the encrypted signals $\mathbf{Enc}(\Psi^1_{33}(t))$ and $\mathbf{Enc}(\xi^1_3(t))$, respectively, which correspond to parts of the output and input signals of the controller.

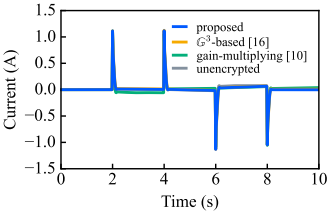
$$\mathbf{Enc}(\bar{\Phi}^1_{11}) = \begin{array}{l}\texttt{(ef99a26e99df01b7c50118dea8b8826fa169177f3c94333f6de844b7faa738a5,}\\ \texttt{f5e78a92d80b0a6ad503a8338905d373b6afae3b1615bdc6280bab18cac4571e,}\\ \texttt{da6e18939379d11f1fb6ca2a7350156adade88f55fac80ecad62b142fe34bd72,}\\ \texttt{4fe15d197c003ee86ee3a35404a8c7cde1e1c1f12a43d963c1d1e2d5f20d5a98,}\\ \texttt{b386194f8a1f016ffc6afdd8469630f7d242db11e5ff6332471048ab8ff7c7f),}\end{array} \tag{11a}$$

$$\mathbf{Enc}(\bar{\Phi}^2_{31}) = \begin{array}{l}\texttt{(c350361fb7d41633662736edb5028dba4cc7ae4d4189d75778aa73c357f2f9d0,}\\ \texttt{73bd85f730994868b02ee2512272c96452aca1575f0317c1ef32de3840c527df,}\\ \texttt{941863c7e67f6ec4f48ba7cdcb04f2da1c1871442da5daaf8e69f88987243546,}\\ \texttt{179a00c5a06fc763972cc5254bdf7beb9d8e4d3057391b679a23dc072c2e3114,}\\ \texttt{112f5a3adc5bdf4d4509195e4c97879328dd158ddee5899c978ba0defb7034b8),}\end{array} \tag{11b}$$

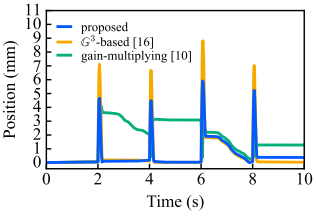
$$\mathbf{Enc}(\bar{\Phi}^2_{32}) = \begin{array}{l}\texttt{(eb6906386c2e66dbfa88403f3297ca0356c28b00e9ac6dbd1db81caffa4a7312,}\\ \texttt{ee15995c854fb987ee47338a31f4dce480635e2e75123d03dc1370b29f204abd,}\\ \texttt{e434b267068ca03fde81d39dd1644f466c8588dc91e1bae366d0591add6d5c09,}\\ \texttt{d9d89949da579ecb3b662c434575425470fffcf1e19c52f34bd9d11b36c35e65,}\\ \texttt{a4cf383732d68e30a05a96398a3dd3fdda246b08a8786c0cd4be46cfdcdcf866).}\end{array} \tag{11c}$$



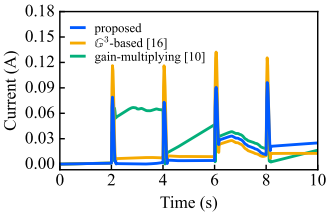
(a) Controlled output: $y(t)$.



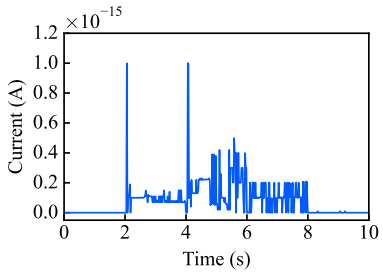
(b) Control input: $u(t)$.



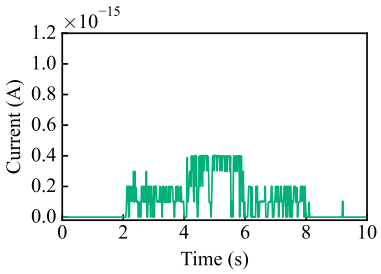
(c) Deviation from the output of the unencrypted control system.



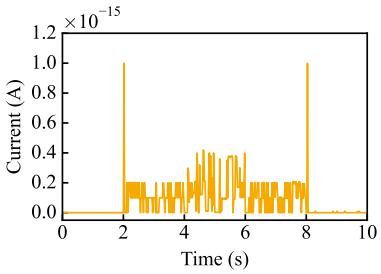
(d) Deviation from the control input of the unencrypted control system.



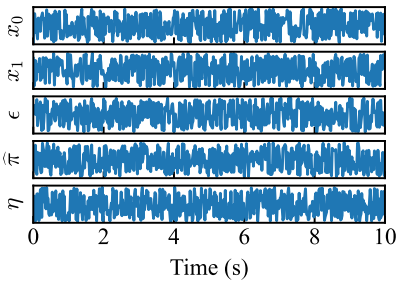
(e) Quantization error in u of the proposed $\mathbb{G}^2$-based quantizer.



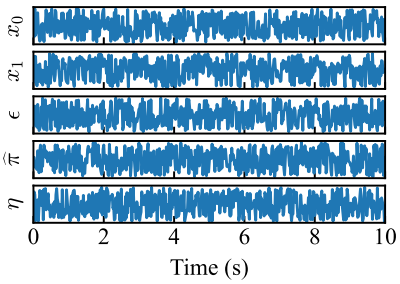
(f) Quantization error in u of the conventional gain-multiplying quantizer.



(g) Quantization error in u of the conventional $\mathbb{G}^3$-based quantizer.



(h) $\mathbf{Enc}(\Psi_{33}^1(t))$.



(i) $\mathbf{Enc}(\xi_3^1(t))$.

FIGURE 6. Experimental results of the four control methods: the KH-PKE-based encrypted control systems with the proposed $\mathbb{G}^2$-based quntizer, the conventional gain-multiplying [10] and $\mathbb{G}^3$-based [16] quantizers, and the unencrypted PID control system (10). The parameters $\ell = 256$, $\gamma_\Phi = 10^{20}$, and $\gamma_\xi = 10^{53}$ are the same for the proposed and conventional encrypted controls.

Figs. 6(c) and (d) confirm that the proposed control system achieves less deviation from the conventional method using the gain-multiplying quantizer. As shown in Table 2, the ℓ_1-norm values of the quantization-error signals in Figs. 6(e), (f), and (g) are 3.880×10^{-14}, 5.074×10^{-14}, and 3.856×10^{-14}, respectively. These scores demonstrate that the modification of the plaintext space from $\mathbb{G}^3$ to $\mathbb{G}^2$ has minimal impact on the quantization error, resulting in only a 0.6 % difference in the resulting control signals. The proposed control system achieves a 30.6 % improvement compared to the gain-multiplying quantizer. Furthermore, the parameters of (11) and signals shown in Figs. 6(h) and (i) were concealed in random numbers. The norm scores imply that the proposed control system is better than conventional systems in terms of control performance degradation and that they are negligibly small from the viewpoint of using variables in the C++ language.

Therefore, the control experimental results confirm that the proposed encrypted control system has a smaller impact on the control performance than the conventional encrypted control systems.

B. OVERFLOW AVOIDANCE

This section shows that **Theorem 3.3** helps us choose the appropriate values of γ_Φ and γ_ξ to avoid overflows in the control operation. Overflow avoidance is validated by showing another control result of the proposed encrypted control with inappropriate values, such as $\gamma_\Phi = 1.0 \times 10^{20}$ and $\gamma_\xi = 1.0 \times 10^{57}$, which do not satisfy the inequality in (6).

The control results for this case are shown in Fig. 7. Figs. 7(a) and (b) show the stage position and the control input, respectively, using the blue line. In this case, an overflow occurred between 2.00 s and 8.16 s, highlighted in yellow. The figures confirm that the control input was too small for the stage to follow the reference. This is because of the large γ_ξ, such that the term $\lceil \gamma |x| \rfloor$ of $\mathscr{A}_\gamma$ is greater than q in encoding, which implies an overflow. Therefore, the control result confirms that **Theorem 3.3** facilitates the desig of parameter values to avoid overflow.

Remark 5.1: If a systematic method of designing parameters is established, $||\xi(t)||_\infty$ must be estimated before starting the control operation or a dynamic quantizer related to γ_ξ using the observation of $\xi(t)$ [36], [37]. The estimation may

TABLE 2. Performance comparison of computation time and quantization error in the experimental results.

Encrypted control system with	Computation time (ms) at a 256-bit key length	Rate to the proposed quantizer (%)	Evaluation of quantization error	Rate to the proposed quantizer (%)
the proposed quantizer	9.12	100	3.880×10^{-14}	100
the $\mathbb{G}^3$-based quantizer [16]	13.43	147.3	3.856×10^{-14}	99.4
the gain-multiplying quantizer [10]	4.96	54.4	5.074×10^{-14}	130.6

be discussed using the equipment properties as stated in Section IV-B, while the dynamic quantizer design requires a different problem setting and further discussion; therefore, the systematic parameter design will be addressed in our future study.

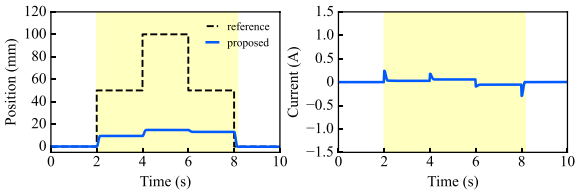
C. ATTACK DETECTION

It is demonstrated that the proposed encrypted control system enables the detection of malleability-based cyberattacks. An attacker does not know the homomorphic operation key $\mathbf{sk_h}$ for **Eval**; therefore, they tamper with the third element of the ciphertext using a constant factor. Because the homomorphic encryption scheme yields malleability, the attacker can obtain the desired decryption result by falsifying the ciphertext [25]. In KH-PKE, the last element of the **Dec** algorithm is $m = \epsilon/\pi \bmod p$, which means, if the third element e of the ciphertext is multiplied by $\lambda \in \mathbb{G}$, the decryption result is λ-fold. Therefore, even if the attackers do not know $\mathbf{sk_h}$, they can tamper with the data.

We consider two cyberattacks in this test: One falsifies an encrypted signal, double $\mathbf{Enc}(\bar{\xi}_4^2(t))$ in 4.0 s to 4.1 s, and the other falsifies two components of the control parameter triple $\mathbf{Enc}(\bar{\Phi}_{31}^2)$ and $\mathbf{Enc}(\bar{\Phi}_{32}^2)$ at 4.0 s, respectively. This means that the cyberattack doubles the signal or triples the two components of the parameter matrix.

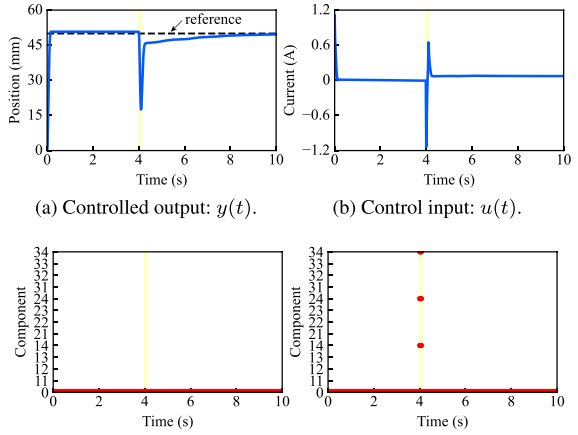
The cyberattack test results for falsifying a signal are shown in Fig. 8. Figs. 8(a) and (b) show the stage position and the control input, respectively. Figs. 8(c) and (d) show the error symbols for $\mathbf{Enc}(\bar{\Psi}^1)$ and $\mathbf{Enc}(\bar{\Psi}^2)$ in **Eval**, respectively. Fig. 8(a) shows that falsification of the sensor values caused spike-like changes in the stage position, indicating that tampering with the sensor values can destroy the control system. For such a falsification attack, the falsification time is confirmed from the error symbol, as shown in Fig. 8(c) and (d). Moreover, the indices of $\mathbf{Enc}(\bar{\Psi}_{14}^2)$, $\mathbf{Enc}(\bar{\Psi}_{24}^2)$, and $\mathbf{Enc}(\bar{\Psi}_{34}^2)$, which were calculated with the attacked signal $\mathbf{Enc}(\bar{\xi}_4^2)$ between 4.0 s and 4.1 s, can be identified.

The cyberattack test results for falsifying the two components in the control parameter are shown in Fig. 9. Figs. 9(a) and (b) show the stage positions of the stage and control input, respectively. Figs. 9(c) and (d) show the error symbols for $\mathbf{Enc}(\bar{\Psi}^1)$ and $\mathbf{Enc}(\bar{\Psi}^2)$ in **Eval**, respectively. Fig. 9(a) shows that the stage position was gradually shifted by falsifying the controller parameters. Fig. 9(b) shows that the falsification effect is not significantly reflected in the control input, which confirms that it is difficult to detect an attack using the threshold method [38]. For the falsification attack, the falsification time was confirmed using the error symbol, as shown in Figs. 9(c) and (d). The indices of the attacked signals $\mathbf{Enc}(\Phi_{31}^2)$ and $\mathbf{Enc}(\Phi_{32}^2)$ could be detected.



(a) Controlled output: $y(t)$. (b) Control input: $u(t)$.

FIGURE 7. Experimental results of the proposed encrypted PID control method. The used parameters are $\gamma_\Phi = 10^{20}$ and $\gamma_\xi = 10^{57}$, which do not satisfy the inequality condition (6).



(a) Controlled output: $y(t)$. (b) Control input: $u(t)$.

(c) Error symbol for $\mathbf{Enc}(\bar{\Psi}^1)$. (d) Error symbol for $\mathbf{Enc}(\bar{\Psi}^2)$.

FIGURE 8. Experimental result of the cyberattack performed by tampering with signals between 4.0 and 4.1 s against the proposed encrypted control system.

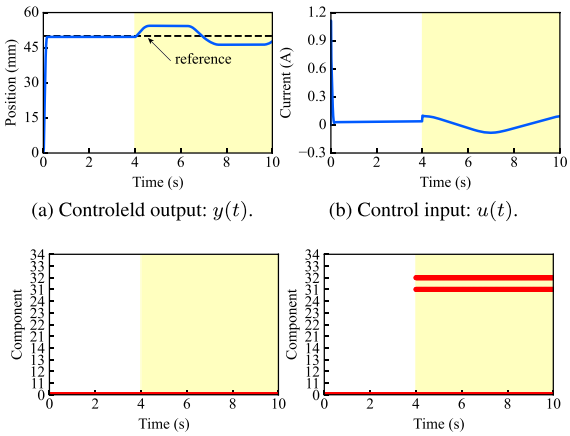
VI. DISCUSSIONS

Based on the results of this study, this section discusses two important issues for future work, to secure control systems.

A. EFFECTS OF A LEAKED HOMOMORPHIC OPERATION KEY

This study considered a situation in which the attacker never has a homomorphic operation key $\mathbf{sk_h}$ in tampering; however, it is also important to consider a situation in which a homomorphic operation key is leaked to a third party. Attackers may use a homomorphic operation to tamper with the ciphertexts in **Eval** to adjust the controlled outputs.

In this case, another detection mechanism is required because the algorithms **Eval** and **Dec** do not output error symbols for detection. One detection approach is to observe unencrypted control inputs from the perspective of a control



(a) Controleld output: $y(t)$. (b) Control input: $u(t)$.

(c) Error symbol for $\mathbf{Enc}(\bar{\Psi}^1)$. (d) Error symbol for $\mathbf{Enc}(\bar{\Psi}^2)$.

FIGURE 9. Experimental results of the cyberattack performed by tampering with control parameters within 4 s against the proposed encrypted control system.

theory, such as threshold-based detection methods [38], [39]. The other is to update the encryption keys in time from the perspective of cryptography, such as storing and replacing the keys periodically [40] and employing an updatable public-key ElGamal encryption scheme [36], [41]. The switching and updatable encryption schemes make it easy to detect falsification and replay attacks, which are difficult to detect in [4]. In this sense, an updatable KH-PKE scheme is expected to enhance the ability to detect cyberattacks on the control systems.

In addition, even if the homomorphic operation key is leaked, the proposed encrypted control system is more secure than an ElGamal-based encryption control system [10]. This is because the KH-PKE scheme retains stronger security than indistinguishability under chosen-ciphertext (IND-CCA1) security even when a key is leaked [14], where IND-CCA1 is the security that homomorphic encryption schemes can achieve [42]. Furthermore, because the controller parameters and signals remain encrypted, the control system is resistant to cyberattacks that require a model of the control system [6], [43].

B. APPROPRIATE SECURITY FOR CONTROL SYSTEMS

Implementing a key of several thousand bits in an encrypted control system with a real-time constraint is challenging, implying the control processes must be completed within a sampling period. The KH-PKE scheme is based on the DDH assumption, and from the viewpoint of cryptology, a key length that can assume the DDH-hardness is needed. Specifically, the NIST document [44] states that a key length of at least 2048 bits is desirable. However, the key length set used in this study was 256 bits to fulfill the real-time constraint under a sampling period of 20 ms, as shown in Fig. 5.

Currently, it is difficult to conclude whether the key length is satisfactory because the answer depends on the security concept we consider. An appropriate security concept exists for control systems, such as indistinguishability against parameter estimation attack (IND-PEA), proposed in [45], which is in provable security and revealed that IND-PEA is equal to indistinguishability under the chosen plaintext attack (IND-CPA). The updatable ElGamal-based encrypted control system [41], [46], which covers computational security, protects the controller parameters from being identified by attackers, even though the key length is shorter than that required by NIST. Furthermore, key updating ideas help solve real-time constraint issues. Such a security concept that is appropriate for control systems has recently been studied; therefore, appropriate security may exist for the 256-bits KH-PKE scheme. Exploring the appropriate security concept is significant for developing the control theory and cryptography fields, which will be explored in our future study. Additionally, in the sense of achieving IND-CCA1/2, the key length is insufficient because it is less than 2048 bits.

VII. CONCLUSION

This study proposed a cyberattack-detectable encrypted control system and validated its effectiveness using an industrial motor PID position-control system. The KH-PKE scheme was employed in the proposed control system for real-time cyberattack detection, and our novel quantizer was used to reduce computation time, as demonstrated by experiments that showed a 47.3 % reduction in computation time while maintaining similar quantization-error impact (with only a 0.6 % difference) compared to our previous quantizer. Furthermore, this study analyzed the conditions for overflow, which are summarized in **Theorem 3.3**. Experimental validations confirmed that the proposed control system concealed the control operation, and the results also confirmed that the theorem helps design quantization gains to avoid overflows. Importantly, this study demonstrated the results of falsification attack tests using homomorphism and confirmed that the proposed control system enables real-time detection of attacked components within signals and control parameters, which is a significant advantage.

Future studies will focus on the following areas. Firstly, the development of countermeasures against leaked homomorphic operation keys to potential attackers, as mentioned in Section VI. The homomorphic operation key is placed in the controller, which poses a risk of leakage to attackers who are interested in breaking into and compromising the control system. Secondly, ensuring the stability of the proposed encrypted control system. The stability of control systems is crucial for safe operation, but the proposed system requires a quantizer, which may destabilize the control system if not stabilized in advance. Finally, exploring security concepts appropriate for control systems and evaluating the security of the encrypted control system developed in this study.

APPENDIX A ALGORITHMS OF DDH-BASED KH-PKE SCHEME

This study uses KH-PKE with multiplicative homomorphism [14] to construct encrypted control systems. The KH-PKE scheme, denoted as $\mathcal{E} = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}, \mathbf{Eval})$, consists of the following four algorithms.

Gen: $\kappa \mapsto (\mathbf{pk}, \mathbf{sk_d}, \mathbf{sk_h})$. The **Gen** algorithm takes security parameter κ and key length ℓ regarding ℓ-bit prime number p and outputs public, private, and homomorphic operation keys, denoted as $\mathbf{pk}$, $\mathbf{sk_d}$, and $\mathbf{sk_h}$, respectively:

$$\begin{aligned}\mathbf{pk} &= (g_0, g_1, s, \widehat{s}, \widetilde{s}_0, \widetilde{s}_1)\,,\\ \mathbf{sk_d} &= \left(k_0, k_1, \widehat{k}_0, \widehat{k}_1, \widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right),\\ \mathbf{sk_h} &= \left(\widetilde{k}_{0,0}, \widetilde{k}_{0,1}, \widetilde{k}_{1,0}, \widetilde{k}_{1,1}\right),\end{aligned}$$

where g_0 and g_1 are randomly chosen from $\mathbb{G}$; $s := g_0^{k_0} g_1^{k_1} \bmod p$; $\widehat{s} := g_0^{\widehat{k}_0} g_1^{\widehat{k}_1} \bmod p$; $\widetilde{s}_0 := g_0^{\widetilde{k}_{0,0}} g_1^{\widetilde{k}_{0,1}} \bmod p$; $\widetilde{s}_1 := g_0^{\widetilde{k}_{1,0}} g_1^{\widetilde{k}_{1,1}} \bmod p$; k_0, k_1, $\widehat{k}_0$, $\widehat{k}_1$, $\widetilde{k}_{0,0}$, $\widetilde{k}_{0,1}$, $\widetilde{k}_{1,0}$, and $\widetilde{k}_{1,1}$ are randomly chosen from $\mathbb{Z}_q$, where $p = 2q + 1$.

Enc: $(\mathbf{pk}, m \in \mathcal{M}) \mapsto c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta) \in \mathcal{C}$. The **Enc** algorithm takes a public key $\mathbf{pk}$ and a plaintext m and outputs a ciphertext c. The components of c are as follows: $x_0 := g_0^{\omega} \bmod p$; $x_1 := g_1^{\omega} \bmod p$; $\epsilon := m\pi \bmod p$; $\widehat{\pi} := \widehat{s}^{\omega} \bmod p$, where $\pi := s^{\omega} \bmod p$ and ω is chosen randomly from $\mathbb{Z}_q$; $\eta := f_{hk}\left(\left(\widetilde{s}_0 \cdot \widetilde{s}_1^{\delta}\right)^{\omega} \bmod p\right)$ with $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$, where γ_{hk} is target collision resistance hash family and f_{hk} is a smooth function [14]. We use SHA-256 to both γ_{hk} and f_{hk}.

Dec: $(\mathbf{sk_d}, c \in \mathcal{C}) \mapsto m \in \mathcal{M} \cup \{\perp\}$. The **Dec** algorithm takes a private key and a ciphertext $c = (x_0, x_1, \epsilon, \widehat{\pi}, \eta)$ and outputs a plaintext m or an error symbol $\perp$. Compute $\widehat{\pi}' := x_0^{\widehat{k}_0} x_1^{\widehat{k}_1} \bmod p$, $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$, and $\eta' := f_{hk}\left(x_0^{\widetilde{k}_{0,0}+\delta\widetilde{k}_{1,0}} x_1^{\widetilde{k}_{0,1}+\delta\widetilde{k}_{1,1}} \bmod p\right)$, where f_{hk} is a smooth function [14]. If either $\widehat{\pi} \neq \widehat{\pi}'$ or $\eta \neq \eta'$, then return an error symbol $\perp$; Otherwise, return $m = \epsilon/\pi \bmod p$, where $\pi := x_0^{k_0} x_1^{k_1} \bmod p$.

Eval: $(\mathbf{sk_h}, c_1, c_2 \in \mathcal{C}) \mapsto c \in \mathcal{C} \cup \{\perp\}$. The **Eval** algorithm takes a homomorphic operation key and two ciphertexts c_i $\forall i \in \{1, 2\}$ and outputs a ciphertext $(x_0, x_1, \epsilon, \widehat{\pi}, \eta)$ or an error symbol $\perp$. The components of the output c are computed as follows: $x_0 := x_{1,0} x_{2,0} g_0^{\omega} \bmod p$, $x_1 := x_{1,1} x_{2,1} g_1^{\omega} \bmod p$, $\epsilon := \epsilon_1 \epsilon_2 s^{\omega} \bmod p$, $\widehat{\pi} := \widehat{\pi}_1 \widehat{\pi}_2 \widehat{s}^{\omega} \bmod p$, and $\eta = f_{hk}\left(x_0^{\widetilde{k}_{0,0}+\delta\widetilde{k}_{1,0}} x_1^{\widetilde{k}_{0,1}+\delta\widetilde{k}_{1,1}} \bmod p\right)$, where $c_i := (x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i, \eta_i)$; $\delta := \gamma_{hk}(x_0, x_1, \epsilon, \widehat{\pi})$; $\delta_i := \gamma_{hk}\left(x_{i,0}, x_{i,1}, \epsilon_i, \widehat{\pi}_i\right)$; ω is randomly chosen from $\mathbb{Z}_q$; $\eta_i' := f_{hk}\left(x_{i,0}^{\widetilde{k}_{0,0}+\delta_i\widetilde{k}_{1,0}} x_{i,1}^{\widetilde{k}_{0,1}+\delta_i\widetilde{k}_{1,1}} \bmod p\right)$. If either $\eta_1 \neq \eta_1'$ or $\eta_2 \neq \eta_2'$, then return $\perp$; Otherwise, return c.

REFERENCES

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, vol. 21, no. 2, p. 210, Feb. 2019.

[4] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918.

[5] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, 2010, pp. 1–6.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[8] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 968–978.

[9] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Comput. Surveys*, vol. 51, no. 4, pp. 1–35, Jul. 2019.

[10] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *Proc. 54th IEEE Conf. Decis. Control (CDC)*, Dec. 2015, pp. 6836–6843.

[11] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.

[12] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 175–180, 2016.

[13] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Syst.*, vol. 41, no. 3, pp. 58–78, Jun. 2021.

[14] K. Emura, G. Hanaoka, K. Nuida, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen ciphertext secure keyed-homomorphic public-key cryptosystems," *Designs, Codes Cryptogr.*, vol. 86, no. 8, pp. 1623–1683, Aug. 2018.

[15] K. Teranishi, N. Shimada, and K. Kogiso, "Stability-guaranteed dynamic ElGamal cryptosystem for encrypted control systems," *IET Control Theory Appl.*, vol. 14, no. 16, pp. 2242–2252, Nov. 2020.

[16] K. Teranishi and K. Kogiso, "ElGamal-type encryption for optimal dynamic quantizer in encrypted control systems," *SICE J. Control, Meas., Syst. Integr.*, vol. 14, no. 1, pp. 59–66, Jan. 2021.

[17] A. B. Alexandru, M. S. Darup, and G. J. Pappas, "Encrypted cooperative control revisited," in *Proc. IEEE Conf. Decis. Control*, Mar. 2019, pp. 7196–7202.

[18] N. Schluter and M. S. Darup, "Encrypted explicit MPC based on two-party computation and convex controller decomposition," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 5469–5476.

[19] M. Kishida, "Encrypted control system with quantizer," *IET Control Theory Appl.*, vol. 13, no. 1, pp. 146–151, 2019.

[20] R. Alisic, J. Kim, and H. Sandberg, "Model-free undetectable attacks on linear systems using LWE-based encryption," *IEEE Control Syst. Lett.*, vol. 7, pp. 1249–1254, 2023.

[21] J. Kim, H. Shim, and K. Han, "Dynamic controller that operates over homomorphically encrypted data for infinite time horizon," *IEEE Trans. Autom. Control*, vol. 68, no. 2, pp. 660–672, Feb. 2023.

[22] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, vol. 5, 1999, pp. 223–238.

[23] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[24] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[25] K. Teranishi and K. Kogiso, "Control-theoretic approach to malleability cancellation by attacked signal normalization," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 297–302, 2019.

[26] J. H. Cheon, K. Han, H. Kim, J. Kim, and H. Shim, "Need for controllers having integer coefficients in homomorphically encrypted dynamic system," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5020–5025.

[27] M. Fauser and P. Zhang, "Resilient homomorphic encryption scheme for cyber-physical systems," in *Proc. 60th IEEE Conf. Decis. Control (CDC)*, Dec. 2021, pp. 5634–5639.

[28] M. Fauser and P. Zhang, "Detection of cyber attacks in encrypted control systems," *IEEE Control Syst. Lett.*, vol. 6, pp. 2365–2370, 2022.

[29] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, and S. Yamada, "Chosen ciphertext secure keyed-homomorphic public-key encryption," in *Proc. Int. Workshop Public Key Cryptography*. Cham, Switzerland: Springer, 2013, pp. 32–50.

[30] B. Libert, T. Peters, M. Joye, and M. Yung, "Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures," in *Proc. Adv. Cryptol. EUROCRYPT*, 2014, pp. 514–532.
[31] C. Jutla and A. Roy, "Dual-system simulation-soundness with applications to UC-PAKE and more," in *Proc. Adv. Cryptol. ASIACRYPT*, 2015, pp. 630–655.
[32] Y. Maeda and K. Nuida, "Chosen ciphertext secure keyed two-level homomorphic encryption," in *Proc. Inf. Secur. Privacy*, 2022, pp. 209–228.
[33] J. Lai, R. H. Deng, C. Ma, K. Sakurai, and J. Weng, "CCA-secure keyed-fully homomorphic encryption," in *Proc. Public-Key Cryptography (PKC)*, 2016, pp. 70–98.
[34] S. Sato, K. Emura, and A. Takayasu, "Keyed-fully homomorphic encryption without indistinguishability obfuscation," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 13269, G. Ateniese and D. Venturi, Eds. Cham, Switzerland: Springer, 2022, pp. 3–23.
[35] Y. Yokokura. *Side Warehouse of Laboratory*. Accessed: Apr. 19, 2023. [Online]. Available: https://www.sidewarehouse.net/arcs6/index.html
[36] K. Teranishi and K. Kogiso, "Dynamic quantizer for encrypted observer-based control," in *Proc. 59th IEEE Conf. Decis. Control (CDC)*, Dec. 2020, pp. 5477–5482.
[37] H. Kawase, K. Teranishi, and K. Kogiso, "Dynamic quantizer synthesis for encrypted state-feedback control systems with partially homomorphic encryption," in *Proc. Amer. Control Conf. (ACC)*, Jun. 2022, pp. 75–81.
[38] B. Rikuna, K. Kogiso, and M. Kishida, "Detection method of controller falsification attacks against encrypted control system," in *Proc. SICE Annu. Conf.*, 2018, pp. 5032–5037.
[39] D. Martynova and P. Zhang, "An approach to encrypted fault detection of cyber-physical systems," in *Proc. Asian Control Conf.*, 2019, pp. 1501–1506.
[40] K. Kogiso, "Attack detection and prevention for encrypted control systems by application of switching-key management," in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 5032–5037.
[41] K. Teranishi, T. Sadamoto, A. Chakrabortty, and K. Kogiso, "Designing optimal key lengths and control laws for encrypted control systems based on sample identifying complexity and deciphering time," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2183–2198, Apr. 2023.
[42] R. Canetti, S. Raghuraman, S. Richelson, and V. Vaikuntanathan, "Chosen-ciphertext secure fully homomorphic encryption," in *Proc. Public Key Cryptography*. Cham, Switzerland: Springer, 2017, pp. 213–240.
[43] R. S. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 90–95, Jan. 2011.
[44] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management part 1: General (revision 5)," Special Publication, NIST, Gaithersburg, MD, USA, Tech. Rep. 800–57, 2020.
[45] K. Teranishi and K. Kogiso, "Towards provably secure encrypted control using homomorphic encryption," in *Proc. IEEE 61st Conf. Decis. Control (CDC)*, Dec. 2022, pp. 7740–7745.
[46] K. Teranishi and K. Kogiso, "Optimal controller and security parameter for encrypted control systems under least squares identification," 2023, *arXiv:2302.12154*.

MASAKI MIYAMOTO (Graduate Student Member, IEEE) received the B.E. and M.E. degrees from The University of Electro Communications, Tokyo, Japan, in 2021 and 2023, respectively. His research interest includes encrypted controls.

KAORU TERANISHI (Graduate Student Member, IEEE) received the B.E. degree in electromechanical engineering from the National Institute of Technology, Ishikawa College, Ishikawa, Japan, in 2019, and the M.E. degree in mechanical and intelligent systems engineering from The University of Electro-Communications, Tokyo, Japan, in 2021, where he is currently pursuing the Ph.D. degree. From October 2019 to September 2020, he was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA. Since April 2021, he has been a Research Fellow with the Japan Society for the Promotion of Science. His research interests include control theory and cryptography for the cybersecurity of control systems.

KEITA EMURA received the M.E. degree from Kanazawa University, in 2004, and the Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST), in 2010. He was with Fujitsu Hokuriku Systems Ltd., from 2004 to 2006. He was a Postdoctoral Researcher with the Center for Highly Dependable Embedded Systems Technology, JAIST, from 2010 to 2012. He has been a Researcher with the National Institute of Information and Communications Technology (NICT), since 2012. Since 2014, he has been a Senior Researcher with NICT, where he has been a Research Manager, since 2021. His research interests include public-key cryptography and information security. He is a member of IEICE, IPSJ, and IACR. He was a recipient of the SCIS Innovation Paper Award from IEICE, in 2012, the CSS Best Paper Award from IPSJ, in 2016, the IPSJ Yamashita SIG Research Award, in 2017, and the Best Paper Award from ProvSec 2022.

KIMINAO KOGISO (Member, IEEE) received the B.E., M.E., and Ph.D. degrees in mechanical engineering from Osaka University, Japan, in 1999, 2001, and 2004, respectively. He was appointed as a Postdoctoral Fellow with the 21st Century COE Program and as an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan, in April 2004 and July 2005, respectively. From November 2010 to December 2011, he was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA. In March 2014, he was promoted to the position of Associate Professor with the Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, Tokyo, Japan, where he has been a Full Professor, since April 2023. His research interests include cybersecurity of control systems, constrained control, control of decision-makers, and their applications.

QualSec: An Automated Quality-Driven Approach for Security Risk Identification in Cyber-Physical Production Systems

Matthias Eckhart, Andreas Ekelhart, Stefan Biffl, *Member, IEEE*, Arndt Lüder, *Senior Member, IEEE*, and Edgar Weippl, *Senior Member, IEEE*

***Abstract*—As the threat landscape in the industrial domain continually advances, security-by-design is an ever-growing concern in the engineering of cyber-physical production systems (CPPSs). Often, quality aspects are not considered when securing CPPSs, which creates attack vectors that could lead to malicious activity affecting the products' quality. Since quality control systems generally provide inadequate protection against intentionally introduced defects, and can be susceptible to attacks, quality considerations must be integrated into security-aware CPPS engineering. For this purpose, we propose the QualSec method that automatically identifies security risks pertaining to CPPSs, building on the quality characteristics associated with manufacturing operations to determine cascading effects. QualSec is based on a semantic representation of engineering knowledge, allowing to efficiently reuse engineering models from AutomationML artifacts. Moreover, QualSec utilizes Petri nets to facilitate the analysis of security risks and cascading effects. In this way, QualSec informs users about possible attack paths for compromising quality characteristics, how attackers may disguise their malicious actions, and the possible consequences of attacks with respect to product quality. We demonstrate the benefits of QualSec in a case study and analyze its scalability through a rigorous performance evaluation.**

***Index Terms*—AutomationML, cyber-physical production systems (CPPSs), industrial control systems (ICSs), information security, petri net (PN), production systems engineering (PSE).**

Manuscript received 9 March 2022; revised 11 June 2022; accepted 5 July 2022. Date of publication 22 July 2022; date of current version 22 March 2023. This work was supported in part by the Austrian Research Promotion Agency (FFG) through the Austrian Competence Center for Digital Production (CDP) under Grant 881843, and in part by Bridge 1 Program under Grant 880609, in part by the Christian Doppler Research Association, in part by the Austrian Federal Ministry for Digital and Economic Affairs, and in part by the National Foundation for Research, Technology, and Development. The COMET Center SBA Research (SBA-K1) was supported by BMVIT, BMDW, and the Federal State of Vienna, through COMET—Competence Centers for Excellent Technologies, and managed by the FFG. Paper no. TII-22-1013. *(Corresponding author: Matthias Eckhart.)*

Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl are with SBA Research, 1040 Vienna, Austria, and also with the Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle, University of Vienna, 1090 Vienna, Austria (e-mail: meckhart@sba-research.org; aekelhart@sba-research.org; edgar.weippl@univie.ac.at).

Stefan Biffl is with the Institute of Information Systems Engineering, TU Wien, 1040 Vienna, Austria, and also with CDP, 1220 Vienna, Austria (e-mail: stefan.biffl@tuwien.ac.at).

Arndt Lüder is with CDP, 1220 Vienna, Austria, and also with the Institute of Ergonomics, Manufacturing Systems and Automation, Otto-von-Guericke U., 39106 Magdeburg, Germany (e-mail: arndt.lueder@ovgu.de).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3193119.

Digital Object Identifier 10.1109/TII.2022.3193119

I. Introduction

SINCE new threats that can compromise the secure and safe operation of cyber-physical production systems (CPPSs) are continuously emerging, managing security risks at the beginning of the systems' lifecycle is paramount. This requires, on the one hand, that the individual engineering activities (e.g., software development and testing [1]), including the exchanged artifacts, are sufficiently protected against adversaries [2]. On the other hand, security must be established as a "first-class citizen" in the engineering process to achieve CPPSs that are secure by design [3]. In the latter case, knowledge from diverse domain experts is essential, given that the engineering of CPPSs is by itself a highly multidisciplinary endeavor. The cyber-physical nature of attacks launched against CPPSs further underlines this need: Attacks executed from cyberspace can lead to physical harm and may endanger human life. Thus, both security and safety concerns need to be considered jointly. In this context, it is worth pointing out that quality is likewise interdependent with security but often not perceived as such. For instance, security risks may manifest themselves as symptoms of a quality control (QC) issue (e.g., data integrity breach due to poor handling of QC logbooks), meaning that addressing this underlying problem could also improve the overall security. Conversely, strengthening the security of a CPPS may also lead to higher quality (e.g., additional sensors put in place to prevent covert product modifications may at the same time unveil defects). Recognizing this interdependence may not only help to promote the fact that information security adds value to an organization (in this case, realized via quality improvements), but also increases the awareness of cyberattacks that focus on the quality of the manufactured products.

The potential severity and multidimensional characteristic of sabotage attacks targeting product quality necessitate a holistic security risk assessment approach that also incorporates quality

1551-3203 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

considerations. However, current risk assessment workflows defined in leading industrial security standards and guidelines (e.g., IEC 62443-3-2 [4] or VDI/VDE 2182-1 [5]) adopt a rather resource-centric view, neglecting the product and process components. This leads to an incomplete understanding of security risks that is also inconsistent with the Product, Process, and Resource (PPR) concept [6], which plays a predominant role in the engineering of CPPSs. In other words, engineers currently consider quality concerns without assuming intentional wrongdoing (i.e., in isolation from security concerns). This isolated view weakens both QCs and security controls.

Moreover, given the vast complexity of designing secure CPPSs, systems integrators need a highly efficient security risk identification method that leverages the data and models that emerge during the engineering process.

The article at hand aims to remedy these pressing issues. Building upon prior work [7], the QualSec method presented in this article interprets the interlinking of PPR engineering information to automatically identify

(i) critical quality characteristics of products,
(ii) attack steps to compromise them, and
(iii) the resulting consequences on the production process.

Since the method can be seamlessly embedded into existing toolchains and makes direct use of already available engineering knowledge contained in AutomationML artifacts, the effectiveness and efficiency of the security risk identification step can be raised significantly. Further, the method automatically generates Petri nets (PNs) that model the sequence of manufacturing processes in a quality-oriented way, allowing to employ reachability analysis that supports risk identification.

The main contributions of this work are as follows:

1) We propose QualSec, that is, a quality-driven method for the automated identification of security risks sourced from engineering models of CPPSs. QualSec draws upon PPR information, including the sequences of manufacturing steps, to thoroughly inform about security risk sources and consequences.
2) We present a quality ontology that contains the QC domain knowledge available in production systems engineering (PSE). This ontology enriches semantics-based security risk assessments and can be interlinked with other ontologies to build knowledge graphs (KGs) for security applications.
3) We introduce the notion of a quality-oriented Petri net (QOPN) to represent the relationships between manufacturing operations, QC steps, and cyberattacks.
4) We provide an open-source implementation of QualSec, test its practicality by conducting a case study, and analyze its scalability via a rigorous performance evaluation.

To the best of our knowledge, this is the first work that considers the relationship between quality and security in a risk identification context with an emphasis on the PPR concept, making it highly relevant to the industrial informatics and information security communities.

The rest of this article is organized as follows. Section II provides background information and discusses related work. In Section III, we motivate the need for quality-driven security risk identification and define the scope of QualSec. Then, in Section IV, we explain the details of our novel method. Section V demonstrates the benefits and practicality of the introduced method by means of a case study. After that, in Section VI, we discuss the results of our performance evaluation. Finally, in Section VII, we conclude our work and give an outlook on future research.

II. Background and Related Work

In this section, we briefly review background information on AutomationML and QC in the context of cyber-physical systems (CPSs) and discuss related work on supporting security-aware CPPS engineering.

A. AutomationML

The Automation Markup Language (AutomationML, hereafter abbreviated as AML) is an XML-based data format that aims to improve the data exchange among heterogeneous engineering tools [8]. This format harmonizes and unifies data models of different engineering disciplines by integrating the Computer Aided Engineering Exchange (CAEX) data format, COLLADA, and PLCopen XML to enable modeling of the topology, geometry and kinematics, and behavior and sequencing of the CPPS [9]. The reason for utilizing AML artifacts to implement the automated identification of quality-driven security risks in CPPSs is threefold: First, AML has been standardized in the IEC 62714 series and gained wide acceptance within the CP(P)S engineering community, many of whom have joined the AutomationML association[1] to develop the format further. Second, the scope of AML far exceeds the mere exchange of information by enabling a model-based engineering approach [10]. Third, the PPR concept fits naturally into the AML architecture as a way of structuring plant models [6]. Thus, the interlinking of information regarding products (e.g., features, quality requirements), processes (e.g., sequencing of manufacturing steps), and resources (e.g., physical and logical objects, networks) can be directly harnessed for risk assessment purposes.

B. Role of QC in CPS Security

Surprisingly, little scholarly work has focused on QC in the context of CPS security thus far. However, of the few works published in this area, we consider the papers by Elhabashy et al. [11], [12] to be most relevant to the article at hand. Elhabashy et al. [11] proposed a taxonomy of cyber-physical attacks involving QC systems, which is composed of

(i) attack objectives,
(ii) targeted components,
(iii) attack methods, and
(iv) attack locations.

Their subsequent work [12] reveals that QC systems may have numerous potential vulnerabilities and shortcomings that attackers can passively exploit (i.e., without changing the QC

[1][Online]. Available: https://www.automationml.org

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

systems themselves). The findings presented in [11] and [12] highlight the importance of adopting a QC perspective when assessing security risks and, therefore, strongly motivate the proposed method.

An interesting observation reported by Wells et al. [13] was that there is a significant need to raise awareness about cyberattacks that have an adverse effect on product quality. Their finding suggests that security needs to be firmly established in the engineering and quality improvement process to become a natural part of the engineer's work. For this reason, our method is designed to allow tight integration into the engineering environment.

Other works, such as [14], [15], analyze sabotage attacks in additive manufacturing (AM) processes. Sturm et al. [14] explored different attack vectors in AM that cybercriminals may use to trick systems into producing faulty products. In particular, they conducted a case study to investigate how `STL` files can be manipulated such that voids inside the produced parts are created. Sturm et al. [14] accentuated that void attacks in AM are typically difficult to detect and may cause a loss of structural integrity. Belikovetsky et al. [15] demonstrated a complete attack scenario involving an AM process, targeting the 3D-printed propellers of a quadcopter. This attack is particularly devious, as the introduced defects remain unnoticed by basic quality checks and cause a critical failure after a certain amount of operating time. Both publications simulate realistic threat scenarios that challenge the state of how product quality issues can be mitigated in the event of an attack, thereby motivating a quality-driven consideration of security risks in CPPSs.

C. Model-Based Security Risk Identification in Cyber-Physical Systems

Several model-driven, risk-based approaches have been proposed in the past years that aim to support the engineering of secure CPPSs. In the following, we briefly summarize the most relevant works.

In [16] and [17], Apvrille and Roudier present an extension for the Systems Modeling Language (SysML) named *SysML-Sec*, which facilitates the model-driven design of safe and secure (sub-)systems (e.g., embedded systems). This extension enables users to incorporate security and safety properties into SysML models, which can then be validated by means of formal verification and simulation. Another security extension for SysML was introduced in [18], which focuses primarily on the architectural aspects of industrial control systems (ICSs), such as CPPSs, rather than the design of the systems' individual components (e.g., a controller). Lemaire et al. [19], [20] have further improved the security-aware, model-based engineering of ICSs by utilizing a formal reasoning framework to automate the identification of security risks in SysML models.

Besides SysML, researchers have also investigated AML for the purpose of extracting relevant information from CPPS blueprints to automate security risk assessments. In [21]–[23], a knowledge-based approach was introduced that applies security rules to AML artifacts in order to discover vulnerabilities in engineering models. These rules were created based on security domain knowledge [24] and modeled with the Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL). In this context, it is worth noting that their approach directly accesses the engineering data in AML without converting it to OWL.

Recently, Eckhart et al. [7] proposed a new method that further advanced this research area. Their method employs an AML-to-OWL transformation mechanism, enabling semantic interlinking, and the use of semantic technologies (e.g., applying semantic reasoning to infer new knowledge). In this way, the method is able to identify threats, vulnerabilities, and consequences automatically by executing a set of queries and rules, which were written in the SPARQL Protocol and RDF Query Language (SPARQL) and the Shapes Constraint Language (SHACL), respectively. The results of the risk identification then serve as an input for the automated generation of attack graphs, which visualize the most critical paths adversaries may take when launching cyberattacks against CPPSs. In this article at hand, we build upon the approach described in [7] to automate the identification of quality-driven security risks in CPPS engineering models.

Finally, it is worth noting that researchers have also applied Petri nets (PNs) for security analysis purposes [25], [26]. Henry et al. [27], [28] employed PNs for attack analysis in the context of ICSs. The authors of [27], [28] then use coverability analysis to determine the extent to which an adversary can gain unauthorized access to resources. Ten et al. [29] used generalized stochastic Petri nets (GSPNs) as part of a framework that aims to quantify the vulnerability of power systems. In comparison to [27]–[29], our proposed method has a clear focus on the quality aspects of the produced parts and provides a significant level of automation in terms of risk identification.

III. Considered Attack Scenario and Scope of QualSec

The attack model considered in the article at hand assumes resourceful adversaries capable of remaining under the radar until defective products caused by intentional sabotage slip through QC and are shipped to customers. Based on a casual review of past cyberattacks against CPPSs, we sketch a realistic scenario in which threat actors either gain their initial foothold within the business network and then pivot to the control system network or directly gain unauthorized access to control devices via unprotected remote maintenance services. Furthermore, we assume that adversaries attack the CPPS at the weakest point they can find, which commonly coincides with exploiting publicly known vulnerabilities. The objective of attackers is to compromise manufacturing systems during operation in order to cause product quality issues deliberately. From an attacker's perspective, overcoming QC that functions as a defense against such attacks can be achieved in two ways: Either by manipulating the products' quality characteristics selectively, affecting only those which are not subject to quality inspection, or by exploiting QC vulnerabilities [12] to avoid detection of malicious product alterations.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

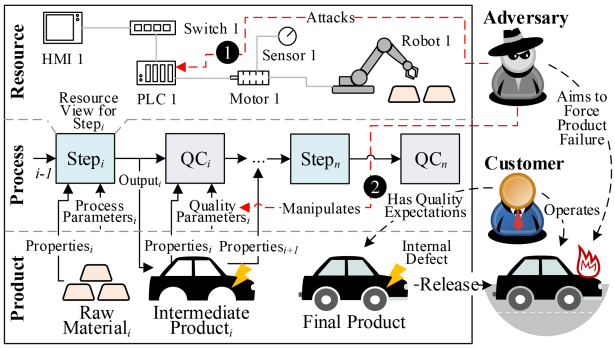


Fig. 1. Attack scenario targeting the products' quality.

Fig. 1 illustrates an example scenario in which an adversary attacks a vulnerable programmable logic controller (PLC) ① in a car manufacturing process. Since the compromised PLC controls a spot welding robot, the adversary can induce subtle changes in the welds, resulting in loss of product integrity (e.g., poor durability of the produced car body) and eventual failure of the vehicle. The consequence of this cyber-physical attack remains undetected throughout the manufacturing process as subsequent inspection for the purpose of QC can be evaded. The reason for this is that QC systems are typically not designed to uncover issues that have been created with malicious intent [13]. Even if the implemented QC checks would detect malicious product changes, an adversary may also exploit the QC systems to manipulate quality parameters (e.g., inspection locations, thresholds) ②, ensuring that any modifications go unnoticed [12]. Furthermore, increasing the defect rate and disrupting production processes constitute additional attack objectives that adversaries may pursue [11].

Our novel method, named QualSec, aims to automate tasks of the risk identification step that are carried out as part of security risk assessments during the engineering of CPPSs. One of its core features is to incorporate the semantics, structure, and sequence of the manufacturing process to identify

(i) product quality characteristics that attackers may compromise, and
(ii) possible propagation effects thereof.

To illustrate the scope and purpose of our contribution, we define the following set of questions.

Q1 *What are the security vulnerabilities in assets of CPPSs that threats may exploit?*
The first question aims to uncover architectural security weaknesses and vulnerabilities in systems that are intended to be integrated into the plant topology. Answers to this question build upon public sources, such as Common Vulnerabilities and Exposures (CVE), security advisories, and industrial security standards and guidelines. We repurpose the method presented in [7] to enable a quality-driven consideration of cyber-physical risk that is realized by answering the next questions.

Q2 *Given a set of vulnerable assets, which quality characteristics of the workpiece or product can attackers deliberately alter, and would these defects remain undetected due to insufficient QC?*
Based on the answer given to Q1, this question aims to inform engineers about potential consequences on product quality that may be caused by an adversary, who exploits vulnerable assets to execute such sabotage attacks. Answers to this question provide engineers guidance on how to prioritize risks.

Q3 *What are the consequences of an attack that targets a certain quality characteristic in terms of cascading effects relating to product quality?*
Similar to the previous question, Q3 focuses on the quality characteristics that adversaries may be able to influence in the course of an attack. However, as the sequence of manufacturing steps can create dependencies among quality attributes (e.g., diameter and location of drilled pilot holes must be correct for subsequent joining), this question places special emphasis on the indirect effects of sabotage attacks. As a result, engineers can quickly spot critical quality characteristics whose malicious alteration would lead to a chain reaction.

Q4 *How can attackers disguise their malicious actions to evade QC?*
Finally, the last question addresses the case, where an adversary might attempt to attack those QC systems that would catch product defects caused by prior manipulations of quality characteristics. Informing engineers about the minimal set of assets needed to be hacked to bypass the QC in place may provide guidance on prioritizing the systems to be hardened.

IV. Method

An overview of our proposed method and its steps is shown in Fig. 2. In the course of engineering CPPSs, professionals from various disciplines design and model systems using specialized tools. The created engineering artifacts are managed in the AML format to facilitate data exchange. In step ①, engineers annotate the plant topology contained in the AML document with security- and quality-relevant information using the AML extension libraries (AMLsec and AMLqual). Step ② transforms both the plant topology and the description of the manufacturing process to OWL. Step ③ builds the Knowledge Base (KB) by connecting the semantic representation of the plant topology and production process with additional know-how from the security ontology [30], the ICS security ontology [7], the quality ontology, and linked open security data. Based on the process description contained in the KB, step ④ generates the quality-oriented Petri net (QOPN). Finally, step ⑤ automatically performs the quality-driven security risk identification by executing rules and queries against the KB and analyzing the QOPN.

Before, we explain each element of QualSec in detail, we state the assumptions that the QualSec method relies on:

1) *Risk Identification at Design Time:* As the purpose of QualSec is to reveal security risks in the CPPS during the engineering process, we only consider what the QC system can check at design time.
2) *Model of the Manufacturing Process:* It is assumed that the manufacturing process is modeled in the sequential

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

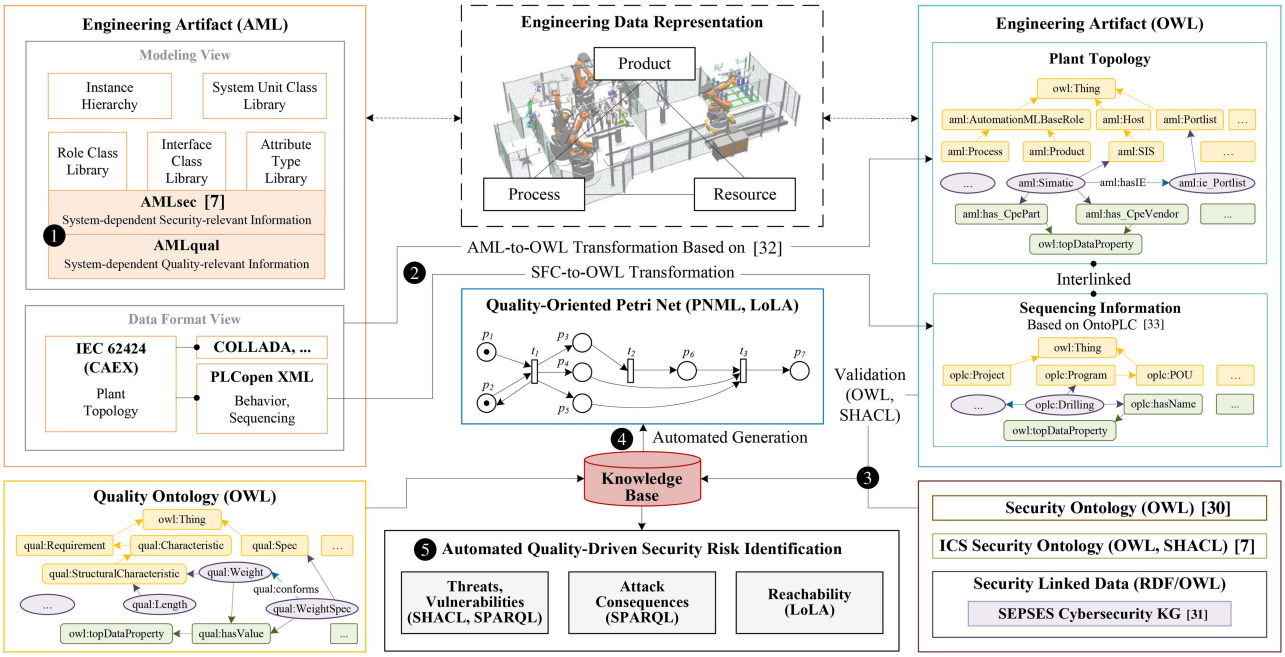


Fig. 2. Overview of QualSec, the quality-driven security risk identification method (based on [7]; robot cell illustration in [34]).

function chart (SFC) language in line with the PLCopen XML specification. To construct the QOPN, we only consider the structure of the SFC network, which can be represented graphically. Other elements of the SFC language, as standardized in the IEC 61131-3, are not relevant to QualSec.

3) *State of a System is Binary:* If an attack against a production system succeeds, it is assumed that the adversary gains full control and can manipulate all quality characteristics that the compromised system can influence during the respective manufacturing step. Similar reasoning applies to QC systems and the outcome of quality checks.
4) *Quality Measurements are Performed In-Line:* Since QualSec incorporates the description of the manufacturing process, we only consider QC efforts that are undertaken along the production line and are modeled as such. Offline quality checks could be accommodated by manually extending the semantic representation of the manufacturing process.

A. Engineering Data Representation

To lift the engineering models contained in AML artifacts to ontologies, we rely on the semantics expressed via AML's libraries of role classes (`RoleClassLib`), interface classes (`InterfaceClassLib`), and attribute types (`AttributeTypeLib`). More precisely, we link the semantics of components modeled in AML to an equivalent representation maintained in our ontologies. The normative libraries specified as part of AML are primarily used for this purpose, thereby reducing the additional modeling effort required to use QualSec. However, certain security-relevant modeling constructs that would significantly enhance QualSec's analysis capabilities are missing in those standard libraries. To overcome this limitation, we reuse AMLsec [7], which comprises libraries that engineers can apply to model security-relevant information (e.g., zones, network protocols, security devices). We carry the idea of realizing semantic matching one step further and introduce a set of libraries named AMLqual that engineers can use to augment their model with quality-relevant information. For example, `AMLqualRoleClassLib` includes, *inter alia*, role classes for QC methods (e.g., ultrasonic testing), to enrich the semantics of `InternalElements` that model the QC system.

Another vital aspect of QualSec is the interlinking of engineering information according to the PPR concept, which can be fully accommodated within the AML format [6]. According to the AML standard, links between modeled products, processes, and resources are established by using an `ExternalInterface` named `PPRConnector`, which is part of the `AutomationMLInterfaceClassLib`. Furthermore, objects within the logic model (i.e., the SFC program), which contains the sequencing information of the manufacturing process, are referenced from CAEX in the usual AML-way by using `LogicElementInterfaces`.

B. Ontological Modeling

As shown in Fig. 2, the KB is composed of the semantically lifted engineering model (i.e., plant topology and sequencing information), the (ICS) security ontology, the quality ontology, and the security-related linked data.

The CAEX-based plant topology within the AML artifact is transformed to OWL using the translation procedure of Hua

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

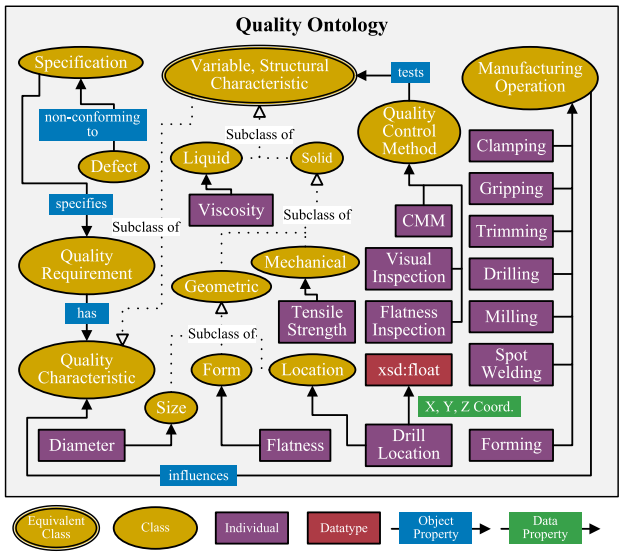


Fig. 3. Visualization of the quality ontology (excerpt).

and Hein [32]. To incorporate the PLCopen XML data into our KB, we have implemented an SFC-to-OWL transformation that instantiates an ontological model from OntoPLC [33]. After lifting the AML artifact to a semantic representation, we perform validation checks using SHACL and then automatically augment the engineering knowledge with security- and quality-specific know-how.

The structure of the security knowledge follows a layered approach, where the middle ontology layer is realized by the security ontology [30] that models rather abstract concepts within the information security domain. The ICS security ontology expands this basic knowledge with information obtained from system-independent (e.g., security standards and guidelines) and system-dependent (e.g., technical requirements of CPPSs) sources. Furthermore, the semantic data model within the KB is interlinked with the *SEPSES Cybersecurity KG* [31] in order to include the latest information on publicly disclosed security issues.

Another vital component of QualSec is the quality ontology. We have designed a comprehensive ontology for the QC domain to capture the knowledge of quality characteristics, methods to check them, and manufacturing processes that influence them (cf. Fig. 3). The rationale behind the quality ontology is to create semantic relations between the PPR information from the engineering model and QC domain knowledge. In this way, we can derive the information that is required to construct the QOPNs that enable quality-driven security risk identification.

To answer Q1, we apply a set of SHACL rules and SPARQL queries that are executed against the KB, yielding risk sources (i.e., threats and vulnerabilities) and attack consequences (i.e., violation of security or safety goals).[2] The employed vulnerability detection rules can be categorized into two classes: First, node and property shapes are used to implement a validation procedure that checks for security weaknesses in the modeled elements of the plant topology (e.g., insecure network protocols and cryptographic algorithms, configuration vulnerabilities). Second, SPARQL-based constraints are employed to detect violations of zone and conduit requirements (ZCR-3.2–3.6) as per the IEC 62443-3-2 [4]. Additionally, we perform a CVE check check by using the SEPSES Cybersecurity KG [31] to determine if the systems intended to be integrated into the plant are affected by known (public) vulnerabilities.

[2]For a more detailed description of this approach, we refer readers to [7].

C. Quality-Oriented PNs

The identification of risks to product quality and consequential events is based on the results of constructing and analyzing PNs that model manufacturing processes. The PN [35] is a well-established formalism with decades of research behind it and represents a convenient tool to model discrete event systems (DESs). In the following, we introduce the notion of QOPNs, specify a generation method for QOPNs, and explain how QOPNs can be analyzed to support the identification of security risks.

1) Preliminaries: Following the definitions given in [36], a marked PN is defined as a 5-tuple (P, T, A, w, x), where (P, T, A, w) is a weighted bipartite graph comprising a finite set of places P, a finite set of transitions T, a set of arcs $A \subseteq (P \times T) \cup (T \times P)$, and a weight function on the arcs $w : A \to \{1, 2, 3, \dots\}$. Further, x is a marking of the set of places that is associated with a row vector $\mathbf{x} = [x(p_1), x(p_2), \dots, x(p_n)] \in \mathbb{N}^n$. The marking row vector $\mathbf{x}$ defines the state of the PN and a transition $t_j \in T$ is enabled, if and only if, $x(p_i) \geq w(p_i, t_j)\ \forall p_i \in I(t_j)$, where $I(t_j) = \{p_i \in P : (p_i, t_j) \in A\}$.

Recall that QualSec incorporates a formal representation of the manufacturing process that is first translated from SFC to OWL and then processed further to construct a QOPN. The beauty of QOPNs is that they capture the dependencies among process steps, quality characteristics, and attacks against them, leading to an enhanced understanding of propagation effects.

In general, a manufacturing process consists of n production steps $o_1, \dots, o_n$ that are executed by m production systems to fulfill l jobs. Each production step o influences h characteristics of the machined part or product, which are then checked by k QC steps to determine whether they meet their stipulated quality specifications. Since the quality-driven security risk identification is performed from a process-centric point of view, the QOPN is based on the process-oriented Petri net (POPN) [37]. In a POPN, a place represents the status of a resource or job order, or an operation, while a transition denotes either the start or end of an operation [37]. The QOPN is a classical PN (P, T, A, w, x), as defined above, that extends the notion of the POPN. In Table I, we assign meaning to P and T to ensure proper interpretation of QOPNs.

It is worth reiterating that we do *not* aim to fully translate SFC programs in their complete form to PNs or one of the PN dialects. Instead, we utilize the sequencing information expressed via the SFC structure, which encodes the description of the manufacturing process, to construct QOPNs that aid security risk identification.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

TABLE I
NOTATION AND SEMANTICS OF QOPNS

Places

P = $\bigcup_{i=1}^{13} S_i$, $S_i \cap S_j = \varnothing$ for all $i, j \in \{1, \ldots, 13\}, i \neq j$, where
S_1 = $\{o_1, \ldots, o_n\}$ is a set of places denoting production steps,
S_2 = $\{r_1, \ldots, r_v\}$ is a set of places denoting the status of resources (i.e., production system or QC system ready), $v = m + k$,
S_3 = $\{u_1, \ldots, u_v\}$ is a set of places denoting that resources are vulnerable,
S_4 = $\{\bar{u}_1, \ldots, \bar{u}_v\}$ is a set of places used as a complement to S_3 (i.e., resources are *not* vulnerable),
S_5 = $\{y_1, \ldots, y_m\}$ is a set of places denoting that manipulating one or multiple quality characteristics through a compromised production system has been completed,
Q_o = $\{q_1, \ldots, q_h\} \in S_6$ is a set of places denoting quality characteristics influenced by production step o,
$\bar{Q}_o$ = $\{\bar{q}_1, \ldots, \bar{q}_h\} \in S_7$ is a set of places denoting that quality characteristics, which are influenced by production step o, have been compromised,
S_8 = $\{c_1, \ldots, c_k\}$ is a set of places denoting QC steps,
S_9 = $\{a_1, \ldots, a_{k*2}\}$ is a set of places denoting whether a defect has been detected by a QC system,
S_{10} = $\{z_1, \ldots, z_k\}$ is a set of places whose user-defined markings predefine that the corresponding (benign) QC system would detect any maliciously introduced defects,
S_{11} = $\{\bar{z}_1, \ldots, \bar{z}_k\}$ is a set of places used as a complement to S_{10},
S_{12} is a set of auxiliary places to model various structures (e.g., XOR-joins), and
S_{13} = $\{s, f, d\}$, where s is a place denoting the job order status, f is a place denoting the finished product, and d is a place denoting the defects.

Transitions

T = $\bigcup_{i=1}^{7} G_i$, $G_i \cap G_j = \varnothing$ for all $i, j \in \{1, \ldots, 7\}, i \neq j$, where
G_1 = $\{\alpha_1, \ldots, \alpha_{n*2}\}$ is a set of transitions denoting the start or end of a production step,
G_2 = $\{\beta_1, \ldots, \beta_{k*3}\}$ is a set of transitions denoting the start or end of a QC step (includes two variants of the end step to cover defect and no defect conditions),
G_3 = $\{\gamma_1, \ldots, \gamma_m\}$ is a set of transitions denoting attacks against production systems,
G_4 = $\{\delta_1, \ldots, \delta_{k*2}\}$ is a set of transitions denoting whether a QC system successfully detected a defect ($\delta^{\dagger}$) or failed to detect it ($\delta^{\ddagger}$) assuming that neither the QC system nor any quality characteristic under test was compromised beforehand,
G_5 = $\{\epsilon_1, \ldots, \epsilon_{k*2}\}$ is a set of transitions denoting whether a QC system detected a defect ($\epsilon^{\dagger}$) or did not detect it ($\epsilon^{\ddagger}$) after a quality characteristic was compromised (yet, the QC system itself remained intact),
G_6 = $\{\zeta_1, \ldots, \zeta_{k*2}\}$ is a set of transitions denoting whether a compromised QC system was manipulated in a way to suppress the detection of a maliciously introduced defect ($\zeta^{\dagger}$) or to detect a non-existent defect with the objective to waste material ($\zeta^{\ddagger}$), and
G_7 is a set of auxiliary transitions (similarly to S_{12}).

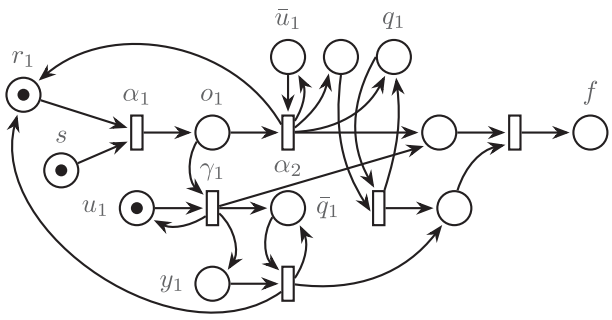


Fig. 4. Minimal QOPN (unlabeled nodes $\in S_{12} \cup G_7$).

2) Modeling and Construction: A QOPN is composed of one or multiple QOPN templates that are assembled according to the formal process description at hand. To achieve a valid QOPN, the SFC model to be transformed must at least contain the sequence *Initial Step* $\rightarrow$ *Production Step* $\rightarrow$ *Terminal Step*, which leads to the template shown in Fig. 4.

The minimal QOPN depicted in Fig. 4 contains only one quality characteristic, q_1, and is shown in its initial state, where

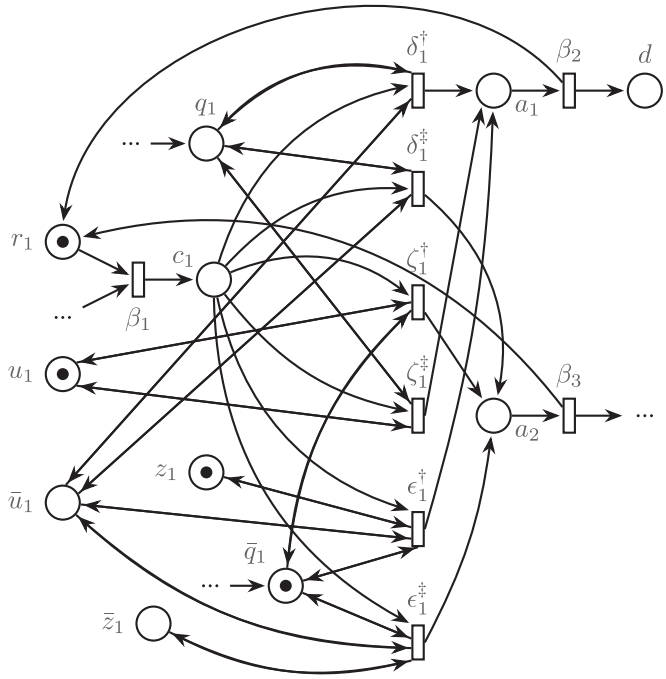


Fig. 5. QOPN template for a QC step with a single quality characteristic under test.

$x(u_1) = 1$ and $x(\bar{u}_1) = 0$ (the complement of $x(u_1)$) were specified arbitrarily for demonstration purposes. Note that the initial state of the generated QOPN depends on prior results of the vulnerability analysis (in particular, to denote vulnerable resources) and optionally on user input (e.g., to predefine the outcome of a QC step). Furthermore, a sequence of manufacturing operations may be followed by one or multiple QC steps to check whether the involved quality characteristics meet the specified requirements. This case is covered by the QOPN template shown in Fig. 5. Owing to the sets G_4, G_5, G_6, and the PN structure given in Fig. 5, various attack scenarios involving QC systems can be modeled. Again, the QOPN depicted in Fig. 5 includes only one quality characteristic, and $x(u_1) = x(z_1) = x(\bar{q}_1) = 1$, as well as $x(\bar{u}_1) = x(q_1) = x(\bar{z}_1) = 0$, were specified arbitrarily for the purpose of illustrating the PN structure.

The templates were designed to ensure boundedness of the constructed QOPN, that is, $\forall \mathbf{x} \in \mathsf{Reach}(QOPN), \forall p \in P : x(p) \leq \kappa$, where $\mathsf{Reach}(QOPN)$ is the reachable state set of the QOPN and κ is a positive number. This property is an essential requirement for applying reachability-based analysis techniques due to the fact that the PN's reachability graph must be finite.

3) Analysis: To answer Q2 and Q3, we reformulate these questions as reachability queries on QOPNs in Computation Tree Logic (CTL). The formulae for checking the desired reachability properties are expressed as EFϕ, where the state predicate ϕ takes the following forms:

Q2 $((\exists s \in \mathcal{S} : \lambda(s) > 0) \wedge (f > 0))$, where $\mathcal{S} = \{u \in S_3 \mid x(u) = 1\}$ and λ is a relation from $\mathcal{S}$ to S_7. Informally, we describe this reachability problem as follows: Is it possible that the manufacturing process

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

finishes without detected defects, even though some quality characteristics were compromised by exploiting vulnerable assets? After checking reachability, we analyze and filter the witness states to obtain a subset of S_7 that provides an answer to this question.

Q3 $((\exists s \in \mathcal{S} : \lambda(s) > 0) \wedge (f > 0))$, where $\mathcal{S} = \{\bar{u} \in S_4 \mid x(\bar{u}) = 1\}$ and λ is a relation from $\mathcal{S}$ to S_7. This reachability problem can be understood as checking if the manufacturing process may finish without detected defects, while some quality characteristics were indirectly compromised by exploiting vulnerable assets in preceding manufacturing steps. Similarly to Q2, we process the witness states after reachability checking to answer this question.

Q4 cannot be answered with a single reachability query and requires an iterative procedure, as shown in Algorithm 1. This algorithm takes a generated QOPN as input and produces a set U', which is a proper subset of S_3 containing places that correspond to resources of QC systems that need to be vulnerable and successfully compromised to evade quality checks. After initializing the result set U' and the set $\mathcal{T}$ that will contain transitions demonstrating the execution path starting from the initial marking, the state predicate ϕ is defined. Since we want to check if there is an execution path, where a product defect is found during a QC inspection, we define the state predicate such that the number of tokens on the place d denoting the detected defects is greater than zero. Based on this, the reachability query is expressed in CTL as the following formula: $\mathrm{EF}(d > 0)$. As long as there is a reachable state satisfying ϕ, the body of the loop is executed. In line 5, $\mathcal{T}$ is filled with the witness path, which is then processed in reverse: In each iteration, it is checked if the current element in the loop is a member of ${G^\dagger}_5$ (i.e., the transition denotes the detection of a defect). In the body of the `if`-statement, we retrieve the place denoting that the resource of the QC system that detected the defect is vulnerable, add it to the result set, retrieve the complementary place (i.e., resource not vulnerable), and adapt the marking such that the QC system is now indicated as vulnerable. Note that the procedure outlined in Algorithm 1 presupposes that at least one quality characteristic can be compromised through the exploitation of a vulnerable asset employed for a production step, since an answer to Q4 should reveal which QC system(s) an adversary would need to manipulate in order to conceal introduced product defects.

Algorithm 1: Reachability Analysis for Q4.

Input: A QOPN $N \leftarrow (P, T, A, w, x)$
Result: A subset of places of N corresponding to resources that need to be compromised in order to disguise an attack on product quality $U' \subset S_3$

```
1  U' ← ∅                                   // result set
2  T ← ∅                                    // witness path set
3  φ ← (d > 0)                              // state predicate
4  while N satisfies EFφ do
5      T ← GetWitnessPath()
6      for i ← |T| to 1 do
7          if T(i) ∈ G†5 then
8              u_i ← GetResourcePlace(T(i))
                                            // vulnerable resource
9              U' ← U' ∪ {u_i}
10             ū_i ← GetComplementaryPlace(u_i)
11             x(u_i) ← 1; x(ū_i) ← 0
12             break
```

D. Implementation

We created the AMLqual libraries with the AutomationML Editor.[3] The quality ontology was modeled with Protégé[4] [38]. Since we build upon the results of Eckhart et al. [7], we have extended their prototype to incorporate our quality-driven risk identification method. In particular, we have implemented the SFC-to-OWL translation, the QOPN construction, and the export to Petri Net Markup Language (PNML) and LoLA file formats in Scala. To conduct reachability analyses, which is an integral part of QualSec, we utilize LoLA 2 [39], [40].

AMLqual, the source code of the implemented prototype, and the AML files used for the case study are publicly available on GitHub.[5]

V. Case Study

This section presents the results of a case study that was conducted to showcase QualSec. The engineering data used in the case at hand is based on the official AML example of a robot cell [34], which aims to demonstrate how AML can be used to model the topology, behavior, and geometry of a robotic spot welding cell. To obtain a more comprehensive model, we extended these artifacts in the following ways:

(i) A description of a stamping process was integrated into the existing SFC (which only models the sequence of joining activities).
(ii) The plant topology was supplemented with PPR relations and communication-related information.
(iii) IT/OT assets were populated with system-dependent, security- and quality-relevant information using AMLsec and AMLqual.

The process considered in the case study comprises activities of vehicle manufacturing. More precisely, we focus on the stamping and joining processes for the inner front door panel, which represent a crucial part of the body in white (BiW) production line. It is evident that the structural characteristics of closures strongly influence the quality of the complete BiW; hence, conducting a quality-driven security analysis already during the engineering of the involved CPPS is prudent.

Fig. 6 illustrates the manufacturing steps from a PPR-centric perspective, where the process view is modeled in the SFC language. Due to space limitations, we cannot present an illustration of the plant topology considered in the case study. We, therefore, refer readers to the web version of the figure.[6]

[3][Online]. Available: https://www.automationml.org/download-archive
[4][Online]. Available: https://protege.stanford.edu
[5][Online]. Available: https://github.com/sbaresearch/amlsec
[6][Online]. Available: https://github.com/sbaresearch/amlsec/blob/master/appendix/qualsec/plant-topology.pdf

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

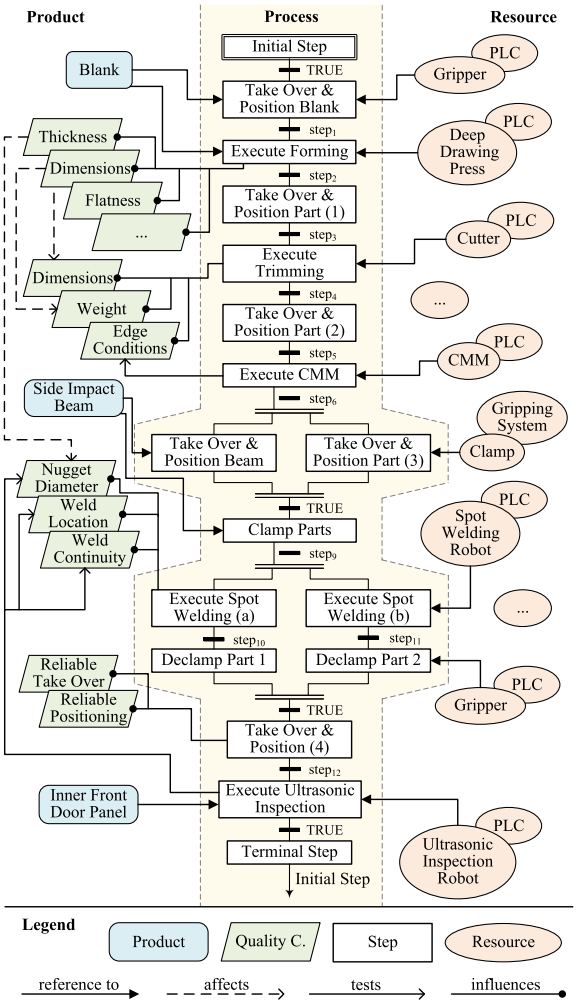


Fig. 6. PPR-centric view of the manufacturing process considered in the case study (gripping and positioning operations are combined into a single step for the sake of brevity).

TABLE II
EXCERPT OF THE QUALSEC ANALYSIS RESULTS

Legend:
vulnerable asset
■ pertains operation or QC
▲ compromised
⊛ affected by compromised qual.
covered by QC
QC evasion

Step	Asset		Quality Characteristics: Edge Conditions	Dimensions	Weight	Thickness	Nugget Diameter	Weld Continuity
Forming	S71516F_7	●	▲	▲	▲	▲		
Trimming	S71518_1	○	■	⊛	⊛			
CMM	S71518_2	○	■					
Spot Welding (a)	KRC4_1	○				⊛	■	
Spot Welding (b)	KRC4_2	○					■	
Ultrasonic Insp.	S71516F_11	●					■	

A. Results

In the following, we describe the most important results that we obtained by executing the QualSec prototype with the described input of the case study:

Q1 The results of the threat, vulnerability, and consequence identification indicate that 47 of the 370 assets of the plant topology (67 of which have the class OTComponent) have 193 vulnerabilities that may be exploited by 9 distinct threats, possibly leading to 80 consequences.

Q2 The CVE check revealed that the PLC `S71516F_7`, which controls the deep drawing press, has a known vulnerability. If this vulnerable asset is compromised, the sheet metal forming step could be influenced to manipulate several quality characteristics of the stamped pieces, including their thickness, dimensions, and edge conditions. Possible defects resulting from this attack would remain undetected because the employed coordinate-measuring machine (CMM) only tests the edge conditions of the trimmed pieces.

Q3 Since the subsequent manufacturing operation relies on the correct dimensions of the formed blanks, an attack launched against the deep drawing press could also affect the dimensions and weight of the trimmed parts. Furthermore, an incorrect blank thickness would require a different size of the weld nugget formed as part of the spot welding step. Although the nugget diameter is checked through ultrasonic testing, the PLC `S71516F_11` controlling the spot welding quality inspection robot is vulnerable and can therefore be circumvented if successfully attacked.

An excerpt of these results is displayed in Table II. In a second iteration, the plant topology has been adapted based on the answers to Q1–Q3 given above to make the CPPS more resilient. More specifically, the vulnerability in `S71516F_11` has been mitigated and the CMM now also tests the dimensions of the stamped and trimmed parts.

Q4 To validate if the performed adaptations yield a security improvement, we execute the reachability analysis outlined in Algorithm 1, intending to identify those QC assets that potentially detect malicious product changes. The results showed that an attack against the deep drawing press could only be disguised by compromising the PLCs `S71518_2` and `S71516F_11`, which control the CMM and ultrasonic testing robot, respectively. Ideally, these devices are hardened to detect attacks that target the product quality.

B. Discussion

In the following, we reflect on the results of the case study and critically evaluate the usefulness of QualSec. To this end, we briefly reiterate the gaps in the literature and analyze how well QualSec achieves its goals to address them.

1) *Efficient Security Risk Identification:* Systems integrators are in need of a method that assists engineers in addressing security issues during the integration phase [2]. Our work is based on [7], which represents a first step toward a fully automated identification of security risks using engineering data. We improved the method proposed in [7] by incorporating the model of the manufacturing process

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

(i.e., sequencing information) into our KB to enrich its results. In this way, the security vulnerabilities identified for answering Q1 can be associated via PPR links to individual steps of the manufacturing process, which may support risk analysis and risk evaluation. However, note that the vulnerability analysis operates at the plant topology level. This limits the scope of analysis to the plant model and public sources (e.g., industrial security standards, advisories, CVEs). Furthermore, we only consider the structure of SFC programs to construct PNs (more specifically, QOPNs), whereas other transformation techniques (e.g., [41]) provide more comprehensive coverage.

2) *QC and Security:* One of the first serious discussions of the relationship between QC and CPS security appeared in 2018 when Elhabashy et al. [11] proposed a cyber-physical attack taxonomy featuring a QC perspective. In a later work [12], they identified weaknesses in QC systems that adversaries might exploit to conceal the physical effects of attacks. Both works [11], [12] emphasize the necessity of taking QC aspects into account when designing CPPSs in order to make them more resilient to such attacks. QualSec aims to address this need by providing a risk-based approach that helps engineers better understand the impact of potential cyber-physical attacks in terms of product quality. The answers to Q2 and Q3 obtained through QualSec allow users to pinpoint compromised quality characteristics of workpieces in attack scenarios and analyze the dependencies among them. The method's results also indicate under which conditions the QC systems included in the plant topology could potentially detect malicious product changes. Since QualSec is intended to be used as a risk identification tool by systems integrators, its assessment scope is limited to the hierarchical structure of the plant, and it assumes the reasonable worst case. In other words, the presented method was not specifically designed to identify security issues in fine-grained system models (e.g., described in SysML) that would allow for a meaningful representation of vulnerability preconditions and postconditions. Thus, QualSec neglects the product supplier perspective entirely.
3) *What-If Scenarios:* Engineers can use QualSec as a planning tool to perform what-if analyses that allow a safe simulation of attack scenarios involving malicious quality loss. QualSec's results for Q4 help defenders to determine potential chokepoints in the designed QC program that would allow adversaries to bypass QC systems if they are not adequately secured.

VI. Performance Evaluation

The performance and scalability of the prototypical implementation were measured through multiple tests that were carried out using different-sized engineering models (cf. Table III). The smallest dataset (A) corresponds to the engineering model that was used for the case study, which contains the plant topology for one site[7] and the corresponding logic model depicted in Fig. 6. For datasets B–F, we expanded the base model by increasing the number of sites (Vienna `InternalElement`) and the process description (SFC) in steps of two.

TABLE III
Overview of the Datasets Used for the Evaluation

	A	B	C	D	E	F
Engineering Data						
`InternalElements` (in K)	0.87	1.74	3.49	5.23	6.97	8.71
AML Size (in MB)	1.00	2.00	4.00	6.00	8.10	10.10
Steps in SFC	23	44	86	128	170	212
After AML & SFC Trans.						
Triples (in K)	18.96	34.01	64.09	94.17	124.26	154.34
Knowledge Base Size (in MB)	2.20	4.00	7.60	11.20	14.80	18.40
After Method Execution						
Triples (in MM)	0.06	0.12	0.32	0.60	0.97	1.42
Knowledge Base Size (in MB)	5.50	11.90	30.70	57.40	92.00	134.60
QOPN Places (in K)	0.23	0.46	0.91	1.36	1.81	2.26
QOPN Transitions (in K)	0.12	0.24	0.47	0.71	0.95	1.18
QOPN Arcs (in K)	0.75	1.50	3.00	4.50	6.00	7.50
Assets (in K)	0.37	0.74	1.48	2.22	2.95	3.69

We measured the execution time of 60 experiments that were conducted by performing five runs per dataset with two cluster configurations. The first cluster consisted of the following three nodes: Node 1 hosted the triple store (Apache Jena Fuseki), a database for storing events (Apache Cassandra), and actors to provide a front-end and manage work items. Nodes 2 and 3 were used to run the work executor actors that perform the actual QualSec method. The second cluster consisted of two additional work executor nodes (i.e., five nodes in total). All nodes of both cluster configurations were cloud-hosted virtual machines running Fedora 35 x64 with 16 vCPUs and 32 GB RAM.

Fig. 7 summarizes the performance evaluation. In Fig. 7(a), we show the average execution time of the main steps of the setup phase (viz., AML-to-OWL transformation, SFC-to-OWL transformation, and model augmentation), the generation of the QOPN, and the reachability analyses for answering Q2–Q4. Note that these reported measurements were made with both cluster configurations (i.e., 10 runs per dataset) since the respective tasks were not processed in parallel by multiple work executor actors. The average execution time for the risk identification logic and the QualSec method in total are plotted per cluster setup in Fig. 7(b) and (c), respectively.

Building upon earlier work [7], we answer Q1 by executing a set of SPARQL queries and SHACL rules. Consequently, the performance of the threat, vulnerability, and attack consequence identification depends on the following factors:

1) The implementation of the SPARQL, SHACL, and inference engines.
2) The executed queries and rules.
3) The size and structure of the semantic data.

As can be seen from Fig. 7(b), scaling out the QualSec application with additional work executor nodes in a cluster

[7]See footnote 6.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

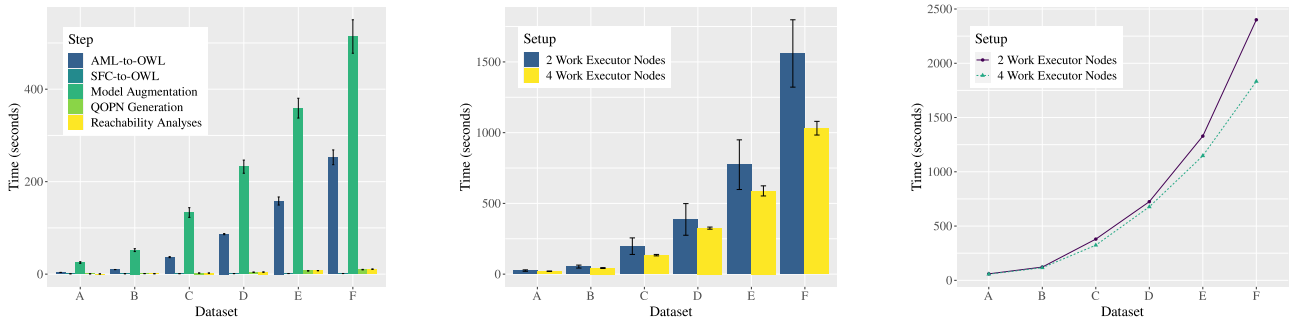


Fig. 7. Performance assessment results of our implemented prototype (error bars indicate standard deviations). (a) Setup, QOPN generation, case study. (b) Validation and risk identification. (c) Total.

can yield considerable performance improvements, especially for larger datasets.

Due to the fact that answering Q2–Q4 necessitates the construction of reachability graphs, the presented method suffers from the well-known *state explosion problem* [42]. Thus, albeit the reachability graphs are finite given the boundedness of QOPNs, the size of the state space can be unmanageable. Increasing the practicality of reachability analysis of PNs is a long line of research that has spawned various techniques to reduce the state space (e.g., stubborn sets [43]). LoLA [40] implements, inter alia, partial order reduction (the stubborn set method) and symmetry reduction, which can also be applied in combination [44]. We observe that the state space reduction techniques implemented in LoLA [40] alleviate state explosion, at least to the extent that Q2–Q4 can be answered within reasonable time (avg. 0.51 ± 0.03 s for dataset A). In fact, as can be seen from Fig. 7(a) and (b), the execution time of the QOPN generation mechanism and reachability analysis to answer Q2–Q4 is negligible compared to the security risk identification phase that answers Q1.

VII. Conclusion

In this article, we have presented a method named QualSec that automates the identification of security risks pertaining to CPPSs based on engineering data. The novelty of QualSec was that it stimulates a quality-driven perspective on security that places special emphasis on the quality characteristics of the manufactured products. Our proposed method can reveal security issues in the plant topology and expose weaknesses in QC that adversaries may exploit to introduce defects during manufacturing deliberately. QualSec utilizes PPR knowledge modeled in CAEX and SFC as part of AML to create a semantic KB. Threats, vulnerabilities, and attack consequences are then automatically identified by executing several SHACL rules and SPARQL queries against the KB. Furthermore, the structure of the modeled manufacturing process was used to construct a QOPN automatically. This QOPN serves as a basis for reachability analysis to answer risk-related questions. Systems integrators can apply QualSec to initiate proper mitigation of security risks during the engineering phase. The resulting CPPSs may be more secure by design and thereby inhibit attackers from compromising the quality of manufactured goods, possibly contributing to a decline in the number of faulty products entering the market.

Further research should be undertaken to improve QualSec in the following ways: The current version of our method is intended to be used during the engineering of CPPSs and, therefore, heavily relies on the engineering data exchange format AML. However, since a QOPN is constructed based on a semantic representation of the production process, the input format does not necessarily have to be PLCopen XML. Incorporating additional sources into QualSec would extend the method's scope to cover the operation phase.

Another possible improvement of QualSec would be to increase the degree of detail of the systems' state. In this article, we make the (relatively strong) assumption that the successful exploitation of a vulnerability results in full control of the system and allows an adversary to manipulate all quality characteristics that the compromised system can influence. The rationale behind this assumption is twofold:

(i) The abstraction level of the plant model available at the engineering phase may hinder the definition of postconditions of exploiting vulnerabilities.

(ii) Users might be primarily interested in worst-case scenarios.

Nevertheless, enriching the KB may enable a finer-grained analysis of how quality characteristics can be influenced based on the privileges gained by an adversary.

There is also room for improvement with respect to the engineering data sources used for risk identification. In its current version, QualSec processes the plant topology in CAEX and the sequencing information in PLCopen XML, which are both part of AML. Utilizing COLLADA interfaces to incorporate geometry and kinematics information into QualSec appears to be an appealing extension of our work. In this way, the attack consequence identification component could be enhanced to address safety aspects more thoroughly.

Finally, we want to suggest some ideas to advance the PN-based analysis further. Probabilistic PNs may be applied to better reflect various quality inspection strategies (e.g., random sampling). Additionally, attaining a more rigorous translation

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

from SFC to PN, also including timing information (time PN), would be worthwhile.

Acknowledgment

The authors would like to thank Walid Fdhila for informative discussions on the submitted manuscript and Yameng An for providing the initial version of OntoPLC [33].

References

[1] M. Eckhart, K. Meixner, D. Winkler, and A. Ekelhart, "Securing the testing process for industrial automation software," *Comput. Secur.*, vol. 85, pp. 156–180, 2019.
[2] P. Kieseberg and E. Weippl, "Security challenges in cyber-physical production systems," in *Proc. Softw. Qual., Methods Tools Better Softw. Syst.*, 2018, pp. 3–16.
[3] M. Eckhart, A. Ekelhart, A. Lüder, S. Biffl, and E. Weippl, "Security development lifecycle for cyber-physical production systems," in *Proc. 45th Annu. Conf. IEEE Ind. Electron. Soc.*, 2019, pp. 3004–3011.
[4] *Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment and System Design*, Int. Electrotech. Commission, Geneva, Switzerland, Standard IEC 62443-3-2:2020, 2020.
[5] *IT-Security for Industrial Automation - General Model*, Verlag des Vereins Deutscher Ingenieure, Düsseldorf, Germany, Standard VDI/VDE 2182-1, 2011.
[6] M. Schleipen and R. Drath, "Three-view-concept for modeling process or manufacturing plants with AutomationML," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, 2009, pp. 1–4.
[7] M. Eckhart, A. Ekelhart, and E. Weippl, "Automated security risk identification using AutomationML-based engineering data," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 1655–1672, May./Jun. 2022.
[8] R. Drath, A. Lüder, J. Peschke, and L. Hundt, "AutomationML - the glue for seamless automation engineering," in *Proc. IEEE Conf. Emerg. Technol. Factory Autom.*, 2008, pp. 616–623.
[9] N. Schmidt and A. Lüder, "AutomationML in a nutshell," AutomationML e.V., Tech. Rep., Nov. 2015.
[10] S. Faltinski, O. Niggemann, N. Moriz, and A. Mankowski, "AutomationML: From data exchange to system planning and simulation," in *Proc. IEEE Int. Conf. Ind. Technol.*, 2012, pp. 378–383.
[11] A. E. Elhabashy, L. J. Wells, J. A. Camelio, and W. H. Woodall, "A cyber-physical attack taxonomy for production systems: A quality control perspective," *J. Intell. Manuf.*, vol. 30, no. 6, pp. 2489–2504, 2018.
[12] A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical attack vulnerabilities in manufacturing quality control tools," *Qual. Eng.*, vol. 32, no. 4, pp. 676–692, 2020.
[13] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manuf. Lett.*, vol. 2, no. 2, pp. 74–77, 2014.
[14] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vunerabilities in additive manufacturing systems," *Int. Solid Freeform Fabr. Symp.*, vol. 7, pp. 951–963, 2014.
[15] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "dr0wned cyber-physical attack with additive manufacturing," in *Proc. 11th USENIX Workshop Offensive Technol.*, 2017, pp. 1–16,.
[16] L. Apvrille and Y. Roudier, "SysML-Sec: A SysML environment for the design and development of secure embedded systems," in *Proc. Int. Conf. Asia-Pacific Council Syst. Eng.*, 2013, pp. 1–16.
[17] Y. Roudier and L. Apvrille, "SysML-Sec: A model driven approach for designing safe and secure systems," in *Proc. 3rd Int. Conf. Model-Driven Eng. Softw. Dev.*, 2015, pp. 655–664.
[18] R. Oates, F. Thom, and G. Herries, "Security-aware, model-based systems engineering with SysML," in *Proc. 1st Int. Symp. ICS SCADA Cyber Secur. Res.*, 2013, pp. 78–87.
[19] L. Lemaire, J. Lapon, B. De Decker, and V. Naessens, "A SysML extension for security analysis of industrial control systems," in *Proc. 2nd Int. Symp. ICS SCADA Cyber Secur. Res.*, 2014, pp. 1–9.
[20] L. Lemaire, J. Vossaert, J. Jansen, and V. Naessens, "Extracting vulnerabilities in industrial control systems using a knowledge-based system," in *Proc. 3rd Int. Symp. ICS SCADA Cyber Secur. Res.*, 2015, pp. 1–10.
[21] M. Glawe, C. Tebbe, A. Fay, and K.-H. Niemann, "Knowledge-based engineering of automation systems using ontologies and engineering data," in *Proc. Int. Joint Conf. Knowl. Discov., Knowl. Eng. Knowl. Manage.*, 2015, pp. 291–300.
[22] C. Tebbe, M. Glawe, A. Scholz, K.-H. Niemann, A. Fay, and J. Dittgen, "Wissensbasierte Sicherheitsanalyse in der Automation," *atp magazin*, vol. 57, no. 04, pp. 56–66, 2015.
[23] M. Glawe and A. Fay, "Wissensbasiertes Engineering automatisierter Anlagen unter Verwendung von AutomationML und OWL," *at-Automatisierungstechnik*, vol. 64, no. 3, pp. 186–198, 2016.
[24] C. Tebbe, M. Glawe, K.-H. Niemann, and A. Fay, "Informationsbedarf für automatische IT-Sicherheitsanalysen automatisierungstechnischer Anlagen," *at-Automatisierungstechnik,* vol. 65, no. 1, pp. 87–97, 2017.
[25] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016.
[26] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 9, pp. 52–80, 2015.
[27] M. H. Henry, R. M. Layer, K. Z. Snow, and D. R. Zaret, "Evaluating the risk of cyber attacks on SCADA systems via petri net analysis with application to hazardous liquid loading operations," in *Proc. IEEE Conf. Technol. Homeland Secur.*, 2009, pp. 607–614.
[28] M. H. Henry, R. M. Layer, and D. R. Zaret, "Coupled petri nets for computer network risk analysis," *Int. J. Crit. Infrastruct. Prot.*, vol. 3, no. 2, pp. 67–75, 2010.
[29] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
[30] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur.*, 2009, pp. 183–194.
[31] E. Kiesling, A. Ekelhart, K. Kurniawan, and F. Ekaputra, "The SEPSES knowledge graph: An integrated resource for cybersecurity," in *Proc. Int. Conf. Semantic Web*, 2019, pp. 198–214.
[32] Y. Hua and B. Hein, "Interpreting OWL complex classes in AutomationML based on bidirectional translation," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom.*, 2019, pp. 79–86.
[33] Y. An, F. Qin, B. Chen, R. Simon, and H. Wu, "OntoPLC: Semantic model of PLC programs for code exchange and software reuse," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1702–1711, Mar. 2021.
[34] AutomationML, "AutomationML example: Robot cell," AutomationML, Tech. Rep., Mar. 2017. [Online]. Available: https://www.automationml.org/wp-content/uploads/2021/06/AML_RobotCell_en_public.zip
[35] C. A. Petri, "Kommunikation mit Automaten," Ph.D. dissertation, Universität Hamburg, 1962.
[36] C. G. Cassandras and S. Lafortune, "Petri nets," in *Introduction to Discrete Event Systems*, 2nd ed. New York, NY, USA: Springer, 2008, pp. 223–267.
[37] M. Zhou and N. Wu, "Process-oriented Petri net modeling," in *System Modeling and Control with Resource-Oriented Petri Nets*, 1st ed. Boca Raton, FL, USA: CRC Press, 2010, pp. 43–55.
[38] N. F. Noy, M. Sintek, S. Decker, M. Crubezy, R. W. Fergerson, and M. A. Musen, "Creating semantic web contents with Protégé-2000," *IEEE Intell. Syst.*, vol. 16, no. 2, pp. 60–71, Mar./Apr. 2001.
[39] K. Schmidt, "LoLA: A low level analyser," in *Proc. 21st Int. Conf. Appl. Theory Petri Nets*, 2000, pp. 465–474.
[40] K. Wolf, "Petri net model checking with LoLA 2," in *Proc. 39th Int. Conf. Appl. Theory Petri Nets Concurr.*, 2018, pp. 351–362.
[41] N. Wightkin, U. Buy, and H. Darabi, "Formal modeling of sequential function charts with time Petri nets," *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 2, pp. 455–464, Mar. 2011.
[42] A. Valmari, "The state explosion problem," in *Proc. Lectures Petri Nets I: Basic Models: Adv. Petri Nets*, 1998, pp. 429–528.
[43] A. Valmari, "Stubborn sets for reduced state space generation," in *Proc. 10th Int. Conf. Appl. Theory Petri Nets*, 1991, pp. 491–515.
[44] K. Wolf, "Generating Petri net state spaces," in *Proc. 28th Int. Conf. Appl. Theory Petri Nets Models Concurr.*, 2007, pp. 29–42.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:21:27 UTC from IEEE Xplore. Restrictions apply.

A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry

Imran Ashraf, Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, *Senior Member, IEEE*, and Summera Nosheen

***Abstract*— Impressive technological advancements over the past decades commenced significant advantages in the maritime industry sector and elevated commercial, operational, and financial benefits. However, technological development introduces several novel risks that pose serious and potential threats to the maritime industry and considerably impact the maritime industry. Keeping in view the importance of maritime cyber security, this study presents the cyber security threats to understand their impact and loss scale. It serves as a guideline for the stakeholders to implement effective preventive and corrective strategies. Cyber security risks are discussed concerning maritime security, confidentiality, integrity, and availability, and their impact is analyzed. The proneness of the digital transformation is analyzed regarding the use of internet of things (IoT) devices, modern security frameworks for ships, and sensors and devices used in modern ships. In addition, risk assessment methods are discussed to determine the potential threat and severity along with the cyber risk mitigation schemes and frameworks. Possible recommendations and countermeasures are elaborated to alleviate the impact of cyber security breaches. Finally, recommendations about the future prospects to safeguard the maritime industry from cyber-attacks are discussed, and the necessity of efficient security policies is highlighted.**

***Index Terms*— Maritime security, IoT, cyber security threats, vulnerability, malware.**

I. Introduction

TECHNOLOGICAL developments have shown unprecedented speed over the past decade and revolutionized many fields by incorporating novel technologies, policies, and operational procedures. Analogous to several other domains, advanced digitization, information, and operation technology have also made their way in the maritime industry.

The maritime freight-forwarding industry serves as the foundation for international trade carrying around 80% of goods globally and contributing 70% of trade value [1], [2]. Consequently, large investments from multinational companies like Maersk, IBM, and Google, etc., accelerated the revolutionization of the maritime industry. Not only that, Maersk and IBM are working on projects to commercialize the blockchain technology for digital global trade platforms [3]. Shipping automation and incorporation of intelligent systems in maritime is to be deployed by Google, and Rolls Royce [4]. Similarly, projects on digitizing the platforms are carried out under Det Norske Veritas, and Germanischer Lloyd [5]. With the digitalization of the maritime operational platforms, safe navigation, low manning requirements, and security are visioned. With a large increase in the operations of the maritime freight industry over the past decade, further, expansion is expected in the near future. Figure 1 shows the statistics of container throughput for worldwide ports for this decade, indicating a substantial increase in the throughput from 622 million twenty-foot equivalent units (TEUs) in 2012 to an expected 945 million TEUs in 2024 [6].

The maritime industry has evolved from traditional mechanical systems to electromechanical and digital systems involving changes in industrial control systems over the past decade. Consequently, the modern maritime industry operates on semi-automatic/automatic controlled systems, automated harbors, satellite communication, and navigation systems. Such systems combine sophisticated hardware and software systems operated through mobile networks involving the maritime industry stakeholders. Marine communication is carried out using board systems involving shore stations and satellites. Digital selective calling (DSC) is used for distress alerts, safety calls, and routine priority messages, digital selective calling (DSC) is used, which can be integrated with very high frequency (VHF) radios used for ship-to-ship communication. Similarly, satellite communication is used for areas where the shore stations have no coverage [7]. Maritime communication systems contain equipment and devices, a large number of which are connected to the internet or telecommunication systems [8] and can be attacked remotely using both simple as well as sophisticated cyber attacks. Predominantly, the maritime organizations are

Manuscript received 14 December 2021; revised 1 March 2022; accepted 30 March 2022. Date of publication 15 April 2022; date of current version 8 February 2023. This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education under Grant NRF-2021R1A6A1A03039493; in part by NRF Grant by the Korean Government through the Ministry of Science and ICT (MSIT) under Grant NRF-2022R1A2C1004401; and in part by the Taif University Researchers Supporting Project, Taif University, Taif, Saudi Arabia, under Grant TURSP-2020/36. The Associate Editor for this article was A. K. Bashir. *(Imran Ashraf and Yongwan Park are co-first authors.) (Corresponding authors: Yousaf Bin Zikria; Summera Nosheen.)*

Imran Ashraf, Yongwan Park, Soojung Hur, Sung Won Kim, and Yousaf Bin Zikria are with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: imranashraf@ynu.ac.kr; ywpark@yu.ac.kr; sjheo@ynu.ac.kr; swon@yu.ac.kr; yousafbinzikria@ynu.ac.kr).

Roobaea Alroobaea is with the Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia (e-mail: r.robai@tu.edu.sa).

Summera Nosheen is with the Faculty of Engineering, School of Computer Science, The University of Sydney, Sydney, NSW 2006, Australia (e-mail: summera.nosheen@sydney.edu.au).

Digital Object Identifier 10.1109/TITS.2022.3164678

1558-0016 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

TABLE I
A SUMMARY OF CYBER SECURITY THREATS, THREAT ACTORS AND OBJECTIVES

Threat	Level	Threat actors	Objectives
Cyber vandalism	1	Hackers, vandalist, angered employees, activist	Data stealing, destroying, or public posting for media coverage.
Cyber Theft	2	Individual, small groups (political, ideological), spammers	Information, disruption of destruction of business operations, profit or ideological gains
Cyber Incursion	3	Organized enterprise, government entity, terrorist groups	Information of weaknesses, backdoor planting, access, alter or destroy information.
Cyber Sabotage	4	Organized professional organizations, military secret operatives	High-level information regarding secret R&D critical for organization/government, cracking security procedures, infiltration
Cyber Conflict	5	Government operatives, highly skilled terrorist groups, sophisticated hacker group	Infrastructure destruction, high importance mission-critical information
Cyber Internal	6	Employees, workers, third party service providers	Non-intentional mistakes, carelessness, lack of skill to open opportunities for 1 to 5 discussed threats.

not well prepared to handle cyber attacks, as pointed out in [9]. For different kinds of breaches, the preparedness varies with respect to the size and scope of the organization. For example, large companies are well prepared for data breaches which are primarily attributed to the higher ratio of data breaches that occurred in large companies. The capability of handling cyber attacks is increased for those organizations who report such attacks and devise countermeasures to prevent similar future attacks. In this regard, this study makes the following contributions

- This study conducts an extensive review of the security threats for the IoT-enabled maritime industry.
- Comprehensive background on maritime security threats space is provided where different threats, threat actors, and objectives for threats are discussed.
- Cybersecurity threats related to the maritime industry are analyzed regarding different elements of maritime infrastructure like vessels, offshore units, etc., and the onboard devices like navigation systems, data recorders, logistics, etc.
- For assessing the potential threat and risk of cyberattacks, various risk analysis methods are elaborated with their advantages and disadvantages. In addition, different threat mitigation methods are discussed.
- A brief and compact prospective discussion is provided for the shortcomings of existing defense strategies for handling the maritime risks, and future directions are outlined.

A taxonomy of the research papers covered in this study is provided in Figure 2. The rest of the study is organized in the following fashion. Section II provides the background of the cyber security threats and their various types. Maritime cyber security threats are discussed in Section III. Risk impact analysis of cyber security threats is performed in Section IV while risk mitigation schemes are given in Section V. Overview of probable threats with respect to Industry 4.0 is described in Section VI. Future research directions are provided in Section VII while the conclusion is given in Section VIII.

II. BACKGROUND ON CYBER SECURITY THREATS

Keeping in view the proneness of the electromechanical and digital systems, involving connected hardware and software components, the associated risks and threats are large and complex, necessitating the extensive evaluation of

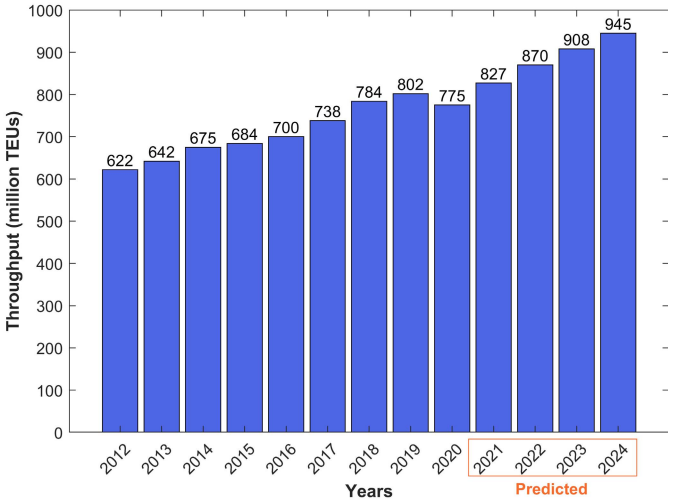


Fig. 1. Container throughput in million TEUs for maritime world wide [6].

systems' vulnerabilities. The security threats become worse when geopolitical disputes and piracy attacks are considered. Maritime security threats can be broadly categorized under two groups: intentional threats and unintentional threats.

A. Intentional Threats

Intentional direct threats are cyber security threats caused by a large number of adversaries and involve different methods and techniques.

1) Cyber Vandalism: Representing an ideological motivation, such individuals/groups steal sensitive information to exploit their target. Often inspired by different individuals, cyber vandalists, also called hacktivists, misuse the stolen data for malicious purposes, such as blackmail, extortion, and ransom, etc. [10].

2) Cyber Sabotage: Cyber sabotage, also called espionage, threats come from industry rivals and market competitors, often targeting the intellectual properties of a target company [11]. It is the planned and organized intrusion to steal confidential information, alter if it provides an institutional benefit, or destroy data/products to outwit the competitor. Espionage aims at obtaining a competitive edge by empowering own skills by stealing intellectual property or disrupting the competitors' business operations [12].

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

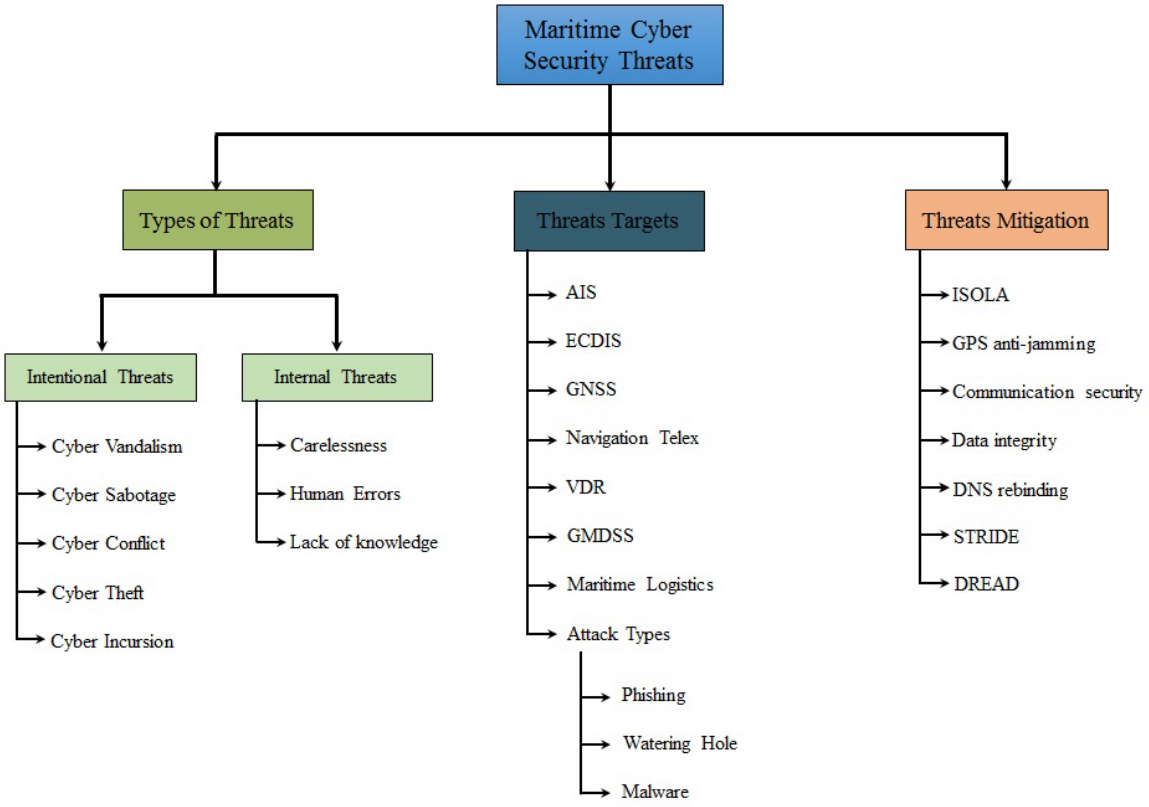


Fig. 2. Taxonomy of the papers discussed in this study.

3) Cyber Conflict: The scale and scope of the intentional attacks become wide when it is state-sponsored or government-driven. Countries may launch cyber attacks on the maritime industry of an opponent or competing country [12]. Primarily such attacks are made for obtaining state secrets and similarly other important information that may provide leverage. Similarly, secret business agreements and similar other commercial information of high importance can be targeted [13]. State-sponsored attacks are launched for economic dominance, information control, or national destabilization [14].

4) Cyber Theft: Cyber thieves, also called Terrorist groups, are often formed by certain religious, political, and social doctrines and take actions to target the opposing groups, nations, and countries. The maritime sector can also target such groups where the attacks are carried out using electronic and computerized media for obtaining unauthorized access to confidential information. Attacks are aimed at both destroying these resources, as well as using them for ransom and gaining the upper hand [12].

5) Cyber Incursion: Individuals or criminal organizations may also launch Cyber-attacks for criminal activities. Such attacks are launched for extortion, fraudulent activities, and illegal access to the intellectual property of an organization [12]. By gaining access to different controlling systems, weapons, drugs, and contraband operations are performed for economic benefits and stealing secret information for blackmail, ransom, and information selling to other groups [15].

B. Internal Cyber Threats

Besides the intentional cyber security threats for the maritime industry, the harm can be done unintentionally due to the negligence of employees or third-party service providers. Threats from internal employees can occur due to carelessness, human errors, or lack of knowledge about particular tools or procedures [16]. The intensity of internal threats varies with respect to the importance of the system being exposed to the security threat. Adversaries can misuse exposed systems to control and exploit them for secret information. Internal threats are often the outcome of improper training, lack of skills to handle a system, human judgmental error, and ignorance [12]. Third-party software and hardware systems can also jeopardize maritime security if software containing back doors, poorly tested software and error-containing systems are installed.

A schematic diagram of cyber security risks in the maritime industry and the associated risk level is portrayed in Figure 3. The number represents the risk level, with a higher number indicating the higher risk. Numbers from 1 to 6 are attributed to ‘low’, ‘moderate’, ‘high’, ‘very high’, ‘severe’, and ‘extreme’ risk for these threats. Cyber internal threats indicate the highest threat level and expose the companies to the maximum risk.

Table I provides the overview of the types of cyber security threats for the maritime industry, along with the possible threat actors and their objectives. The cyber internal threat category is ranked with the highest risk level as employees’ carelessness, lack of proper training, and knowledge may expose an organization’s infrastructure to all the threats described here.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

Fig. 3. Cyber security threats and associated risk level.

III. Analyzing Cyber Security Threats Related to Maritime

Basic components of the maritime infrastructure are depicted in Figure 4 indicating three important components: vessels, ground infrastructure, and communication network. Vessels contain on-board systems such as global maritime distress and safety systems (GMDSS), maritime administrative systems, communication systems, etc., prone to different kinds of cyberattacks. Similarly, off-shore systems comprise public infrastructure, including automatic identification systems for vessels and crew managers, private service providers, off-shore security systems, etc. Different adversaries can attack to obtain unauthorized access. A schematic diagram of on-board and off-board systems is given in Figure 5.

A. Automatic Identification System Related Attacks

An automatic identification system (AIS) provides safe navigation in the sea and collision avoidance by providing navigation-related information of other ships such as ship type, course, speed, ship status (anchor, or underway), etc. AIS aims at reducing the risks of possible collisions with other ships by communicating with them. However, communication makes AIS the most vulnerable system of the ship [17], [18].

With technological advancement, the AIS data can be reproduced, and a virtual ship can be placed with false speed, heading, course, and other information to deceive other ships. Weather information can be generated and sent to other ships to change their route. AIS attacks occur due to a lack of appropriate procedures to ensure integrity and encryption protocols which makes it easy for the attackers to intercept AIS transmission [19]. For example, an Iranian oil ship used falsified AIS data and pretended to be Tanzanian to navigate to Syria [20]. Using a very high frequency (VHF), an attacker can intercept AIS transmission, tamper the AIS data to steal identity information, communicate with a ship by impersonating port authorities, block the communication with other ships, and direct the vessel to the desired location by impersonating as competent maritime authority [21], [22]. AIS can also be the target of a denial-of-service attack, fake close point to alert collision alert, and data flood by transmitting at higher frequency [22], [23].

B. Electronic Chart Display and Information System

ECIDS has been a mandatory part of the ships since January 1, 2011, and contains several important functions in hardware and software for safe navigation. ECDIS is used for displaying ships course for the crew using the bridge-placed operating system. ECDIS contains position, compass, speed, etc., and is connected to ship systems and sensors and is updated via USB or the internet. Despite being an essential part of ships, it is found to be the easy target of adversaries [24]. The primary source of malicious code execution on ECDIS is the obsolete baseline operating systems or operating systems that do not allow upgrades [25].

C. Global Navigation Satellite System

Similar to navigation at land, GNSS provides important information for safe sailing at sea through guided navigation by GPS. After the AIS, GNSS has been regarded as the most vulnerable asset in the maritime sector [25].

Spoofing and jamming are the two most prominent threats to GPS technology. Spoofing involves using the port, access control address, and internet protocol (IP) to conceal the original identity for performing malicious activities. During the jamming, the GPS signals are disrupted or disturbed by intercepting the boat's frequency. Unlike spoofing, which is an impersonating act, jamming involves electronic or mechanical intervention to disrupt radar or radio communications [26]. Jamming attacks are usually carried out by commercial devices that are low cost and easy to buy online [27]. Spoofing attacks are complex as compared to jamming, as they require simulating the satellite signals that require high power and complicated apparatus [28].

Research shows that the navigational systems are the primary target of maritime cyber attacks due to their vulnerability, followed by ECDIS and engine control [29].

D. Navigation Telex

Navigation Telex (NAVTEX) provides urgent navigation and meteorological information for safe navigation by the port authorities. The information is disseminated by telex in the ship that operates at specific frequencies, and information is available via the website as well [30]. NAVTEX is connected to the internet, storage devices, and other systems prone to attacks. Attacks may result in incorrect messages to misguide the ship and blocking the service to send the messages from the attacker to guide the ship to the location of the attacker's choice [31].

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

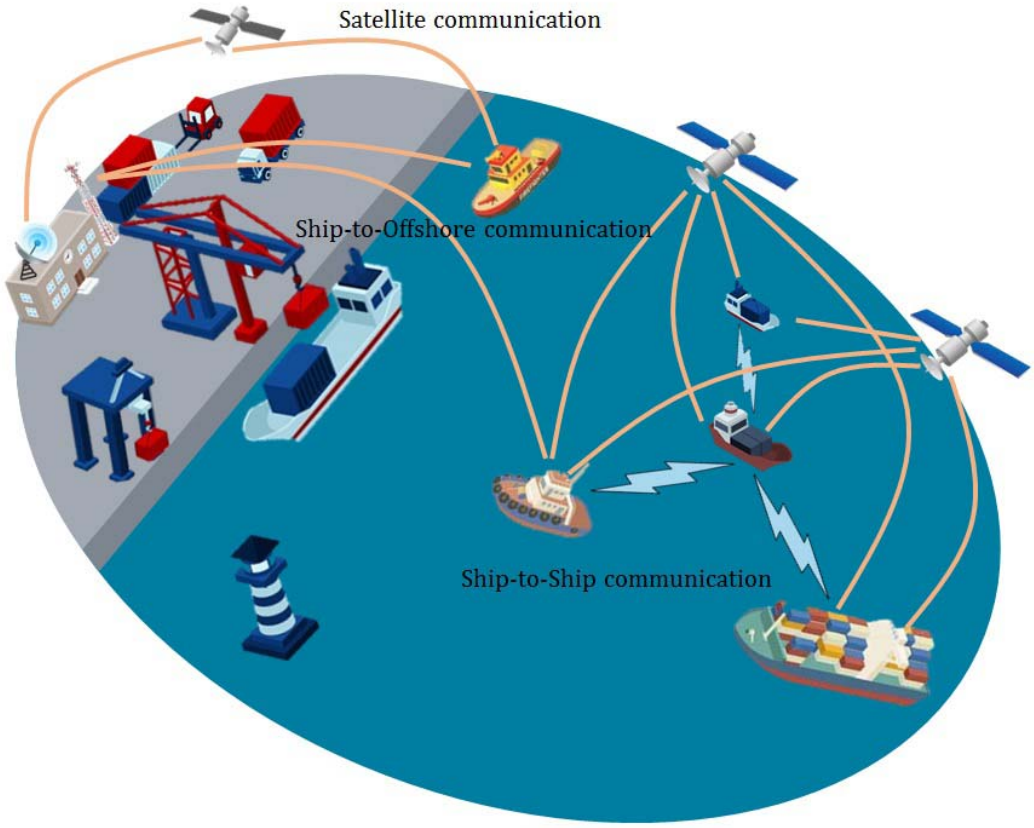


Fig. 4. Basic components of maritime infrastructure.

E. Voyage Data Recorders

A voyage data recorder (VDR) is used to store the voyage details of the ship and can be a potential tool for investigating ship accidents. It serves a similar purpose, as BlackBox does for the airplane, with superior functions. It records the speed, direction, position, conversations, etc. of the last 12 hours that can be used to analyze ship performance, accident analysis, and damage analysis. VDR is prone to intruder attacks, and the attacker needs to be inside the ship as it is connected to a local area network (LAN). Attacks happen due to inappropriate authentication mechanisms, weak encryption protocols, and obsolete firmware [32], [33]. VDR can be attacked for denial of service for obfuscation through the USB, CD, and DVD, etc. [34].

F. Global Maritime Distress and Safety System

GMDSS is the fundamental system for distress management and involves sending distress messages to shores and requesting search and rescue support. It also broadcasts the maritime safety information (MSI) for other ships in the vicinity that could help the distressed ship to a safe route []. Malware infections are targeted on GMDSS, resulting in partial damage or complete destruction. The control can also be taken to guide the ship to a designated location by the attacker. The identity of another ship can be spoofed using the GMDSS to initiate communication with other ships for influencing cargo safety. GMDSS interactions with SCC (shore control center) can be compromised to steal sensitive information of ship operations. Owing to the importance of GMDSS during emergency and rescue operations, any disruption can risk the rescue operations [35]. Similarly, jamming attacks can cause damage and denial-of-service for GMDSS [36]. To mitigate the impact of cyber attacks on GMDSS, counterpart systems are a potential solution [37].

G. Threats to Maritime Logistics Environment

With the advancements in technology, traditional supply chain and logistics systems have been transformed into supervisory control and data acquisition (SCADA) systems where the flow of goods can be remotely controlled. This infrastructure involves internet of things (IoT) platforms, satellites, and ICT procedures to control and monitor the maritime logistics and supply chain (MLSC). Consequently, SCADA infrastructure and cyber-physical systems (CPS) are prone to cyber-attacks from adversaries. MLSC systems comprise several CPS that has been the target of adversaries during the recent events [38]–[40].

SCADA systems in the current maritime sector involve interoperable components integrated with ICT systems and involve communication. Sensors and devices used for position tracking and monitoring, such as IoT sensors and cameras, satellite communication, etc., are susceptible to different cyberattacks [41]. SCADA systems can be the victim of five different kinds of cyberattacks.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

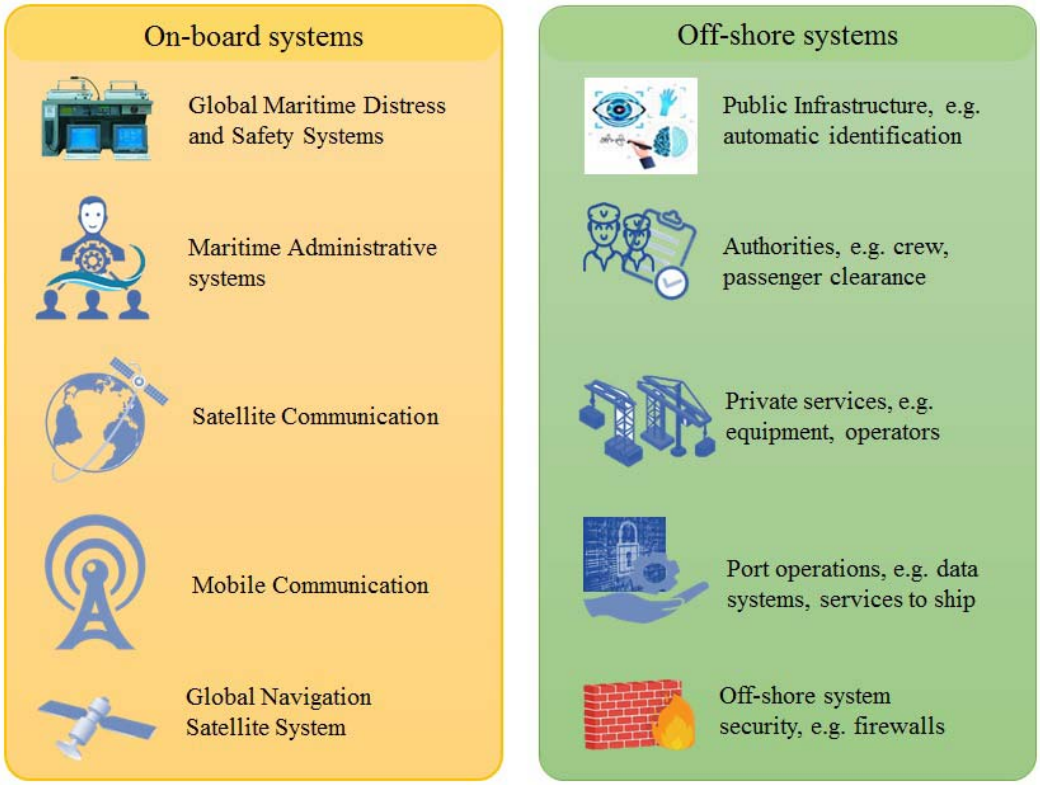


Fig. 5. Maritime systems for on-board and off-shore platforms.

1) Attacks can be directed to a communication stack such as a network layer.
2) Transport layer can be attacked using SYN flood attack types which involves sending transmission control protocol (TCP) connection requests faster, making it impossible for the machine to handle it. It leads to a denial-of-service (DoS) outcome.
3) Attacks like packet replay on the application layer. Such attacks normally happen due to weak security controls.
4) Adversaries attack hardware to obtain unauthorized access and remotely control the devices. Hardware attacks traditionally occur where the authentication controls or appropriate or missing.
5) Software cyber attacks include attacking the software working as an application layer between the sensors and application packages. For example, structure query language (SQL) can be the victim of SQL injection attacks.

In addition to the above-discussed SCADA attacks, the use of social media platforms for accessing the alerts, news regarding hazards, and similar other events can affect the operational capability of such system in emergency response scenarios [42].

H. Cyberattacks in Maritime

1) Phishing Attacks: The phishing attack is the most commonly used cyberattack, including social engineering and malware attacks. The former utilizes email services and fake websites to inflict damage or steal information, while the latter uses different malware installed on a personal computer. Phishing attacks aim at getting the users' personal information such as username, and password, etc., by tricking the user into visiting a fake website [43]. Phishing also includes a sub-category, spear phishing targets the company's employees through emails very similar to the company's legitimate emails. The email contains an attachment that can steal sensitive information stored on the computer once it is clicked to view.

2) Watering Hole Attack: Watering hole attacks target a specific group for a security exploit by using the group's specific websites known to be visited. Such attacks are specifically targeted on the employees of an organization/crew members to gain access to their personal computer by infecting the legitimate websites [44]. Malicious codes are placed on famous websites by exploiting their vulnerabilities and weaknesses and redirecting the users to attackers' websites [45]. Although uncommon, watering hole attacks are harder to detect as they come from legitimate and famous websites. Systems that analyze the compromised websites have been proposed to alleviate the cyber risks of watering hole attacks [46]–[48].

3) Malware: Malware is a group of computer code programs intended to steal or destroy the data on a computer using viruses, spyware, and ransomware. Malware is used for recording a user's activity and stealing confidential information for blackmail and publishing online [49]. With the increase in the number of IoT devices for the modern maritime industry, experts have regarded malware as an attractive choice to

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

penetrate and breach cyber security [50]. Malware is also used for identity fraud and to commit crimes and terrorist activities in the maritime sector. Similarly, ransomware is also malware containing the zip or other files where opening these files can block access to resources. The attacker requires a ransom amount to allow access. The malware aims at creating man-in-the-middle attacks by exploiting (SSL) or (TSL) weaknesses to download important data from the user's computer [51], [52].

IV. Cyber Risk Analysis Methods

International maritime organization (IMO) is the central agency from the United Nations (UN) to devise policies and procedures for the maritime industry's safety and security, including the risks to the maritime sector and maritime induced risks for the environment. For safeguarding the ships from cyber attacks, it has defined protocols and procedures for a preventive and corrective course of actions, including the elements of cyber risk management [53], as shown in Figure 6. IMO defines five elements for cyber risk management, including identification, protection, detection, responding to risks, and recovering. In addition, the national institute of standards and technology of the United States (US) further elaborates this framework and provides detailed discussions on how to use it [54]. Similarly, the institute of engineering and technology (IET) [55] provides the code of practicing cyber security for ships, and the Baltic and international maritime council (BIMCO) drafts the guidelines for onboard ships [21]. Several models have been contrived to analyze risk impact analysis for maritime cyber risks based on these elements. On the other hand, several individual works outline the guidelines for cyber security for commercial maritime and policies for managing cyber risk [56].

Several models have been designed to analyze the cyber risks with the maritime industry. Maritime risk assessment utilizes qualitative and quantitative methods where the former prioritizes the risks based on their probability. At the same time, the latter performs numerical analysis by awarding risk values to each risk. Predominantly, maritime physical risks analysis relies on probability analysis based on empirical statistics [57], [58]. A qualitative risk analysis is performed for inertial navigation system-related cyber risks in [59]. In addition to the crew interviews, testing is also performed to analyze different vulnerabilities. Results show that remote desktop, terminal service, and remote protocols are vulnerable to arbitrary remote code and man-in-the-middle attacks, respectively. A more critical risk is the server message block service which can be exploited to arbitrary code execution and disclosure of sensitive information. An interview and survey-based method is adopted by [60] for ECDIS cyber vulnerabilities. Unsupported windows, server message block (SMB) vulnerability, improper handling of remote procedure call (RPC), SMB remote execution, and SMB security update are critical risks for ECDIS in maritime ships.

The authors perform cyber risk analysis with a framework based on IMO and IET guidelines in [61] following an on-board survey and cyber security testing for analyzing ECDIS-related cyber risks. Cyber security testing involves vulnerability scanning and penetration testing techniques. The study finds out that the Apache webserver poses a high level of risk as it is obsoleted. As a result, the functionality of the ECDIS can be fully destroyed. Similarly, an experimental ship assessment is carried out in [62] involving the cyber security survey and cyber vulnerability computational scanning to analyze the ECDIS vulnerabilities. Results suggest that obsolete operating systems, server service vulnerability, SMB vulnerability, and SBM security updates are the cyber threats that can be exploited to run arbitrary code from a remote location. Along the same direction, study [63] performs cyber security testing for ECDIS vulnerabilities. Web servers are outdated, printer sharing and operating systems are vulnerable to unauthorized access, leading to a denial of service, crashing ECDIS, stealing sensitive information, man-in-the-middle attacks, etc. In addition, the study analyzes the cyber security risks associated with the third-party service provided and finds out that third-party abandoned and out-of-date components and components involving insecure setup are the major threats.

A survey is conducted in [64] for cyber security vulnerabilities in maritime involving mariners, port officers, IT system experts, and third-party service providers. Survey results highlight the crew-training standards inappropriate (74%), followed by the cyber-attacks with 55%. A total of 60% are found to be explaining the lack of cyber security training. Additionally, 50% of the participants blamed IT as the vulnerable technology for cyber-attacks, while 41% regarded IT and OT as equally responsible. Regarding the cyber crimes, malware, phishing scams, and web-based attacks have been placed at the top three with 31%, 13%, and 13%, respectively of all the cyber crimes in the maritime. The authors of [65] investigate the factors responsible for cyber threats in maritime through a survey. An 80% of the participants considered the crew training insufficient, while 56% ranked cyberattacks as the leading problem for the maritime sector. The majority of the participants (57%) did not receive training regarding cyber security, and 80% suggested the importance of maritime cyber training over general cyber security training. Malware, phishing, and web attacks have been regarded as the leading cyber attacks with 26%, 16%, and 16%, respectively, of all the cyber attacks in the maritime sector.

In the same fashion, the role of human behavior on the cyber security of maritime systems is studied in [66], where the crew members are divided into different groups such as introvert, extrovert, and intuitive, etc. Interviews with the crew members indicate that majority of the people attached with the IT have a medium or low level of knowledge. Despite the installed security systems on the ships, the crew members are not well trained to operate the sophisticated programs. Often, cyber incidents happen due to operators' mistakes due to lack of proper training, carelessness, or poor skill set. A future prospect of the maritime cyber risk is presented in [67] by conducting a survey where 93% of the respondents suggest that the frequency and intensity of the cyber attacks will increase. In addition, the perceptions and potential of social media as a tool for cyber attacks are evaluated, indicating that 74% of the participants believe social media is a potential source of cyber attacks. An 87% believe that the cyberattacks

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

can be handled more prudently if properly reported and investigated to mitigate future attacks. Study [68] discusses the cyber threats to critical maritime infrastructure, including on-board systems and port operations. Analyzed incidents include high-value cargo theft by infecting authentication data, software malware to shut down port operations, and software infection to interrupt port operations. The study discusses several challenges associated with maritime cyber attacks handling.

The maritime cyber risk analysis (MaCRA) model is one of the risk assessment models in the maritime sector [69] that combines cyber and maritime factors for risk analysis. By considering ship functions, configurations, users, and environmental factors, the framework provides the maritime cyber risks associated with a particular ship type and assists in devising appropriate security procedures. The maCRA model is extended for risk analysis in the autonomous ships by [34] to provide anticipated risks for the futuristic ships. In this regard, the risks are discussed with respect to navigation systems and cargo systems, considering the reward, ease of exploit, and system vulnerability.

GPS jamming has significant repercussions for navigation. [70] shows that the positioning error during GPS jamming is too high to produce catastrophic outcomes if the sailing is continued. Similarly, GPS jamming makes AIS useless as AIS uses GPS signals for slot timing sources which are required for VHS communication based on self-organized time division multiple access (SOTDMA). Jamming GPS also has a strong impact on radar communications, and radar-based detection has erroneous estimations [70]. In addition, if the GPS data is used for slot timing in digital communication such as cellular telephone and satellite communication, GPS jamming would affect these systems.

Risk assessment methods for SCADA can be qualitative, quantitative, and hybrid, combining the first both. Fault tree events analysis [71], object-based event scenario tree [72] and probabilistic risk analysis tools [73] follow a semi-qualitative approach while [74], [75] present quantitative models for risk assessment. For SCADA-related risks assessment, several important research works can be found that extensively studied different approaches for the past two decades [60], [76]–[78]. These research works cover risk assessment methods for static and real-time systems, including monitoring, detection, impact analysis, and countermeasures.

The study [79] presents an automated threat modeling approach regarding cyber security threats to the maritime industry. It comprises three modules each for feature extraction, cyber threat intelligence (CTI)-based detection, and CTI-based attack categorization. The proposed approach performs automated CTI contrary to traditional systems where threat-related features are manually extracted [80]. The model provides increased accuracy as compared to the state-of-the-art approaches.

V. Threat Mitigation Methods

In general, the maritime sector lacks a timely response to introduce the appropriate countermeasures for resolving

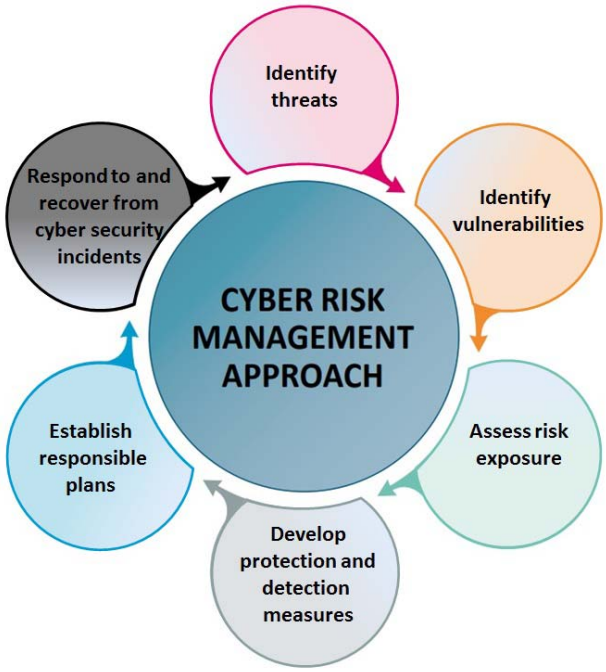


Fig. 6. Elements of cyber risk management, adopted from [21].

technical vulnerabilities, which increase the susceptibility of the onboard systems [81]. Due to the better maintenance off-shore systems in the maritime sector, they experience a low number of cyberattacks compared to their counterparts. Secondly, onboard systems rely on obsolete underlying operating systems or those operating systems that do not allow upgrades. The upgrade failures may occur due to conflicting IT and OT technologies standards where the upgrade of one may not support the other. Out of date systems put the entire ship at the hand of the adversaries. Maritime needs to prioritize the critical systems and ensure their safety first, such as navigation, ECDIS, and VDR [82].

Several frameworks and techniques have been presented to mitigate the probability of cyber risks by building detection and correction procedures for cyber attacks. For example, A novel framework, innovative and integrated security system onboard covering the life cycle of a passenger ships voyage (ISOLA), is presented in [83] that performs risk analysis for cruising ships at sea. The analysis covers both vulnerabilities and threats for onboard and off-shore cyber attacks and recommends several data fusion solutions to mitigate the risk impact. The authors present an integrated framework in [84] to monitor the air-sea-ground space for oil ships. Comprising of sensing, network, and application layers, the sensing layer is used to collect the data from air, sea, and ground transmitted via the network layer. The spaceborne synthetic aperture radar (SAR) is used for data collection. The collected observations combined with the forecasting model can provide reliable and accurate trajectory predictions in case of distress situations.

With increasing threats to GPS spoofing and jamming, an authentication scheme is presented by [85] for 6G-IoT-enable maritime transportation. The proposed approach is

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

TABLE II
A BRIEF SUMMARY OF MODELS USED FOR CYBER RISK ANALYSIS

Ref.	Model	Application	Objectives
[34]	maCRA for autonomous ships	Autonomous ships	Anticipation of probable risks for futuristic autonomous ships in maritime sector.
[59]	Qualitative	INS risk analysis	Analyzing risks associated with navigation tools, charts and interfaces.
[60]	Qualitative	ECDIS risk analysis	Risk analysis for ECDIS components such as SMB, RPC, etc.
[61]	maCRA	Ship with different functionalities, users and configurations	Risk analysis for different kinds of ships, by considering ease of vulnerabilities and exploit reward.
[62]	Mixed	ECDIS risk analysis	Risk analysis using vulnerability scanning and penetration testing techniques.
[63]	Mixed	ECDIS vulnerability	Onboard ship security survey and computational scanning for cyber vulnerability.
[64]	Computational penetration testing	ECDIS third-party service vulnerability	Computational penetration for cyber security threats associated with ECDIS third party services.
[65]	Survey	Maritime cyber risk analysis	Highlighting the most vulnerable component of the maritime including the crew, IT, and operation technology.
[66]	Interviewing	Human factors in cyber risk	Evaluating and highlighting the human factors leading to cyber attacks.
[67]	Survey	Factors for cyber risk	Analyze factors responsible for cyber risks in maritime such as training, IT procedures vulnerability, etc.
[68]	Survey	Cyber risk analysis	Finding factors related to maritime cyber attack to mitigate risk impact, such as social media, human factors, etc.

based on a lightweight message exchange protocol with increased security following initialization, vessel registration, and mutual authentication. The protocol is validated by using the Real-Or-Random model. Results indicate the superior performance of the proposed approach with respect to security and security-to-efficiency trade-off. Along the same lines, an attribute-based data aggregation scheme is proposed in [86] that focuses on the security of isolated IoT-enabled maritime ships. In the proposed scheme, onboard sensors are incorporated for the aggregation of the maritime terminal. The zero-knowledge proof ensures that only legitimate participants can participate in the communication. Results prove the security reliability of the scheme and the reduced computation cost.

The study [87] proposes a framework to detect and defend against the domain name system (DNS) rebinding attacks. A Markov chain model is used to model the DNS rebinding attack. The important attributes are extracted and used with a novel detection model. Experimental results show that the model is suitable for onboard local IoT devices and provides a defense mechanism against DNS rebinding attacks. Similarly, a security and privacy-preserving protocol is proposed in [88] to secure the communication between the maritime electric vehicles and charged grids. The proposed solution is based on blockchain technology and utilizes encryption and consensus algorithms to ensure secure communication [89]. Another endeavor to secure the data sharing between maritime ships and offshore servers is [90] that designed an identity-based information-sharing scheme. The scheme utilizes the blockchain in the fog environment, and smart contracts are used to control secure access to the data. With the proposed scheme, increased security is obtained with reduced computational complexity. Similarly, the authors propose a data integrity framework for maritime transportation systems in [91]. The data blocks are encoded using the erasure coding that provides security against malicious attacks. The data is stored on the cloud and can be recovered in case of data loss. The proposed approach proves to have a low computational head.

Several threat modeling approaches have been devised and adopted for maritime cyber risk analysis and mitigation. STRIDE covers six security threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges and performs qualitative analysis of cyber risks [92]. Threat analysis is carried out by developing attack scenarios regarding security objectives such as integrity, authorization, etc. STRIDE is especially useful for discovering vulnerabilities in the systems under design, thus enabling the authorities to eliminate such vulnerabilities in the design process [93], [94]. DREAD is another model for risk mitigation that weights the risks by considering five aspects, including damage potential, reproducibility, exploitability, affected users, and discoverability [35]. Damage refers to the content inflicted to the system regarding the affected things (both users and systems). Reproducibility is the attackers' ability to reproduce it, and exploitability is the extent to which the systems are vulnerable. In contrast, the ability of the attacker to find the system's vulnerability is discoverability. Unlike STRIDE, which focuses on a qualitative analysis, DREAD quantifies the risks by performing a quantitative risk analysis. The values of DREAD elements are determined into high, medium, and low that are used to assign a cyber attack weight for each of the CPS [95].

A hybrid framework based on STRIDE and DREAD is presented in [96] for minimizing the threat of cyber attacks in the maritime sector. By analyzing various CPS's qualitative and quantitative risk factors, the study suggests appropriate controls to alleviate the risk of maritime cyber-attacks. The authors present MITIGATE, a threat mitigation scheme for maritime supply chain [97]. It can be used for MLSC infrastructure and the SCADA system to analyze the risk of cyber risk in a dynamic environment.

VI. INDUSTRY 4.0

Industry 3.0, which focused on automation, computers, and electronics, has been shifting towards Industry 4.0. It includes cyber-physical systems, the internet of things, networks, and

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

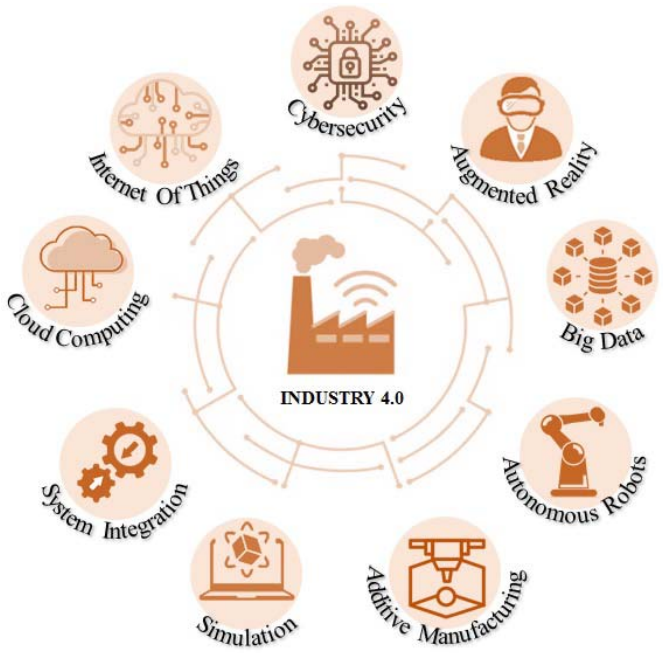


Fig. 7. Industry 4.0 envisions digital transformation, adopted from [98].

many more, as shown in Figure 7 is now performing digital transformation of maritime and its related industries. Using information and communication technology, Industry 4.0 aims at integrating machines and processes to make intelligent networks.

Technology and systems are becoming complicated and connected with every passing day. The concept of digital twins [99] and virtual reality based on the simulation present significant opportunities for the maritime sector to offer training and knowledge for crew members, third-party staff, and other people related to maritime [100]. Although digital twins are not very useful for analyzing cyber risks, virtual reality can play a significant role. It can be used to study maritime vulnerabilities arising in the foreseen Industry 4.0, where everything is connected.

Industry 4.0 is heavily reliant on the concept of IoT, where different small devices communicate via the internet, and the IoT networks can be very complex, and massive [101]. With the availability of cheaper computing power and the proliferation of mobile devices, a massive number of devices will be connected and communicating regarding ships/ports. This ubiquity will also increase the vulnerability of the communication network as more and more devices are connected [102]. So, real-time connected systems are to be modeled to study the probable cyber risks and analyze their impact. This need is further enhanced with the inception of autonomous ships, which are built on the IoT network [103]. With autonomous ships, cyber-physical systems become more prevalent and imminent because a higher number of devices will be used in physical operations.

The major cyber threats are directed remotely via the internet. However, with short-range communication in IoT devices for Industry 4.0, the intrusion threats are expected to be higher than remote threats necessitating tightly secured and well-encrypted protocols. Three important steps for the safekeeping of maritime IT and OT systems are the IT security procedures, cyberattack response and recovery, and preparedness for cyberattacks [104]. The manager should be trained to accept and embrace the IT security mechanisms and protocols to implement IT hygiene. Cyber security training should be considered an integral part of maritime security, and appropriate response and recovery procedures should be in place [105]. Additionally, the procedures should be updated periodically to ensure that they are up-to-date. Last but most importantly, a risk-free cyber environment does not exist. No matter how advanced the technologies become, related vulnerabilities and cyber risks emerge in new forms, which necessitates the importance of being prepared to expect the threats and respond to them accordingly.

VII. Discussions and Future Directions

A. Ship Diversity and Disparate Environment

Many challenges in maritime cyber security bar appropriate cyber security measures and mechanisms. A major challenge is the diversity of the ships and the disparate environments they operate. With ships from different classes, the installed systems, operated environments, requirements for onboard systems, and security procedures vary significantly, making it very difficult to define standard security mechanisms that would fit all. Another problem is the lack of reliable cyber security protocols for ship equipment like GPS and ECDIS [106] due to heterogeneous vendors and manufacturers where the implementation of a security protocol may be very different. The third complexity arises from the third-party service providers that deal with the maritime operational systems. The short visitations during the ashore stay of the ship limit their capability to fix problems appropriately.

B. Improper Cyber Security Risk Assessment

One major shortcoming for the secured maritime industry is the improper risk assessment of cyber security threats. For example, different nations in the European Union (EU) implement disparate security policies and practices, complicating risk assessment comparison. In addition, targeted risk assessment procedures should be developed with respect to the nature of the MLSC infrastructure, where processes are both distributed and interconnected. Research shows that the training and knowledge of the crew member are not up to the mark to deal with the cyber risks. The majority of maritime professionals suggest a lack of knowledge specifically in the field of maritime cyber security [50]. Lack of training and expertise for cyber security led to 88% to 90% of the shipping accidents, as stated in [107], [108]. Similarly, the reliance on obsolete and outdated systems in the maritime is a major problem [109], [110].

C. Lack of Real-World Testing

Poor crew skills, complexity and sophistication of on-board systems, outdated and vulnerable information systems, inappropriate integration of IT and OT procedures, network/system

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

heterogeneity, and lack of updating the cyber security procedures are the leading challenges for elevated maritime cyber security risks. Lack of real-world testing systems can make it very difficult to analyze the risk impact of cyber attacks fully. Especially, systems for penetration testing in the dynamic environment are needed for futuristic cyber attacks analysis and prevention. Ethical hacking should also be promoted to make beforehand preparations to counter cyber risks [111]. GPS jamming and spoofing is the leading cyberattack that caused potential damage to the maritime industry. Relying on one navigation guide technology seems a bottleneck and inappropriate. With more sensors on-board such as radar and LIDAR (light detection and ranging) in future ships, these sensors can be used for navigation and utilize other resources for navigation guides.

D. Increased Dependence on Cyber Technology

Recent automation and digitization have evolved the maritime sector by combining IT and OT more than ever. With the advanced digital technology, the maritime infrastructure relies on cyber technology increasing its proneness to different kinds of cyberattacks. Maritime-related cyberattacks are challenging due to a lack of information on the cyberattacks, economic and disruptive impact, and insightful investigations. Cyber attacks on the maritime can target navigation, cargo movement, ECDIS elements, off-shore AIS, third-party service providers, and other processes and threaten human lives, ecosystem, and maritime trade. Cyber attackers aim to obtain media attention, ransom, destroy an organization's resources, sell confidential data, and sabotage. In addition, ship transportation to the desired location, intervening in cyber security defense, and gaining critical information regarding national infrastructure are the primary goals of different types of adversaries. However, most of these attacks happen due to obsolete operational systems, especially software, and the carelessness of the maritime staff. The proper training and knowledge of Crews can significantly enhance the defense against such attacks, and so can the up-to-date operational procedures. A recent increase in maritime cyber security threats requires next-generation cyber security dealing procedures in real-time which means that the equipment and protocols to perform real-world experiments using vulnerability testing and penetration testing are need of the hour.

E. Need to Adopt Emerging Solutions

To ensure increased defense against evolving cyber attacks, novel and emerging solutions must be adopted. In this regard, two technologies can play a pivotal role in alleviating the risk of cyber attacks on maritime ships: satellite IoT and high altitude platform (HAP) solutions. With increased GPS jamming and spoofing attacks on maritime ships, satellite IoT can work as a complementary solution with wide coverage and therefore can be advantageous in many ways [112]. Such low orbit satellites can provide communication at lower latency with lower transmission loss and supplement the GNSS [113], [114]. The third generation partnership project (3GPP) incorporates the solutions for new radio (NR) to support non-terrestrial networks (NTN) communications [115]. In the same way, HAP systems can provide broadband connectivity and telecommunication services to remote areas where connectivity to the core network is not possible. In case of distress situations, HAP systems can provide the connectivity for mobile and core network for backhauling [116]. Since HAP systems require minimal ground infrastructure, they can be pivotal for disaster, distress, and emergency response cases.

VIII. Conclusion

With rapid technological advancements, the maritime sector has prospered regarding technology like sensors, communication, and security. Despite the potential benefits of embracing such digital transformation, the proneness of the maritime industry has been substantially increased as well, opening new ways and paradigms for cyber attacks. This study analyzes the cyber security threats for the maritime industry regarding the devices used for sensing, communication, navigation, and emergency response in case of distress. It is observed that the ships lack the technical staff to handle the under attack situation. The ship crew does not possess competence or is not well trained to handle cyberattacks, and the cyber security aspect of ships is overlooked. Despite several systems being in place, the relied-on systems/software are often obsolete, not fully operational, or unsuitable for real-world situations. In addition, security devices and frameworks are heterogeneous and lack standard operating procedures.

References

[1] European Community Shipowners' Associations, *Shipping and Global Trade Towards an EU External Shipping Policy*. Accessed: Nov. 22, 2021. [Online]. Available: https://www.ecsa.eu/sites/default/files/publications/2017-02-27-ECSA-External-Shipping-Agenda-FINAL.pdf

[2] M. Kalouptsidi, *The Role of Shipping in World Trade*. Accessed: Nov. 22, 2021. [Online]. Available: https://econofact.org/the-role-of-shipping-in-world-trade

[3] A. Roger. (2018). *Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitise Supply Chains*. [Online]. Available: https://www.forbes.com/sites/rogeraitken/2018/01/16/ibm-forges-global-joint-venture-with-maersk-applying-blockchain-to-digitize-global-trade/?sh=3d6b0a36547e

[4] B. S. Rivkin, "Unmanned ships: Navigation and more," *Gyroscopy Navigat.*, vol. 12, no. 1, pp. 96–108, Jan. 2021.

[5] L. Register, "Cyber-enabled ships shipright procedure assignment for cyber descriptive notes for autonomous & remote access ships," Lloyd's Register, London, U.K., Tech. Rep., 2017.

[6] M. Placek. (2021). *Container Throughput at Ports Worldwide From 2012 to 2020 With a Forecast for 2021 Until 2024*. [Online]. Available: https://www.statista.com/statistics/913398/container-throughput-worldwide/

[7] A. Chakrabarty. *What Marine Communication Systems Are Used in the Maritime Industry*. Accessed: Nov. 27, 2021. [Online]. Available: https://www.marineinsight.com/marine-navigation/marine-communication-systems-used-in-the-maritime-industry/

[8] Y.-C. Lee, S.-K. Park, W.-K. Lee, and J. Kang, "Improving cyber security awareness in maritime transport: A way forward," *J. Korean Soc. Mar. Eng.*, vol. 41, no. 8, pp. 738–745, Oct. 2017.

[9] A. R. Lee and H. P. Wogan, "All at sea: The modern seascape of cybersecurity threats of the maritime industry," in *Proc. OCEANS MTS/IEEE Charleston*, 2018, pp. 1–8.

[10] J. J. George and D. E. Leidner, "From clicktivism to hacktivism: Understanding digital activism," *Inf. Org.*, vol. 29, no. 3, Sep. 2019, Art. no. 100249.

[11] A. Bagchi and J. A. Paul, "Espionage and the optimal standard of the customs-trade partnership against terrorism (C-TPAT) program in maritime security," *Eur. J. Oper. Res.*, vol. 262, no. 1, pp. 89–107, Oct. 2017.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

[12] H. Boyes, R. Isbell, and A. Luck, "Code of practice: Cyber security for ports and port systems," *Inst. Eng. Technol.*, vol. 28, p. 2016, Oct. 2016.

[13] A. Oruc and M. S. M. MIMarEST, "Claims of state-sponsored cyberattack in the maritime industry," in *Proc. Int. Naval Eng. Conf. & Exhib.*, 2020, doi: 10.24868/issn.2515-818X.2020.021.

[14] D. Volz, "Chinese hackers target universities in pursuit of maritime military secrets," *Wall Street J.*, Jan. 2019. Accessed: Nov. 29, 2021. [Online]. Available: https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800

[15] D. J. Bodeau, R. Graubart, and J. Fabius-Greene, "Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels," in *Proc. IEEE 2nd Int. Conf. social Comput.*, Oct. 2010, pp. 1147–1152.

[16] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber physical systems security for maritime assets," *J. Mar. Sci. Eng.*, vol. 9, no. 12, p. 1384, Dec. 2021.

[17] J. DiRenzo, D. A. Goward, and F. S. Roberts, "The little-known challenge of maritime cyber security," in *Proc. 6th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, 2015, pp. 1–5.

[18] B. Mednikarov, Y. Tsonev, and A. Lazarov, "Analysis of cybersecurity issues in the maritime industry," *Int. J. Inf. Secur.*, vol. 47, no. 1, pp. 27–43, 2020.

[19] G. C. Kessler, J. P. Craiger, and J. C. Haass, "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system," *Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 12, no. 3, p. 429, 2018.

[20] BIMCO. (2016). *The Guidelines on Cyber Security onboard Ships*. [Online]. Available: https://www.liscr.com/sites/default/files/online_library/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016(3).pdf

[21] *The Guidelines Cyber Secur. Onboard Ships*, BIMCO, Copenhagen, Denmark, 2016.

[22] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, 2014, pp. 436–445.

[23] B. Hyra, "Analyzing the attack surface of ships," M.S. thesis, DTU Comput. Dept. Appl. Math. Comput. Sci., Technical Univ. Denmark, Lyngby, Denmark, 2019. [Online]. Available: https://backend.orbit.dtu.dk/ws/portalfiles/portal/174011206/190401_Analyzing_the_Attack_Surface_of_Ships.pdf

[24] B. Svilicic, D. Bráic, S. Žuékin, and D. Kalebic, "Raising awareness on cyber security of ECDIS," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 13, no. 1, pp. 231–236, 2019.

[25] T. Pseftelis and G. Chondrokoukis, "A study about the role of the human factor in maritime cybersecurity," *SPOUDAI-J. Econ. Bus.*, vol. 71, nos. 1–2, pp. 55–72, 2021.

[26] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION, J. Inst. Navigat.*, vol. 64, no. 1, pp. 51–66, 2017.

[27] M. Filić, "Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver," *Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 12, no. 4, pp. 1–8, 2018.

[28] M. S. K. Awan and M. A. Al Ghamdi, "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 350, 2019.

[29] A. Androjna and M. Perkoviá, "Impact of spoofing of navigation systems on maritime situational awareness," *Trans. Maritime Sci.*, vol. 10, no. 2, pp. 361–373, Oct. 2021.

[30] K. Korcz, "Maritime radio information systems," *J. KONES*, vol. 24, pp. 1–8, Dec. 2017.

[31] K. Tam, K. Moara-Nkwe, and K. Jones, "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training," *Maritime Technol. Res.*, vol. 3, no. 1, pp. 16–30, Jul. 2020.

[32] R. Santamarta, "Maritime security: Hacking into a voyage data recorder (VDR)," IOActive, Seattle, WA, USA, 2016. Accessed: Nov. 29, 2021. [Online]. Available: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/

[33] A. Cantelli-Forti, "Forensic analysis of industrial critical systems: The costa concordia's voyage data recorder case," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 458–463.

[34] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," in *Proc. Int. Conf. Cyber Secur. Protection Digit. Services*, Jun. 2018, pp. 1–8.

[35] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-attacks against the autonomous ship," in *Computing Security*. Cham, Switzerland: Springer, 2018, pp. 20–36.

[36] K. Tam and K. D. Jones, "Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping," *J. Cyber Policy*, vol. 3, no. 2, pp. 147–164, May 2018.

[37] F. X. M. de Osés and A. U. Juncadella, 'Global maritime surveillance and oceanic vessel traffic services: Towards the E-navigation," *WMU J. Maritime Affairs*, vol. 20, no. 3, pp. 1–14, 2021.

[38] L. O'Donnell-Welch. (2021). *Cybercriminals Target Transport and Logistics Industry*. [Online]. Available: https://duo.com/decipher/cybercriminals-target-global-logistics-industry

[39] A. Kinsey. (2021). *Cyber Security Threats Challenge International Shipping Industry*. [Online]. Available: https://www.maritimeprofessional.com/news/cyber-security-threats-challenge-international-369770

[40] C. Clmpanu. (2020). *All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-Attacks*. [Online]. Available: https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

[41] E.-M. Kalogeraki, N. Polemi, S. Papastergiou, and T. Panayiotopoulos, "Modeling SCADA attacks," in *Smart Trends System, Security Sustainability*. Cham, Switzerland: Springer, 2018, pp. 47–55.

[42] D. Kravets. (2009). *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*. [Online]. Available: http://www. wired.com/2009/03/feds-hacker-dis

[43] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017.

[44] J. Allen *et al.*, "Mnemosyne: An effective and efficient postmortem watering hole attack investigation system," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 787–802.

[45] K. A. Ismail, M. M. Singh, N. Mustaffa, P. Keikhosrokiani, and Z. Zulkefli, "Security strategies for hindering watering hole cyber crime attack," *Proc. Comput. Sci.*, vol. 124, pp. 656–663, Oct. 2017.

[46] K. Borgolte, C. Kruegel, and G. Vigna, "Delta: Automatic identification of unknown web-based infection campaigns," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 109–120.

[47] K. Borgolte, C. Kruegel, and G. Vigna, "Meerkat: Detecting website defacements through image-based object recognition," in *Proc. 24th Secur. Symp.*, 2015, pp. 595–610.

[48] Z. Li, S. Alrwais, X. Wang, and E. Alowaisheq, "Hunting the red fox online: Understanding and detection of mass redirect-script injections," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 3–18.

[49] P. R. Toth *et al.*, "Small business information security: The fundamentals," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. (NISTIR) 7621 Rev. 1, 2016.

[50] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," *Transp. Res. Proc.*, vol. 45, pp. 547–554, Jan. 2020.

[51] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Internet of Things and the man-in-the-middle attacks–security and economic risks," *MEST J.*, vol. 5, no. 2, pp. 15–25, 2017.

[52] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," *J. Pendidikan Teknol. Inf.*, vol. 2, no. 2, pp. 109–134, 2019.

[53] *Guidelines on Maritime Cyber Risk Management*, Int. Maritime Org. London, U.K., 2017.

[54] M. P. Barrett *et al.*, "Framework for improving critical infrastructure cybersecurity version 1.1," Nat. Inst. Standards and Technol., Gaithersburg, Maryland, USA, Tech. Rep., 2018. [Online]. Available: https://www.nist.gov/cyberframework, doi: 10.6028/NIST.CSWP.04162018.

[55] H. Boyes and R. Isbell, *Code Practice: Cyber Security for Ships*. London, U.K.: Institution of Engineering and Technology, 2017.

[56] A. Rana, "Commercial maritime and cyber risk management," *Saf. Defense*, vol. 5, no. 1, pp. 46–48, 2019.

[57] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, "A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels," *Rel. Eng. Syst. Saf.*, vol. 124, pp. 142–157, Apr. 2014.

[58] J. Nordström *et al.*, "Vessel TRIAGE: A method for assessing and communicating the safety status of vessels in maritime distress situations," *Saf. Sci.*, vol. 85, pp. 117–129, Jun. 2016.

[59] R. Svilicic J. Zec, "A study on cyber security threats in a shipboard integrated navigational system," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 364, Oct. 2019.

[60] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

[61] B. Svilicic, J. Kamahara, J. Celic, and J. Bolmsten, "Assessing ship cyber risks: A framework and case study of ECDIS security," *WMU J. Maritime Affairs*, vol. 18, no. 3, pp. 509–520, Sep. 2019.
[62] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime cyber risk management: An experimental ship assessment," *J. Navigat.*, vol. 72, no. 5, pp. 1108–1120, Sep. 2019.
[63] B. Svilicic and I. Rudan, "Shipboard ECDIS cyber security: Third-party component threats," *Pomorstvo*, vol. 33, no. 2, pp. 176–180, Dec. 2019.
[64] K. Tam and K. Jones, "Situational awareness: Examining factors that affect cyber-risks in the maritime sector," *Int. J. Cyber Situational Aware.*, vol. 4, pp. 40–68, 2019.
[65] K. Tam and K. Jones, "Factors affecting cyber risk in maritime," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment*, 2019, pp. 1–8.
[66] R. Hanzu-Pazara, G. Raicu, and R. Zagan, "The impact of human behaviour on cyber security of the maritime systems," *Adv. Eng. Forum*, vol. 34, pp. 267–274, Oct. 2019.
[67] S. Karamperidis, G. Koligiannis, and F. Moustakis, "Building a digital armour for the maritime sector against cyber-attacks," Tech. Rep., 2020.
[68] A. Androjna and E. Twrdy, "Cyber threats to maritime critical infrastructure," *Cyber Terrorism Extremism as Threat to Crit. Infrastructure Protection*. Ljubljana, Slovenia: Ministry Defence Republic, 2020.
[69] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU J. Maritime Affairs*, vol. 18, no. 1, pp. 129–163, Mar. 2019.
[70] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *J. Navigat.*, vol. 62, no. 2, pp. 173–187, Apr. 2009.
[71] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Trans.*, vol. 46, no. 4, pp. 583–594, 2007.
[72] G. D. Wyss and F. A. Durán, "OBEST: The object-based event scenario tree methodology," Sandia National Labs., Albuquerque, NM, USA, Tech. Rep. SAND2001-0828, 2001.
[73] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Quantitative cyber risk reduction estimation methodology for a small SCADA control system," in *Proc. 39th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2006, p. 226.
[74] D. I. Gertman, R. Folkers, and J. Roberts, "Scenario-based approach to risk analysis in support of cyber security," in *Proc. Int. Topical Meeting Nucl. Plant Instrum. Controls, Hum. Mach. Interface Technol.*, 2006, pp. 1–5.
[75] C. Beggs and M. Warren, "Safeguarding Australia from cyber-terrorism: A proposed cyber-terrorism SCADA risk framework for industry adoptionn," *J. Inf. Warfare*, vol. 7, no. 1, pp. 24–35, 2008.
[76] J. D. Markovic-Petrovic and M. D. Stojanovic, "An improved risk assessment method for SCADA information security," *Elektron. Elektrotechn.*, vol. 20, no. 7, pp. 69–72, Sep. 2014.
[77] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, "Privacy preservation intrusion detection technique for SCADA systems," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2017, pp. 1–6.
[78] T. Marsden, N. Moustafa, E. Sitnikova, and G. Creech, "Probability risk identification based intrusion detection system for scada systems," in *Int. Conf. Mobile Netw. Manage.* Cham, Switzerland, Springer, 2017, pp. 353–363.
[79] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg, and M. M. Hassan, "DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 16, 2021, doi: 10.1109/TITS.2021.3122368.
[80] R. Arul, S. Basheer, A. Abbas, and A. K. Bashir, "Role of deep learning algorithms in securing Internet of Things applications," in *Deep Learning for Internet Things Infrastructure*. Boca Raton, FL, USA: CRC Press, 2021, pp. 145–164.
[81] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, "Assessing cyber challenges of maritime navigation," *J. Mar. Sci. Eng.*, vol. 8, no. 10, p. 776, Oct. 2020.
[82] D. Trimble, J. Monken, and A. F. Sand, "A framework for cybersecurity assessments of critical port infrastructure," in *Proc. Int. Conf. Cyber Conflict*, 2017, pp. 1–7.
[83] P. M. Laso *et al.*, "ISOLA: An innovative approach to cyber threat detection in cruise shipping," in *Developments and Advances in Defense and Security*. Singapore, Springer, 2022, pp. 71–81.
[84] Q. Pan *et al.*, "Space-air-sea-ground integrated monitoring network-based maritime transportation emergency forecasting," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2843–2852, Mar. 2021.
[85] S. A. Chaudhry *et al.*, "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 22, 2021, doi: 10.1109/TITS.2021.3134643.
[86] C. Wang, J. Shen, P. Vijayakumar, and B. B. Gupta, "Attribute-based secure data aggregation for isolated IoT-enabled maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 1, 2021, doi: 10.1109/TITS.2021.3127436.
[87] X. He *et al.*, "DNS rebinding threat modeling and security analysis for local area network of maritime transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 22, 2021, doi: 10.1109/TITS.2021.3135197.
[88] A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani, and M. Boulares, "Path planning for energy management of smart maritime electric vehicles: A blockchain-based solution," *IEEE Trans. Intell. Transp. Syst.*, early access, Dec. 15, 2021, doi: 10.1109/TITS.2021.3131815.
[89] Z. Zheng, T. Wang, A. K. Bashir, M. Alazab, S. Mumtaz, and X. Wang, "A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid," *IEEE Trans. Comput.*, early access, Nov. 24, 2021, doi: 10.1109/TC.2021.3130402.
[90] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 15, 2021, doi: 10.1109/TITS.2021.3125402.
[91] D. Liu, Y. Zhang, W. Wang, K. Dev, and S. A. Khowaja, "Flexible data integrity checking with original data recovery in iot-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, Nov. 15, 2021, doi: 10.1109/TITS.2021.3125070.
[92] A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014.
[93] D. Seifert and H. Reza, "A security analysis of cyber-physical systems architecture for healthcare," *Computers*, vol. 5, no. 4, p. 27, Oct. 2016.
[94] G. Kavallieratos and S. Katsikas, "Attack path analysis for cyber physical systems," in *Computing Security*. Cham, Switzerland: Springer, 2020, pp. 19–33.
[95] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1361–1396, 2nd Quart., 2018.
[96] G. Kavallieratos and S. Katsikas, "Managing cyber security risks of the cyber-enabled ship," *J. Mar. Sci. Eng.*, vol. 8, no. 10, p. 768, Sep. 2020.
[97] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, "A novel risk assessment methodology for SCADA maritime logistics environments," *Appl. Sci.*, vol. 8, no. 9, p. 1477, Aug. 2018.
[98] I. Sceep. (2021). *Industry 4.0 and the Fourth Industrial Revolution Explained*. [Online]. Available: https://www.i-scoop.eu/industry-4-0/
[99] F. Tao, F. Sui, A. Liu, Q. Qi, M. Zhang, B. Song, Z. Guo, S. C.-Y. Lu, and A. Y. C. Nee, "Digital twin-driven product design framework," *Int. J. Prod. Res.*, vol. 57, no. 12, pp. 3935–3953, 2018.
[100] S. Frydenberg, K. Nordby, and J. O. Eikenes, "Exploring designs of augmented reality systems for ship bridges in Arctic waters," *Hum. Factors*, vol. 26, p. 27, Dec. 2018.
[101] S. D. Pizzo, A. De Martino, G. De Viti, R. L. Testa, and G. De Angelis, "IoT for buoy monitoring system," in *Proc. IEEE Int. Workshop Metrol. Sea, Learn. Measure Sea Health Parameters (MetroSea)*, Oct. 2018, pp. 232–236.
[102] A. Zolich *et al.*, "Survey on communication and networks for autonomous marine systems," *J. Intell. Robot. Syst.*, vol. 95, no. 3, pp. 789–813, 2019.
[103] K. Tam, K. Forshaw, and K. Jones, "Cyber-SHIP: Developing next generation maritime cyber research capabilities," in *Proc. Conf. ICMET Oman*, 2019.
[104] H. Oe and H. Nguyen, "Opportunities, challenges, and the future of cruise ship tourism: Beyond covid-19 with ubiquitous information sharing and decision-making," *Int. J. Manage. Decis. Making*, vol. 20, no. 3, pp. 221–240, 2021.
[105] G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, "Shipping 4.0: Security requirements for the cyber-enabled ship," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6617–6625, Oct. 2020.
[106] L. Kelion. (2018). *Ship Hack 'Risks Chaos In English Channel*. Accessed: Dec. 2, 2021. [Online]. Available: https://mfame.guru/ship-hack-risks-chaos-in-english-channel/
[107] C. Heij and S. Knapp, "Predictive power of inspection outcomes for future shipping accidents—An empirical appraisal with special attention for human factor aspects," *Maritime Policy Manage.*, vol. 45, no. 5, pp. 604–621, Jul. 2018.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.

[108] C. Park, W. Shi, W. Zhang, C. Kontovas, and C. Chang, "Cybersecurity in the maritime industry: A literature review," in *Proc. 20th Commemorative Annu. Gen. Assem.*, 2019, pp. 79–86.
[109] R. Sen, "Cyber and infomation threats to seaports and ships," *Maritime Secur.*, vol. 4, pp. 281–302, Dec. 2016.
[110] K. D. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," *Eng. Technol. Ref.*, vol. 1, 2012.
[111] R. Chia, "The need for ethical hacking in the maritime industry," *Soc. Nav. Architects Mar. Eng.*, vol. 38, pp. 108–121, Sep. 2019.
[112] D. Yang, Y. Zhou, W. Huang, and X. Zhou, "5G mobile communication convergence protocol architecture and key technologies in satellite Internet of Things system," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 465–476, Feb. 2021.
[113] M. Jia and Q. Guo, "Editorial: Intelligent cognitive internet of integrated space and terrestrial things," *Mobile Netw. Appl.*, vol. 24, no. 6, pp. 1924–1925, Dec. 2019.
[114] Y. Qian, L. Ma, and X. Liang, "The performance of chirp signal used in LEO satellite Internet of Things," *IEEE Commun. Lett.*, vol. 23, no. 8, pp. 1319–1322, Aug. 2019.
[115] *Solutions for NR to Support Non-Terrestrial Networks (NTN)*, document 38.821, 3GPP, 2019.
[116] M. Q. Vu, N. T. Dang, and A. T. Pham, "HAP-aided relaying satellite FSO/QKD systems for secure vehicular networks," in *Proc. IEEE 89th Veh. Technol. Conf.*, Apr. 2019, pp. 1–6.

Imran Ashraf received the M.S. degree (Hons.) in computer science from the Blekinge Institute of Technology, Karlskrona, Sweden, in 2010, and the Ph.D. degree in information and communication engineering from Yeungnam University, Gyeongsan, South Korea, in 2018. He has worked as a Post-Doctoral Fellow at Yeungnam University. He is currently working as an Assistant Professor with the Information and Communication Engineering Department, Yeungnam University. His research areas include positioning using next-generation networks, communication in 5G and beyond, location-based services in wireless communication, smart sensors (LIDAR) for smart cars, and data analytics.

Yongwan Park received the B.E. and M.E. degrees in electrical engineering from Kyungpook University, Daegu, South Korea, in 1982 and 1984, respectively, and the M.S. and Ph.D. degrees in electrical engineering from the State University of New York at Buffalo, USA, in 1989 and 1992, respectively. He worked at the California Institute of Technology as a Research Fellow from 1992 to 1993. From 1994 to 1996, he served as a Chief Researcher for developing IMT-2000 system at SK Telecom, South Korea. Since 1996, he has been a Professor of information and communication engineering at Yeungnam University, South Korea. From January 2000 to February 2000, he was an Invited Professor at the NTT DoCoMo Wireless Laboratory, Japan. He was also a Visiting Professor at UC Irvine, USA, in 2003. From 2008 to 2009, he served as the Director of the Technology Innovation Center for Wireless Multimedia, Korean Government. From 2009 to March 2017, he also served as the President of the Gyeongbuk Institute of IT Convergence Industry Technology (GITC), South Korea. He is also serving as the Chairman of 5G Forum Convergence Service Committee, South Korea. His current research interests include 5G systems in communication, OFDM, PAPR reduction, indoor location-based services in wireless communication, and smart sensors (LIDAR) for smart car.

Soojung Hur received the B.S. degree from Daegu University, Gyeongbuk, South Korea, in 2001, the M.S. degree in electrical engineering from San Diego State University, San Diego, in 2004, and the M.S. and Ph.D. degrees in information and communication engineering from Yeungnam University, South Korea, in 2007 and 2012, respectively. She is working as a Research Professor with the Mobile Communication Laboratory, Yeungnam University. Her current research interests include the performance of mobile communication, indoor/outdoor location, and unnamed vehicle.

Sung Won Kim received the B.S. and M.S. degrees from the Department of Control and Instrumentation Engineering, Seoul National University, South Korea, in 1990 and 1992, respectively, and the Ph.D. degree from the School of Electrical Engineering and Computer Sciences, Seoul National University, in August 2002. From January 1992 to August 2001, he was a Researcher at the Research and Development Center of LG Electronics, South Korea. From August 2001 to August 2003, he was a Researcher at the Research and Development Center of AL Tech, South Korea. From August 2003 to February 2005, he was a Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, USA. In March 2005, he joined the Department of Information and Communication Engineering, Yeungnam University, Gyeongsangbuk-do, South Korea, where he is currently a Professor. His research interests include resource management, wireless networks, mobile computing, performance evaluation, and machine learning.

Roobaea Alroobaea received the bachelor's degree (Hons.) in computer science from King Abdulaziz University (KAU), Saudi Arabia, in 2008, and the master's degree in information system and the Ph.D. degree in computer science from the University of East Anglia, U.K., in 2012 and 2016, respectively. He is currently an Associate Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His research interests include human–computer interaction, software engendering, cloud computing, the Internet of Thing, artificial intelligent, and machine learning.

Yousaf Bin Zikria (Senior Member, IEEE) is currently working as an Assistant Professor with the Department of Information and Communication Engineering, Yeungnam University, South Korea. He authored more than 100 refereed articles, conference papers, book chapters, and patents. His journal article's cumulative impact factor (IF) is more than 320. He published papers at the top venue, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, *IEEE Wireless Communications Magazine*, IEEE NETWORK, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, *Future Generation Computer Systems* (Elsevier), *Sustainable Cities and Society* (Elsevier), and *Journal of Network and Computer Applications* (Elsevier). He has managed numerous FT/SI in SCI/E indexed journals. His research interests include the IoT, 5G, machine learning, wireless communications and networks, WSNs, routing protocols, CRAHN, CRASN, transport protocols, VANETS, embedded systems, and network and information security. He also held the prestigious CISA, JNCIS-SEC, JNCIS-ER, JNCIA-ER, JNCIA-EX, and Advance Routing Switching and WAN Technologies certifications. He is listed in the world's top 2% of researchers published by Elsevier and Stanford University. GoogleScholar: https://scholar.google.com/citations?user = K90qMyMAAAAJhl = en Website: https://sites.google.com/view/ybzikria Researchgate: https://www.researchgate.net/profile/Yousaf-Zikria

Summera Nosheen received the Ph.D. degree from the School of Electrical Engineering and Computing, The University of Newcastle, NSW, Australia, in 2021. She is currently with the Faculty of Engineering, The University of Sydney, NSW, Australia. She received the Commonwealth Department of Education, Science and Training and The University of Newcastle Research Training Program (RTP) tuition fee and stipend scholarships. Her research interests include wireless networks, quality of service, quality of experience, and MAC layer resource allocation.

Authorized licensed use limited to: Zhejiang University. Downloaded on September 15,2024 at 04:17:19 UTC from IEEE Xplore. Restrictions apply.