

A Comprehensive Review of Cybersecurity Frameworks and Defense Mechanisms for Modbus and HTTP in Industrial Control Systems

LUKUMBA PHIRI, MUKUBESA KAMUTUMWA*

Department of Electrical Engineering,
University of Zambia, Lusaka,
ZAMBIA

**Corresponding Author*

Abstract: Industrial Control Systems (ICS) form the backbone of critical infrastructure, enabling automation and control in sectors such as energy, water, and manufacturing. The convergence of Operational Technology (OT) and Information Technology (IT) has introduced significant cybersecurity challenges, particularly for legacy communication protocols like Modbus and HTTP, which were not designed with security in mind. This paper provides a comprehensive framework for understanding the attack and defense mechanisms associated with two protocols i.e., Modbus and HTTP, used in ICS. We systematically analyze the inherent vulnerabilities of these protocols, survey proposed security enhancements including cryptographic solutions, intrusion detection systems, and security-by-design approaches, and evaluate existing cybersecurity frameworks such as MITRE ATT&CK, NIST CSF, and the Cyber Kill Chain. The review identifies a persistent gap in integrated, protocol-specific frameworks that address both attack simulation and defense validation in virtualized ICS environments. By synthesizing current research, this study highlights trends in threat modeling, machine learning-based anomaly detection, and the evolution of testbeds, providing a foundation for future work aimed at developing holistic security frameworks for Modbus and HTTP-based industrial networks.

Keywords: Industrial Control Systems (ICS), Modbus, HTTP, Cybersecurity, Threat Modeling, Intrusion Detection, Security Frameworks, Critical Infrastructure.

Received: April 19, 2026. Revised: May 12, 2026. Accepted: June 15, 2026. Published: September 30, 2026.

1 Introduction

Industrial Control Systems (ICS) are integrated hardware and software architectures designed to monitor and control industrial processes across critical infrastructure sectors, including power generation, water treatment, and manufacturing. Traditionally, ICS existed in isolation from the Internet, but business intelligence required tracking and managing their industrial networks by leveraging commercial networks instead of developing dedicated ICS networks for the best vision of their production, supply chain system [1]. The shift from ‘offline’ to ‘online’ ICS has unlocked new opportunities for efficient information sharing [2]. Improvements in cost and performance have encouraged this evolution and resulted in many of today’s “smart” technologies, such as the smart electric grid, smart transportation, smart buildings, smart manufacturing, and the Internet of Things (IoT) [3]. More innovative technologies are being developed, enabling remote access and control over the internet and within IT environments. This shift towards increased automation and connectivity aims to achieve substantial business

benefits. However, it also presents a challenge, as integrating ICS with external networks, such as the internet, expands the attack surface, making them more susceptible to cyber threats without proper security measures [4]. Although one of the oldest recorded incidents related to Industrial Automated Control Systems (IACS) cybersecurity dates back to the late 1990s, it was not until the 2010 Natanz nuclear power plant cyberattack (also known as Stuxnet) that IACS cybersecurity came under the spotlight [6].

ICS has been using complex proprietary communication protocols, such as Modbus, Profibus, DNP3, IEC, ICCP, OPC, etc. These communication protocols complete the ICS data exchange and acquisition, business monitoring, and many other important functions [7]. Modbus is the world's first truly bus protocol for industrial applications. Modbus protocol also appeared in many variants, such as those based on a serial link, MODBUS RTU, MODBUS ASCII, MODBUS PLUS, and MODBUS TCP, based on Ethernet. Modbus Protocol uses a master-slave structure and provides communication between devices that are connected to a different type of client/server [7]. In

the TCP/IP implementation, the Modbus protocol is sent as application-layer data. There is no authentication, authorization, or encryption of the protocol [8].

The most popular and widely adopted application protocol over the Internet is Hypertext Transfer Protocol (HTTP) [9]. The role of the internet signal within ICS is clear. It serves to transmit the messages through the ICS network and make the asset's devices talk with each other [10]. HTTP uses the synchronous communication model for peer-to-peer and request-response exchange of data [11].

Without integrity and authenticity, protocols such as Modbus/TCP are vulnerable to Man-in-the-Middle (MITM) attacks [5]. ICS are susceptible to various vulnerabilities. Trend Micro found that these vulnerabilities are mainly divided into several categories: 20% memory corruption, 19% poor management of login credentials, lack of authentication/ authorization mechanism, and insecure default value of 12%, and 9% of code injection vulnerabilities [12], [13]. Researchers have proposed various defensive strategies to protect ICS from cyber threats. Defensive cyber deception emerged as a potent strategy to enhance the cybersecurity of the ICS systems, encompassing various approaches such as monitoring, preplanned countermeasures, and deception techniques [13].

This literature review aims to synthesize current research on cybersecurity for Modbus and HTTP-based ICS. Specifically, we:

- i. Examine the inherent vulnerabilities of Modbus and HTTP protocols in industrial contexts.
- ii. Survey proposed defense mechanisms, including cryptographic solutions, network segmentation, and anomaly detection.
- iii. Analyze existing cybersecurity frameworks and evaluation methodologies.
- iv. Identify gaps in current research and suggest directions for future work.

The remainder of this paper is organized as follows: Section II discusses the evolution of ICS and the role of Modbus and HTTP. Section III discusses the threat landscape and attack vectors of ICS utilizing HTTP and Modbus, delving into historical incidents and emerging threats, and further exploring various attack vectors. Section IV discusses various defense mechanisms and security enhancements, including cryptographic solutions, network security measures, intrusion and anomaly detection, as well as security by design and security enhancements. Section V

discusses cybersecurity frameworks such as NIST, STRIDE, and MITRE, and the three types of evaluation testbeds, which are physical, virtual, and hybrid. Section VI discusses research gaps and suggests future directions. Section VII marks the conclusion of this paper.

2 Industrial Control Systems: Evolution and Protocol Landscape

2.1 The Evolution from Isolated to Connected Systems

The First Industrial Revolution, also known as Industry 1.0, began in England in 1760, revolutionizing production methods by shifting from manual labor to machine-based processes. The Second Industrial Revolution (Industry 2.0) spanned from 1871 to 1914 and brought further technological advancements, such as electricity and the development of the assembly line. The Third Industrial Revolution, also known as the Digital Revolution or Industry 3.0, began in the 1970s. This era saw the integration of digital technologies into manufacturing, with innovations like computers, microprocessors, and PLCs. The Industry 4.0 denomination was coined within a strategic program of the German Government called Digital Agenda that started in 2009. Known as Industrie 4.0 in Germany, it was presented at the Hanover Fair in 2011 and started a new wave of developments for the digital industry [14]. Industry 4.0 combines physical and digital technologies, such as the IoT, artificial intelligence (AI), and cloud computing. By interconnecting machines, sensors, and data systems, Industry 4.0 in manufacturing enables greater efficiency, flexibility, and data-driven decision-making [15]. With this development comes the need of qualified individuals to program, protect and manage this new technology, thereby shaping the education sector. While Industry 4.0 is expected to enable interconnection and digitization in traditional industries, the current state of production processes still lacks the necessary interoperability for information exchange, especially concerning legacy equipment [14]. A challenge we have found with various Industry 4.0 frameworks is that the solutions they provide are conceptual and hard to implement in real factories. Another being the cost of changing ICS components such as field buses, task often times proves to be unrealistic but available literature often under mines its gravity. Instead of effectively promoting convergence,

Industry 4.0 has led to protocol proliferation, increasing system complexity and integration overhead.

Figure 1 illustrates the industrial evolution from Industry 1.0 to Industry 4.0.

While Industry 4.0 is expected to enable interconnection and digitization in the traditional industries, the current state of production processes still lacks the necessary interoperability for information exchange, especially concerning legacy equipment [14]. A key challenge we have identified with various Industry 4.0 frameworks is that the solutions they provide remain conceptual and difficult to implement in real factories. Furthermore, the cost of replacing ICS components such as field buses often proves unrealistic, yet available literature frequently underestimates this gravity. Instead of effectively promoting convergence, Industry 4.0 has, in practice led to protocol proliferation, increasing system complexity and integration overhead.

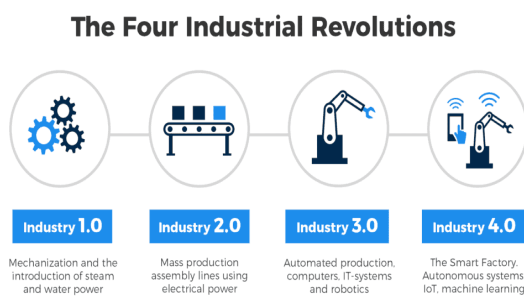


Figure 1: Illustrating industrial evolution [15].

2.2 Modbus Protocol: Design and Limitations

The Modicon Communication Bus (Modbus) [2] is one of the most widely used industrial communications protocols, especially in industrial control applications, energy management, and building automation systems [16]. The Modbus network protocol was designed in 1978 by Modicon Inc. It provided an efficient method to transmit control data between controllers and sensors using mainly an RS232 port [17]. Conventional Modbus messages can be packaged in RTU or ASCII frames and packed with a TCP/IP interface so that they can be routed over the Internet [18]. Due to the emerging need for fast, reliable multipoint communication, a network is laid out where a master can communicate with multiple slaves at a time or can have point-to-point communication [19]. A typical Modbus network supports one master and a

maximum of two hundred forty-seven slaves [20]. The simplicity and reliability of Modbus/TCP in transmitting data related to sensors and actuators have driven its extensive use [2].

The Modbus TCP/IP protocol establishes standards for client/server communication between devices on Ethernet TCP/IP networks or other bus systems. The protocol employs a simple application data unit (ADU) format to ensure compatibility among various devices, regardless of the devices in use. The entire Modbus packet is embedded within the data section of the TCP packet and transmitted over the network [21]. Modbus TCP/IP uses two types of ADUs: request and response frames, both containing the Modbus application protocol (MBAP) header, function code, and data segment [21].

Modbus has certain limitations with regard to current requirements for automation and control systems, including low transmission rates, limited numbers of networked devices, single master topologies, and the absence of mechanisms for correcting messages corrupted by transmission errors [16]. While Industry 4.0 promotes distributed automated systems, the master-slave architecture of Modbus is centralized that creating a fundamental architectural mismatch. All slaves in Modbus must be predefined, this prevents the plug and play interoperability essential to dynamic Industry 4.0 environments. The lack of authentication and encryption in Modbus creates a big gap in cybersecurity which is essential to industry 4.0 systems.

2.3 HTTP Protocol in Industrial Environments

The most popular and widely adopted application protocol over the Internet is the hypertext transfer protocol (HTTP) [22]. It has been in use by the World-Wide Web global information initiative since 1990 [23]. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet. The current version of the protocol is HTTP/1.1, which adds a few extra features to the previous 1.0 version. HTTP provides a general framework for access control and authentication, via an extensible set of challenge-response authentication schemes, which can be used by a server to challenge a client request and by a client to provide authentication information [23].

The HTTP/1.1 protocol can perform optimizations such as keep-alive (an indicator for connection operation) connections, chunked transfer encoding, byte-range requests, and request pipelining. A limited connection between client and server makes a series of requests to wait for one request to complete before it can fire it off. This condition is termed head-of-line (HoL) blocking in HTTP/1.1, and it is a major drawback of this protocol. This happens when several requests rise on the web servers. The protocol fails to respond even to small requests due to the limited resource volume size on the server side. Hence, it fails to use the transport control protocol (TCP) effectively [22]. The extensive use of the internet has resulted in novel technologies and protocol improvisation. HTTP/1.1 is widely adopted on the Internet. However, HTTP/2 is found to be more efficient over transport control protocol (TCP). The HTTP/2 protocol can withstand the payload overhead when compared to HTTP/1.1 by multiplexing multiple requests. However, both protocols are highly susceptible to application-level denial of service (DoS) attacks [22]. The role of the internet signal within ICS is clear. It serves to transmit the messages through the ICS network and make the asset's devices talk with each other [14]. However, it needs a gateway to exchange data over the internet. HTTP uses the synchronous communication model for peer-to-peer and request-response exchange of data [11]. Figure 2 shows HTTP in Industrial Systems.

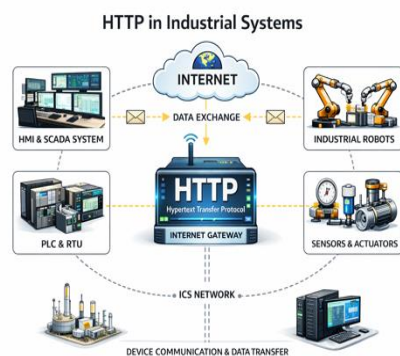


Figure 2: HTTP in Industrial Systems [11].

2.4 The Convergence of IT and OT

ICS is composed of two main zones: The Operational Technology (OT) network, which consists of hardware and software used to monitor and control industrial processes, and the Information Technology (IT) network used for information processing using workstations, servers, and databases [24]. OT machinery long

predates modern computer networks. Specialized industrial devices like programmable logic controllers (PLC) and distributed control systems (DCS) operate advanced automation with embedded firmware and proprietary protocols. They power machinery, retrieve sensor data, and directly control real-time processes, often in hazardous production environments. In contrast, enterprise IT ecosystems emphasize Windows or Linux computers, IP-based networking, and cloud-enabled software [25]. Originally, OT and IT were independent concepts in the industrial domain [24], each optimized for different objectives, OT focused on reliability and safety while IT focused on scalability and data processing. However the convergence of these two technologies has given networking capabilities to ICS, enabling cost savings and flexibility in the remote management and monitoring of industrial processes with the use of cyber-components [24]. The integration facilitates operational efficiency, cost reduction and enhanced monitoring capabilities by incorporating cyber-components and network communication technology. Despite these advantages, the integration of the OT and IT worlds introduces significant security implications. By connecting traditionally isolated OT systems to digital environment, ICS infrastructures inherit many of the vulnerabilities associated with IT networks, thereby significantly expanding the surface for potential cyberattacks. Consequently, emphasizing the urgent need for more robust mechanisms to ensure the security of assets and safety of human workers as a top priority [26]. Figure 3 illustrates the convergence of IT and OT.

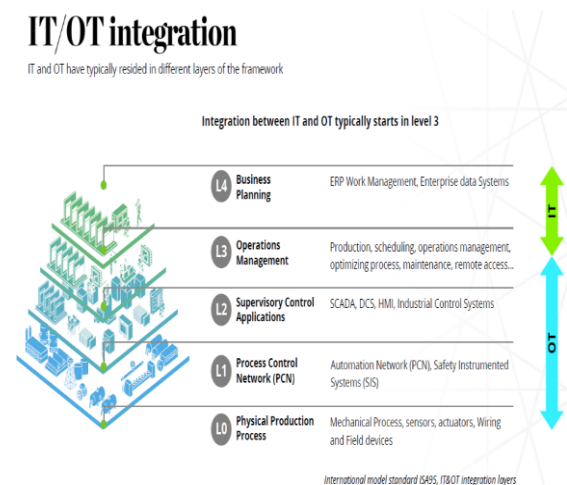


Figure 3: Convergence of IT and OT [27].

3 Threat Landscape and Attack Vectors

3.1 Historical Incidents and Emerging Threats

The threat landscape for ICS is diverse and continually evolving. Cyberattacks targeting ICS can have a devastating impact, ranging from operational disruptions to safety hazards. Several attack vectors are particularly relevant for Modbus and HTTP protocols. Only the implementation, efficiency, and reliability of the Modbus protocol were considered, and security issues were not taken into account when it was designed [7]. Thus, Modbus and HTTP protocols in ICS face significant cybersecurity challenges due to inherent weaknesses and evolving attack methodologies [28].

Traditionally, ICS depend on standard security measures, while most current attacks on ICS networks fall under the category of Advanced Persistent Threats (APTs) [2]. By design, the presence of APT attacks goes invisible to the victim, allowing attackers to steal information over a long period of time [29]. Amer et al. 2025 [2] study states that detecting these complex APT attacks requires systems that can capture long-term causal and contextual information about the fine-grained behaviors of hosts. While Buchta et al (2024) in [30] state that various methodologies can be used to detect APT attacks, among them are Rule-based, Anomaly-based, statistical, classification, and Human Knowledge methodologies. Several attacks have targeted industrial facilities and their devices, from the Stuxnet in 2010, to the Trojan Black Energy in 2015 and Mirai in 2016, to recent ransomware attacks, such as the Wanna Cry in 2017 or the Locker Goga in 2019, resulting in operational and financial impact for affected companies [31]. The 2021 Colonial Pipeline cyberattack exposed the weakness and highlighted the importance of the supply systems, it marked a turning point in the history of cyberattacks on critical infrastructure. This attack was planned by the Dark-Side ransomware group. It temporarily shut down one of the largest fuel pipelines in the United States, which caused major fuel shortages, financial problems, and concerns about national security [32].

Table 1. Cyber Threat Landscape

S N	Referenc e	Type of Attack and Attack Vectors Exploited	System Targete d
1.	[33]	Modbus command injection, e.g., False Command Injection (FCI), False Access Injection (FAI), and False Response Injection (FRI)	PLCs
2.	[34]	Man-in-the- Middle Attack on HTTP communicatio ns	Web- based Control Interfac es
3.	[35]	Distributed Denial of Service (DDoS) Attack exploiting HTTP vulnerabilities	Web Servers and ICS Network
4.	[21]	Exploitation of Modbus Protocol for Command Spoofing	Industri al Devices and Sensors

3.2 Attack Taxonomy for Modbus and HTTP

1. Reconnaissance

A reconnaissance attack, also known as information gathering, is the first phase of a cyber-attack. It is an unauthorized retrieval of information about a target to identify vulnerabilities that an attacker can exploit. It helps the attacker or penetration-tester select the best tools and methods to carry out a successful attack on a target. It is a very dangerous attack that could directly impact the magnitude of the effect of a completed attack. Reconnaissance can be passive or active. Passive reconnaissance is more like a light, non-in-depth approach to gathering information on a target. This goes on without

alerting the target. An active reconnaissance is a more in-depth approach to gathering information on a target, and this alerts the target [36]. Reconnaissance attacks help the attacker derive a map of the target network and its IP addressing scheme. The information collected in reconnaissance attacks is used to identify exploitable vulnerabilities that can be used in future attacks. Reconnaissance is usually followed by the weaponization, delivery, and exploitation steps [37].

2. Spoofing and Injection

Among the most dangerous types of attacks is Domain Name System (DNS) spoofing. DNS spoofing involves redirecting traffic to malicious websites by altering domain name resolutions, enabling attackers to steal sensitive data or manipulate network traffic. This attack can lead to Man-in-the-Middle (MitM) scenarios, where hackers gain unauthorized access to the network, exposing private data and compromising system reliability. The potential impact of such an attack extends beyond privacy concerns [38]. As HTTP queries, a web application accepts input and produces SQL statements as output. The SQL statements created are sent to the database of the web application to collect, store or change the values according to the user's purpose. Here, HTTP requests are specifically interested in SQL statement building. The SQL Injection attack occurs when HTTP requests are not approved. The malicious user will manage unsecured HTTP requests to form a new statement that causes the user harm. The source procedure, for example, uses an HTTP request to create a SQL statement [38].

3. Denial-of-Service

Denial-of-Service (DoS) attacks represent one of the most persistent and evolving threats in the cybersecurity landscape. These attacks aim to disrupt the normal functioning of targeted systems by overwhelming them with traffic or requests, rendering services unavailable to legitimate users [39]. A teardrop attack is a DoS attack that intends to crash the target by transmitting overlapping fragmented packets, thus severing the communication between the target and the other devices. In particular, the attacker sends fragmented Modbus/TCP packets with overlapping or scrambled fragment offsets to violate the fragmentation process. The Modbus payload can consist of either random or specific values [40]. Flag Flood belongs to the DoS category. In particular, it tries to flood the target by using a plethora of TCP packets with specific flags

(ACK, FIN, SYN, and RST) [40]. The Port Pool Exhaustion aims to deplete the available bandwidth of the target. When this attack module is activated, a plethora of concurrent threads is generated to connect to the target Modbus TCP port for a particular time duration, thus destroying the Modbus communication [40].

4. Teardrop attack [2] is a DoS attack, which intends to crash
 5. the target by transmitting overlapping fragmented packets,
 6. thus severing the communication between the target and the
 7. other devices. In particular, the attacker sends fragmented
 8. Modbus/TCP packets with overlapping or scrambled fragment
 9. offsets in order to violate the fragmentation process. The Mod-
 10. bus payload can consist of either random or specific values
- Teardrop attack is a DoS attack, which intends to crash the target by transmitting overlapping fragmented packets, thus severing the communication between the target and the other devices. In particular, the attacker sends fragmented Modbus/TCP packets with overlapping or scrambled fragment offsets in order to violate the fragmentation process. The Mod- bus payload can consist of either random or specific values.

1. Replay Attacks

Replay attacks, often referred to as playback attacks, are a sort of network assault in which honest data transfer has been repeated or purposefully delayed. The perpetrator of this assault could be the one who sent the original data, or an adversary who intercepted and retransmitted it, probably as part of an IP replacement packet spoofing attempt. This technique is regarded as one of the more basic man-in-the-middle attacks. "One way to characterize such an attack is": "an attack on a security protocol using a replay of messages in the intended (or initial and expected) sense from a separate context, thereby fooling the honest participant(s) into believing that the protocol run was completed" [41]. The response delay attack belongs to the category of replay attacks. It utilises first an ARP poisoning attack in order to insert the attacker between the two communication points. Thus, the attacker can obtain the exchanged request packets and send the appropriate responses with a specific delay time. In other words, the response packets are transmitted only by the attacker with a specific delay. Such delays can

have disastrous consequences in an industrial environment [40]. The baseline response replay attack aims at confusing or even interrupting the communication between two endpoints by capturing and replaying the information sent between two devices. Specifically, the attacker executes an ARP poisoning attack to receive the exchanged traffic. Next, some of the packets are replayed to the destination [40]. Only the implementation, efficiency, and reliability of the Modbus protocol were considered, and security issues were not taken into account when it was designed [7]. Thus, Modbus and HTTP protocols in Industrial Control Systems (ICS) face significant cybersecurity challenges due to inherent weaknesses and evolving attack methodologies. It allows its exploitation by malicious software or unauthorized users (hackers), as it can easily be intercepted and altered in the middle of communication (man-in-the-middle attack), sending malicious (false command injection), malformed (false access injection), or delayed (replay attacks) data packets that lead to a denial of service (DoS) of the system [28].

Table 2. Summary of Attack Taxonomy

S N	Referen ce	Attack Taxonomy
1.	[36]	Reconnaissance
2.	[38]	Spoofing and Injection
3.	[39]	Denial-of-Service
4.	[41]	Replay Attacks

4 Defense Mechanisms and Security Enhancements

Traditional industrial protocols, such as Modbus TCP/IP, lack fundamental security features like authentication, integrity, verification, and encryption, making Industrial Control Systems (ICS) vulnerable to cyber threats [42]. It is crucial to implement sufficient safety measures to enhance the security [43]. Key precautions involve limited perimeters, patch management, robust cryptography, and, notably, segregating the control network and corporate network through the defense-in-depth approach [43]. Recently, there has also been a considerable interest in the use of emerging technologies such as Digital Twins (DT), Software Defined Networking (SDN), Network Function Virtualisation (NFV), Cloud, Edge Computing (ED), Fog Computing, Machine learning, and Blockchain for enhancing security in ICS [44].

SDN, NFV, and DT technologies provide specific mechanisms to secure critical infrastructures [44]. For instance, the SDN Controller having an overall visibility over its network can help to achieve better situational awareness with respect to detecting attacks. NFV can provide dynamic enforcement of security policies. DT enables representation of a holistic critical environment using virtualisation technology for researchers to visualize and analyse the impact of attacks and use data analytics to predict the consequences of ongoing attacks [44]. However, these technologies also have their own limitations. For instance, the overall network view available at the SDN Controller can itself be vulnerable to cyber threats. Issues such as real-time updates and a single point of failure can affect the availability of the SDN Controller. Dynamic placement of security functions using NFV can itself increase the security vulnerabilities, and DT can also result in attacks being transferred from DT to ICS networks [44].

4.1 Cryptograph Solution

By introducing cryptographic proxies acting as intermediaries between PLCs and external clients like Human Machine Interfaces (HMIs), we ensured secure communication while maintaining compatibility with existing industrial infrastructures [42]. Traditional SCADA standards such as IEC 60,870, DNP3, IEC 61,850, and Modbus are known to have various security limitations. However, the AGA-12 standard has been developed to provide improved security features compared to these traditional standards [43]. AGA-12 incorporates three primary algorithms, namely, AES with a minimum key length of 124 bits, RSA with a minimum key length of 1024 bits, and ECDSA with a key length of at least 160 bits, along with SHA-1 for cryptographic operations. These algorithms are utilized in AGA-12 to ensure confidentiality, integrity, and authentication [43]. Implementing well-designed key exchange and management systems is essential for maintaining the security and resilience of SCADA-based ICS [43]. These systems are responsible for establishing and managing cryptographic keys that are used to secure communication channels, authenticate users and devices, and protect sensitive information in the SCADA environment [43].

Mathematical analysis of computational overhead: In resource-constrained PLC environments, the choice of cryptographic algorithm significantly impacts performance. Let

us define the computational complexity for encryption operations:

- **AES (symmetric encryption):** $O(n)$ where n is the block size. For a message of L length bits, AES requires approximately $L/128$ rounds of 10/12/14 cycles depending on key size (128/192/256 bits respectively). This linear complexity makes AES suitable for real-time industrial communication.

- **RSA (asymmetric encryption):** $O(k^3)$ where k is the key length in bits. For RSA-1024 ($k=1024$), modular exponentiation requires $O(\log k)$ multiplications of $O(k^2)$ bit complexity, yielding $O(k^3)$ overall. This cubic relationship means RSA-2048 is approximately 8x more expensive than RSA-1024.

For a typical PLC with constrained processing capabilities, the latency L can be expressed as equation 1:

$$L_{\text{encrypt}} = C_{\text{process}} \times O(f(\text{algorithm})) + C_{\text{transmit}} \quad (1)$$

Where C_{process} depends on processor speed, and C_{transmit} presents network transmission latency. Empirical studies suggest AES-128 introduces approximately 1 – 5 ms overhead, making RSA impractical for real-time control loops with sub-100ms deadlines.

Implementing well-designed key exchange and management systems is essential for maintaining the security and resilience of SCADA-based ICS. These systems establish and manage cryptographic keys used to secure communication channels, authenticate users and devices, and protect sensitive information in SCADA environments [43].

4.2 Network Security Measure

To mitigate the increasing cyber threats targeting ICS, many government advisory reports and industrial standards propose Defense-in-Depth (DID) as the best practice to defend ICS [45]. DID aims to protect a system by establishing a multi-layer defense by combining various defensive controls, such as advanced firewalls with DMZ, security awareness training programs, a vulnerability management system, intrusion detection with effective access policies, and incident response mechanisms [45]. A DID approach applies security measures at multiple layers to provide robust protection. It usually includes data encryption, access control policies, an intrusion detection system, etc [46]. At the policy level, guidelines establish rules for processes like access control and patch

management. Best practices need to be defined for processes like access management, patching, and backup [47]. The process layer involves technical protections such as firewalls, intrusion detection, and authentication controls. At the process layer, technologies like firewalls, intrusion detection systems, and access controls provide protection. Finally, the technology layer strengthens security at the network, endpoint, and data levels through encryption, firewalls, whitelisting, and antivirus software [47]. And, at the technical level, encryption, VPNs, and traffic filtering safeguard communications, while endpoint security is strengthened through hardening, whitelisting, and antivirus tools. Data encryption is used to ensure the confidentiality of data transmission, usage, and storage. The access control policy is a direct way to protect the ICS from hostile detection [46]. And the intrusion detection system is a commonly used way to monitor malicious activity or policy violations in the ICS [46]. However, as there are numerous controls involved, it needs a deployment plan to [46] optimally distribute the defensive resources over those controls before such practice could produce the most effective protection with limited resources [45]. Only a comprehensive DID strategy implementing complementary controls across policy standards, operational workflows, and technical defenses can adequately counter cyber threats by targeting modern operational technology environments [47]. Otherwise, the high financial and managerial costs make defense-in-depth impractical to fully implement [45].

4.3 Intrusion Detection and Anomaly Detection

Intrusion detection system (IDS) [48] represents a critical layer of defense within a cybersecurity framework. By monitoring network traffic and system activities for signs of malicious behavior or policy violations, IDSs provide organizations with the ability to detect and respond to threats in real time. The classification of IDSs is a complex task, as different systems are designed to address specific operational environments, threat models, and performance requirements. Broadly speaking, IDSs can be categorized into NIDSs, HIDSs, and hybrid IDSs, with additional distinctions based on detection methodology, such as signature-based, anomaly-based, and specification-based systems [49].

Anomaly detection creates a model of “normal” system behaviour and processes, such as logs, network information, or users’ activities, to build and keep a historical record. After a baseline

is built, all deviations from it—whether unintentional or intentional—are labelled as anomalies. Detection models include statistical methods (e.g., z-scores, moving averages), clustering algorithms (e.g., DBSCAN, k-means), as well as machine learning techniques that classify behaviours based on learned patterns [50]. A novel approach for anomaly detection by modeling device interactions on the network through the analysis of Modbus frame sequences using a Non-deterministic Finite Automaton (NFA) framework, termed the Modbus-NFA Behavior Distinguisher (MNBD) model [2]. NFA is a computational model designed for pattern recognition and the representation of regular languages [2]. It extends the concept of a Deterministic Finite Automaton (DFA) by incorporating additional flexibility. NFAs are crucial in theoretical computer science, with significant applications in formal language theory, automata theory, and compiler construction. They are widely used in practical domains such as lexical analysis, pattern matching, and network protocol verification [2]. The NFA framework is particularly effective for this purpose as it can represent multiple potential states and transitions within a network, thereby capturing the complexity and variability of network behaviors. This capability allows the MNBD model to detect deviations from normal behavior, identifying potential anomalies with high accuracy. The MNBD model was evaluated against several existing ICS network traffic datasets. The results demonstrate that the Modbus-NFA approach not only surpasses traditional machine learning models but also outperforms sequence-based deep learning models [2].

The MNBD model represents Modbus communication patterns as a Non-deterministic Finite Automaton (NFA), defined as equation 2: $N=(Q,\Sigma,\delta,q_0,F)$ (2) where: Q = finite set of states representing valid Modbus communication stages, Σ = input alphabet (Modbus function codes, e.g., read/write operations), $\delta:Q\times(\Sigma\cup\{\epsilon\})\rightarrow 2^Q$ transition function, $q_0\in Q$ initial state, $F\subseteq Q$ = set of accepting (legitimate) states.

The proposed MNBD model, consists of two primary phases: the training phase and the testing phase. The training phase encompasses three key stages: data chunking, data preprocessing, and traffic modeling. In the testing phase, the same data chunking procedure from the

training phase is utilized and a new stage called Maximum Likelihood Model Fitting is introduced.

In the proposed approach, NFA is modified to model Modbus data by implementing two key changes. First, accept states are deemed unnecessary because the intrusion detection system continuously monitors an ongoing and repetitive data stream. Instead, an NFA where each state transition, as defined by the transition function δ , is paired with a specific action is used. Any deviation from the expected data pattern triggers a δ transition that is associated with an error action, potentially raising an alert in the intrusion detection system depending on the severity of the deviation. Additionally, the start state is defined as the state corresponding to the first identified query within the periodic traffic pattern. [2]. ICS Honeynets are virtual simulations of real ICS systems, which are used to prevent hackers from attacking real systems [12]. There are many different types of honeypots, ranging from emulating specific services such as SSH to a fully-fledged system running several services at the same time [51]. The goal of a honeypot is to lure attackers into targeting it [51]. The honeynet is very suitable for collecting various realistic statistics, such as current hacker attack trends, methods, tools, hacker's geographic location, number of attacks, and other analysis information [12]. Although there is almost no statistical information available for these new systems, they are likely to reveal the scale of the attack on the ICS system and the complexity of the attackers. But ICS Honeynets does provide information that can help improve the security of the ICS system [12].

4.4 Security-by-Design and Zero Trust

Zero Trust is a model where different elements of the architecture do not implicitly trust each other, but there is a continuous identification and authorization process for all the components [52]. The Zero Trust security model is a set of principles and strategies based on the awareness that cyber threats exist and can originate from outside but also inside the perimeter of traditional networks [52]. It is a cybersecurity strategy that shifts from a location-centric to a more data-centric approach for better security controls between users, systems, data, and assets that may change over time [53]. Hence, everything must be tailored to the specific needs and goals of the infrastructure to which we want to apply it [52]. Security professionals must eliminate the idea of untrusted networks and trusted networks (internal networks),

as it considers all network traffic to be untrusted and upholds the following three fundamental principles: all entities are untrusted by default, the least privilege access is enforced, and comprehensive security monitoring is implemented [28]. Zero trust offers numerous benefits, such as a streamlined security stack, reduced operational overhead, and more efficient and flexible onboarding of employees and vendors [53]. Despite the growing interest in trust management frameworks, the cybersecurity community still grapples with significant challenges. Trust management involves complex decision-making, relationship assessment, and the need for continuous adaptation to emerging threats [54].

Security-by-design [55] requires manufacturers and system integrators to implement cybersecurity measures from the design phase, adhering to the principles of security by design [55]. Effective cybersecurity, however, extends beyond merely deploying dedicated protective components such as firewalls. Instead, it results from a combination of factors, including system architecture, component selection criteria, configuration strategies, and operational requirements [55]. Additionally, security requirements are often intertwined with and dispersed across system functional requirements. Consequently, neglecting security during the early development lifecycle complicates the integration of its requirements in later phases [55].

The Modbus Organization has laid out a specification for secure data transmission through the Modbus-TCP Security protocol using Transport Layer Security (TLS) [56]. This new variant guarantees the integrity and the confidentiality of the session that is established between the client device and the server through PKI (public key infrastructure) and also proposes the transmission of RBAC (role-based access control) information using X.509v3 certificate extension [28]. However, with the rapid evolution of TLS, standards quickly become obsolete by the time new industrial devices are introduced [56].

In order to include security mechanisms in the protocol, in October 2018, the Modbus organization released security specifications, which provide robust protection through the blending of Transport Layer Security (TLS) with the traditional Modbus protocol. TLS will encapsulate Modbus packets to provide both authentication and message integrity protection. The security features leverage X.509v3 digital certificates for the authentication of both the server

and the client. The protocol also supports the transmission of RBAC information using an X.509v3 extension to authorize the request of the client [57].

Table 3. Defense Mechanisms and Security Enhancements.

SN	Reference	Type of Mechanism	Merits	Demerits
1.	[42]	Cryptographic Solutions	Ensures secure communication; compatible with existing infrastructure	Complexity in implementation; management of cryptographic keys can be challenging
2.	[43]	AGA-12 Security Standard	Incorporates strong algorithms (AES, RSA, ECDSA) for confidentiality and integrity	Limited adoption; may require updates to legacy systems.
3.	[45]	Defense-in-Depth (DiD)	Provides multi-layered protection; combines various defensive controls	High financial and managerial costs; it can be impractical to fully implement
4.	[48]	Intrusion Detection	Real-time monitoring and	Potential for false positive

		Syste ms (IDS)	respons e to threats	s; requires continu ous tuning and updates
5.	[2]	Anom aly Detect ion using Modb us- NFA	High accurac y in detectin g deviat ions from normal behavio r	Comple xity in establis hing baselin e behavio r may require extensi ve training
6.	[12]	ICS Honey nets	Collect s data on attack trends and techniq ues; helps improv e overall security	Resour ce- intensiv e; may not provide real- time protecti on
7.	[52]	Zero Trust Model	Enhanc es security by treating all traffic as untruste d; reduces risk of insider threats	Implem entation comple xity requires cultural change and compre hensive monitor ing
8.	[55]	Securi ty-by- Desig n	Integrat es security from the design phase; address es	Neglect ing security in early phases complic ates later

			security in the develop ment lifecycl e	integrat ion.
9.	[56]	Modb us- TCP Securi ty Protoc ol with TLS	Guarant ees integrit y and confide ntiality; modern izes traditio nal Modbu s	Rapid evoluti on of standar ds may lead to obsoles cence; it requires ongoing updates

5 Cybersecurity Frameworks and Evaluation Testbeds

Several cybersecurity frameworks and evaluation testbeds exist to guide organizations in improving the security of ICS.

5.1 Standardized Frameworks

5.1.1 The ICSSIM Framework

The ICSSIM framework is a tool to build customized virtual and semi-virtual ICS security testbeds that enable researchers to research and experiment with cyber threats on their local testbed [58]. ICSSIM testbeds could be used to develop and evaluate AI-based Intrusion Detection Systems (IDS) [58]. We can utilize ICSSIM testbeds to investigate physical process disruptions induced by cyber incidents and leverage them for intrusion detection. We can also evaluate the physical impacts of cyber-attacks to estimate the risk posed by a particular incident. Attack simulations on testbeds can reveal ICS vulnerabilities in industrial protocols and architecture, thereby opening the door for preventive or mitigation strategies [58]. Figure 4 illustrates the ICSSIM reference architecture.

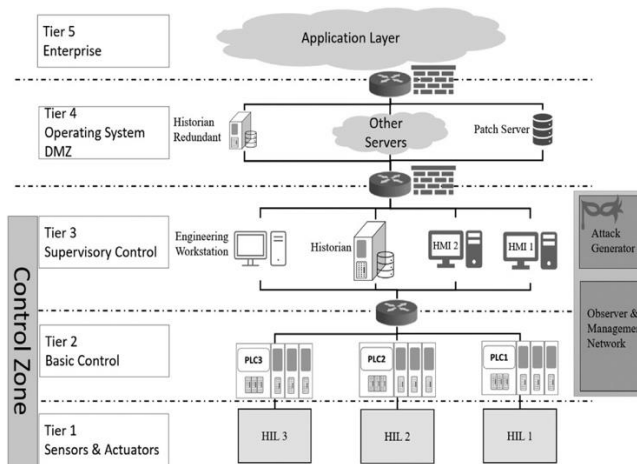


Figure 4: ICSSIM reference architecture [58].

5.2.2 MITRE

Developed in 2013 as part of MITRE's Fort Meade Experiment (FMX), MITRE ATT&CK is a research initiative aimed at enhancing forensic analysis of cyberattacks by emulating adversarial and defensive tactics [59]. MITRE ATT&CK (or Adversarial Tactics, Techniques, and Common Knowledge) is a curated knowledge base that details cyber adversary behavior across various domains, including enterprise, mobile, and industrial control systems (ICS) [59]. It is a widely adopted tool for enhancing cybersecurity, supporting threat intelligence, incident response, attack modeling, and vulnerability prioritization [59]. Organized into matrices, ATT&CK outlines specific adversarial tactics (high-level objectives) and techniques (specific actions) that describe how an attacker seeks to compromise or persist in a system [59]. By enabling the mapping of adversarial tactics, techniques, and procedures (TTPs), ATT&CK enhances the systematic detection and analysis of cyber threats, particularly advanced persistent threats (APTs) [59]. The framework serves as a comprehensive knowledge base of real-world adversarial techniques, focusing on how attackers interact with systems rather than the tools or malware they use. It is structured around four core components: tactics (adversarial goals), techniques (methods to achieve goals), sub-techniques (detailed methods breaking down techniques), and documented usage (procedures and metadata) [59]. Each TTP in MITRE ATT&CK comes with a mitigation strategy that provides solutions to protect critical infrastructures [60]. Therefore, it can help reliably predict and mitigate various types of threats that attackers pursue after an initial intrusion [60]. It addresses the why, how, and who is cyber-attacking a digital infrastructure [61]. It has been widely accepted by

both the research society and the industrial domain and has already met numerous applications varying from adversary emulation, red teaming, behavioral analytics development, to a defensive gap and SOC (Security Operations Center) maturity assessment [61]. It has been used as a foundation for threat modeling in different sectors, such as government, academia, and industry [62]. In September 2020, McAfee and the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC), surveyed security leaders across 325 large (with more than 5000 employees) and medium-sized (with more than 1000 employees) enterprises in the United Kingdom, United States, and Australia. Fifty-seven percent of the survey respondents were large enterprises, and 62% had an in-house security operations center. Diverse sectors were targeted, including IT, technology and telecoms, retail, transport, financial services, manufacturing, and production. Based on their findings, more than 80% of enterprises use MITRE ATT&CK for threat protection. Furthermore, 57% of those participating in the survey declared they use MITRE ATT&CK to determine gaps in deployed security solutions in their enterprise, with 55% recommending it for security policy implementation and 54% using it for threat modeling [61]. By studying MITRE ATT&CK knowledge base and extracting its statistical insights, significantly valuable recommendations and defensive strategies can be issued that cybersecurity experts can apply to digital products, solutions, and services [60]. To enrich the MITRE ATT&CK knowledge-base, individuals and organizations continuously share various threat intelligence data and information, such that cybersecurity professionals integrate this information into the knowledge-base as threat profiles, tactics, techniques, etc [60]. Figure 5 illustrates the MITRE ATT&CK matrix: tactics

and techniques.

Tactics											
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Command and Control	Impact	
- Active Scanning - Gather Victim Host Information - Gather Victim Identity Information - Gather Victim Network Information - Gather Victim Org. Information - Phishing for Information	- Acquire Infrastructure - Compromise Accounts - Establish Public-Facing Application - External Removable Media - Modbus Program Download - Valid Accounts	- Default Accounts - Drive-By Compromise - Exploit Public-Facing Application - Forge Alarm - Execute Through API - Module Firmware - Malicious Program Download - Valid Accounts	- Command and Scripting Interpreter - Forge Alarm - Execute Through API - Module Firmware - Malicious Program Download - Valid Accounts	- Default Password - Hybrid Execution Flow - Implant Custom Image - Manipulating Controller - Modify Program	- Abuse Elevation Control Mechanism - Exploitation for Privilege Escalation - Escape to Host - Hoisting	- Data Destruction - Exploitation for Privilege Escalation - Escape to Host - Hoisting	- Adversary in-the-Middle - Brute Force ID - Brute Force IO - Exploitation for Privilege Escalation - Network Sniffing - Point & Control Systems - Software Configuration	- File and Directory Discovery - Network Service Scanning - Network Sniffing - Point & Control Systems - Software Configuration	- Application Layer Protocol - Commonly Used Port - Custom C2 Protocol - Data Encoding	- Automated Estimation - Transfer Data to Cloud	

Techniques											
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Command and Control	Impact	
- Active Scanning - Gather Victim Host Information - Gather Victim Identity Information - Gather Victim Network Information - Gather Victim Org. Information - Phishing for Information	- Acquire Infrastructure - Compromise Accounts - Establish Public-Facing Application - External Removable Media - Modbus Program Download - Valid Accounts	- Default Accounts - Drive-By Compromise - Exploit Public-Facing Application - Forge Alarm - Execute Through API - Module Firmware - Malicious Program Download - Valid Accounts	- Command and Scripting Interpreter - Forge Alarm - Execute Through API - Module Firmware - Malicious Program Download - Valid Accounts	- Default Password - Hybrid Execution Flow - Implant Custom Image - Manipulating Controller - Modify Program	- Abuse Elevation Control Mechanism - Exploitation for Privilege Escalation - Escape to Host - Hoisting	- Data Destruction - Exploitation for Privilege Escalation - Escape to Host - Hoisting	- Adversary in-the-Middle - Brute Force ID - Brute Force IO - Exploitation for Privilege Escalation - Network Sniffing - Point & Control Systems - Software Configuration	- File and Directory Discovery - Network Service Scanning - Network Sniffing - Point & Control Systems - Software Configuration	- Application Layer Protocol - Commonly Used Port - Custom C2 Protocol - Data Encoding	- Automated Estimation - Transfer Data to Cloud	

Figure 5: MITRE ATT&CK matrix: tactics and techniques [63].

5.2.3 Cyber Kill Chain

The Cyber Kill Chain is a widely recognized cybersecurity framework that outlines the seven stages of a cyberattack, from reconnaissance to actions on objectives [64]. Lockheed Martin first launched it based on a military approach, but it has since been extensively modified [65]. It enables security teams to understand and disrupt attack vectors at various stages, particularly against Advanced Persistent Threats (APTs). By analyzing each phase, defenders can intervene early, reducing the risk of a full-scale compromise [64].

- Reconnaissance:** The attackers aim to gather as much information about the attack targets as possible to determine the attack surface and potential breach points.
- Weaponization:** In this phase, attackers will exploit the vulnerabilities discovered during the reconnaissance phase and create an attack vector.
- Delivery:** Attackers have gained access to the target systems, and they can deliver the payload that will help to carry out the attack.
- Exploitation:** The intended payload has been delivered, and the attackers can execute the malicious code within the target system.
- Installation:** In this phase, the malware or other attack vector will be installed on the target system, and the attackers have gained access to the target system.
- Command and Control:** The attacker can now control the target systems and network and access privileged accounts, search for credentials, and change permissions.
- Actions on Objectives:** Finally, attackers can perform data exfiltration from the system. Their main objective is gathering, encrypting, and

extracting confidential information from the compromised system [65].

This approach provides insights into attackers' tactics, techniques, and procedures (TTPs), improving incident response and enhancing overall system security [64]. However, it does not provide the attacker with a detailed description of the steps taken after the initial compromise and specifically focuses on completing the attacker's goal by launching malware against a target [66]. Although for some goals and attack strategies the "initial compromise" might suffice, many more advanced scenarios and TTPs require deeper penetration into a target's network and systems [66]. Figure 6 illustrates the Cyber Kill Chain Steps.

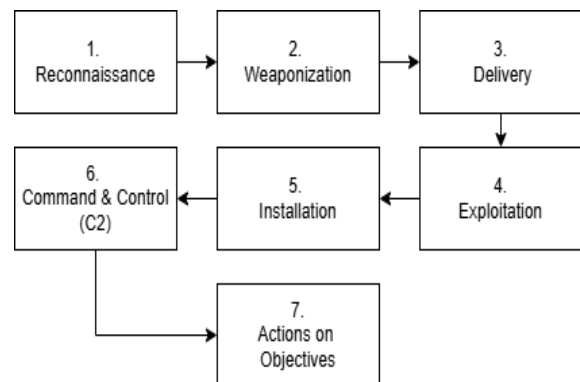


Figure 6: Cyber Kill Chain Steps [64].

5.2.4 STRIDE

The most mature threat modeling method, STRIDE, is an industry-developed threat modeling method [67]. In 1999, Microsoft's Loren Kohnfelder and Praerit Garg introduced the STRIDE methodology through the article "The Threats to Our Products," which includes the systematic management of various threats from the design stage of all Microsoft products [68]. It has been used by Microsoft and other known organizations for decades [67]. Thereafter, Microsoft founder Bill Gates introduced a process of building secure applications, which eventually became the origin of Microsoft's STRIDE and Threat Analysis and Modeling (TAM) (2002) [68]. Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE) [69] focuses on finding the threats without using an impact terminology and ranking approach [67]. STRIDE is a threat enumeration technique that helps to identify potential threats to a system. STRIDE analyzes the system components against 6 main security properties (authenticity, integrity, non-repudiation,

confidentiality, availability, and authorization). This method is complemented by a system modeling approach, called a Data Flow Diagram (DFD) [67].

Formal definitions of STRIDE security properties: For rigorous analysis, each security property can be quantified:

- Confidentiality

Confidentiality = $0.599 - 0.623(CP) + 0.341(TSS) - 1.25(MDH)$ where:

CP = Class Protection, TSS = Total Security Services, MDH = Maximum Depth of Hierarchy [70]

- Availability

Availability = $\frac{MTBF}{MTBF + MTTR}$, [71][72] Where MTBF stands for Mean Time Between Failure, MTTR stands for Mean Time To Repair

- Integrity

Integrity = $\sum_{i=1}^n \omega_i I_i$ Where ω_i = Integrity impact factor, I_i = Weight assigned to each factor [72]

- Authentication

FAR = $\frac{FP}{FP + TN}$, Where FP = False Positives (unauthorized users incorrectly accepted), TN = True Negatives (unauthorized users correctly rejected). This formula calculates the probability that a system incorrectly grants access to an unauthorized user. FRR = $\frac{FN}{FN + TP}$ where FN = False Negatives (authorized users incorrectly rejected), TP = True Positives (authorized users correctly authenticated). The formula calculates the probability that an authorized user is denied access [73].

- Authorization

Authorization = $f(S, O, A, C)$ where S = Subject/User, O = Object/Resource, A = Action/Permission, C = Context/Constraints [74]

A DFD is a graphical representation of a system, and it is composed of four basic elements: processes, data stores, data flows, and external entities. DFD can be used to understand the system's architecture and what information is exchanged between the different components of a system [67]. STRIDE mainly focuses on the security properties of the system (i.e., confidentiality, integrity, availability, authentication, authorization, and non-repudiation). However, there exist some methods that focus on other aspects, such as privacy or safety [75]. STRIDE has been identified by independent agencies like the European Union

Agency for Cybersecurity (ENISA) as a promising starting point for AI threat modeling [76]. Threat modeling methods (e.g., STRIDE) do not have strong threat enumeration constructs beyond their system models. Thus, the success of the threat elicitation usually depends on the experience of the experts involved in the work [75]. Figure 7 illustrates STRIDE model threats and security objective violations.

[71]

Figure 7: STRIDE model threat and security objective violation [69].

5.2.5 NIST

In response to the complex threat landscape, the NIST Cybersecurity Framework (CSF) has emerged as a globally recognized tool for addressing cyber risks. Introduced in 2014 and subsequently updated to version 2.0, this framework provides an adaptable structure that helps organizations identify, protect, detect, respond, and recover from cyber threats [77].

The updated NIST Cybersecurity Framework 2.0 serves as a standardized guideline designed to support organizations across all levels from management to IT staff in implementing comprehensive cybersecurity management approaches [77]. It also guides industry, government agencies, and other organizations to manage cybersecurity risks [78]. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization, regardless of its size, sector, or maturity, to better understand, assess, prioritize, and communicate its cybersecurity efforts. NIST has emphasized that accurate security threat models are critical to designing secure cyber-physical systems [79]. The framework's flexibility allows for integration with other standards, as demonstrated by efforts to create evaluation frameworks that measure information security maturity by combining NIST CSF with COBIT 2019 [77]. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes [78]. However, despite its widespread adoption and proven adaptability, significant questions remain regarding its implementation effectiveness and measurable impact on threat prevention across diverse organizational contexts [77]. Figure 8 illustrates the NIST Cybersecurity framework: Core functions and their cyclical relationship.



Figure 8: NIST Cybersecurity framework: Core functions and their cyclical relationship [77].

5.3 Simulation and Testbeds

To successfully carry out a high-impact industrial control system attack, an attacker must first acquire system access, then exploit a vulnerability. Yet, the likelihood of success of such an attack is reduced if the vulnerability is newly discovered [65]. Any proposed security solution needs a reliable test environment that satisfies its requirements, including repeatability, accuracy, and fidelity [61]. In a broad sense, a test environment includes datasets, testbeds, and attack simulation [62].

1. Physical Testbeds

Several articles have reported the construction of physical ICS testbeds to provide a cyber threats research platform. An ICS physical testbed is a scaled-down version of a control system [80]. Physical testbed [53] consists of real hardware and software for conducting a line of security validation experiments [72]. Physical testbed implementations require substantial time, effort, and costs [53]. Several physically simulated testbeds have been proposed to validate a new security solution [73]. Mathur and Tippenhauer [62] created a small-scale water treatment system (SWaT) testbed for security research. SWaT is a 6-step water treatment process, with each stage regulated autonomously by a local PLC. The footprint of this testbed is approximately 90 square meters, and still, it is a miniature version of an operational water treatment system [53]. Another example of physical ICS testbeds is the National SCADA Testbed (NSTB), which implements a 61-mile 138 kV power grid distribution network to create a testbed. The NSTB was established to assist the security of the nation's energy control systems by providing test scenarios, research facilities, field-scale control systems, and

advanced visualization and modeling tools [53]. Swat and NSTB are comprehensive simulations of operational ICS and can be used for various cybersecurity research. However, due to their geographic location, they are not accessible to most researchers. Moreover, these testbeds are not easily replicable since creating such testbeds is not a feasible solution in most cases due to time and cost constraints [53]. Figure 9 illustrates the architecture of a cyber-physical power system testbed.

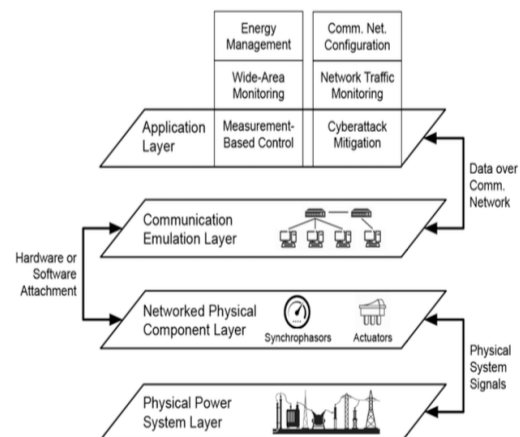


Figure 9: Architecture of a cyber-physical power system testbed [81].

2. Virtual Testbeds

Virtualisation technology is efficient for developing an affordable security testbed with high fidelity and flexibility [82]. Virtual testbeds do not require the use of hardware implementations and could implement all ICS components using software simulations [58]. Queiroz et al. proposed SCADASim, a simulation tool to create SCADA simulations. The strength of this tool is its ability to integrate external devices and applications, which makes the testbeds extremely extensible. However, an interface to use real physical processes is missing, and it should be developed by the users. SCADASim is built on top of OMNET++, a discrete event simulation engine. They extend abstract SScheduler, SGate, and SProxy in OMNET++ to create SCADA components such as Remote Terminal Unit (RTU), PLC, and Master Terminal Unit (MTU). They also implemented two types of cyberattacks: DDoS and MITM with spoofing attacks [58]. A SCADA-specific security testbed was proposed by Yang et al. to evaluate security vulnerabilities in SCADA systems. The testbed consists of the main SCADA components, including HMI, Historian, field devices, and IEC 60870-5-103 communication protocols [82]. A malicious host is implemented to simulate cyberattacks, such as MITM, DoS, and

ARP spoofing. However, it does not support fidelity. GridLAB-D is an open-source power distribution system simulation and analysis tool. This tool employs advanced modelling techniques that provide useful information to designers and operators of distribution systems [83]. Figure 10 illustrates a virtual security testbed for a SCADA system; the cloud symbolizes the virtual environment of the testbed.

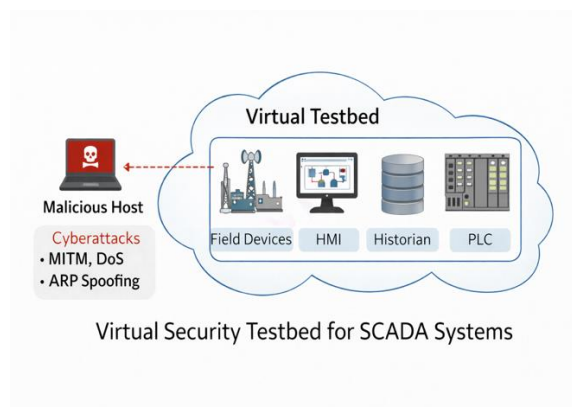


Figure 10: A virtual security testbed for a SCADA system [58].

3. Hybrid Testbeds

Vulnerability assessment on physical testbeds provides the most accurate results; however, the cost of implementing such a system is considerably high. Hybrid testbeds try to address the trade-off between cost and implementation by virtualizing some components, such as sensors and actuators. Other components like PLC and HMI remain physical [81]. The primary focus of a hybrid testbed is to provide a testbed for cybersecurity purposes. In this approach, the SCADA system can simulate, virtualise, and emulate physical devices [83]. In semi-physical testbeds, some essential testbed components, such as networking infrastructure, controlling components, or HIL, are replaced by software simulations [58]. Gao et al. designed and implemented the EPS-ICS testbed according to an ICS layered architecture to facilitate the development of security standards. They used MATLAB/Simulink to simulate mathematical models of HIL and real PLCs to realize a control system [58]. They also emulated networks using Emulab, DETERlab, and PlanetLab. Although the EPS-ICS testbed is a valuable asset for vulnerability digging on PLCs, it lacks fidelity in studying common network attacks against ICS since real network traffic does not exist. Moreover, using real PLCs increases cost and implementation time and forces researchers to dig into the implementation details [58]. Koganti et al. created

a testbed with a simulated HIL, an emulated PLC with Matlab/Simulink, and a real network implementation. The HIL was a power grid distribution substation simulated in a virtual machine (VM). SCADA simulator and attack simulator were two other VMs connected through a Modbus connection on a real network [58]. Considering software simulation of HIL and PLCs, this testbed is highly versatile since the change can only be made in the simulation script. However, this testbed is not comprehensive in scope and requires effective implementation of control system components, such as controlling the HMI. As a result, this testbed is inadequate for simulating a wide spectrum of ICS cyberattacks [58]. Figure 11 illustrates an example of a hybrid testbed.

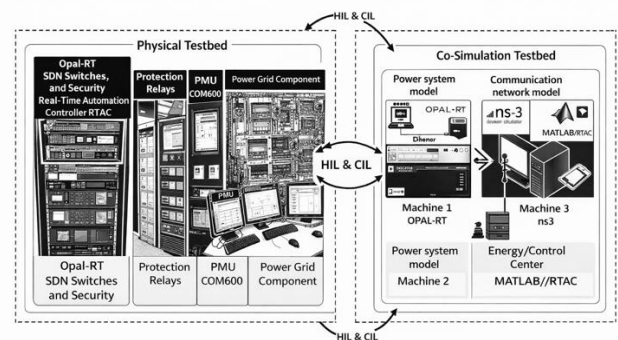


Figure 11: an example of a hybrid Smart Grid Testbed (SGTB) [84].

6 Research Gaps and Future Directions

The increasing integration of Industrial Control Systems (ICS) with the internet has brought out significant vulnerabilities, particularly concerning the Modbus and HTTP protocols, thus increasing the attack surface of these systems. While there has been considerable research on cybersecurity frameworks and defense mechanisms, several gaps remain that warrant further investigation.

1. Research Gaps

Despite a lot of research having been carried out on ICS, there still seem to be various gaps when it comes to those utilising Modbus and HTTP.

- i. While there are various cybersecurity frameworks developed for ICS, they often do not address the unique security requirements of ICS that specifically use the Modbus and HTTP protocols.
- ii. Despite having various defense mechanisms, there is a lack of standardized

evaluation metrics for assessing the effectiveness of defense mechanisms. This means each party uses their own standard of measure, and while results may vary, they also cannot be compared.

- iii. Many researchers have addressed the various threats to ICS utilizing Modbus and HTTP; there is a lack of comprehensive threat modeling for these ICS. More detailed models are required to understand the attack vectors and the potential effect of successful attacks.
- iv. There is limited research on incident response and detection mechanisms for Modbus and HTTP. There is a need for adaptive response strategies that can handle the dynamic nature of cyber threats in ICS.
- v. Machine learning has been underexplored when it comes to Modbus and HTTP ICS. There are various ICS protocols, and while there are many existing solutions, they are not compatible with all protocols.

2. Future Directions

This paper suggests various future directions, including the development of tailored cybersecurity frameworks. Future research focusing on developing cybersecurity frameworks specifically designed for Modbus and HTTP protocols within ICS would greatly bridge this gap. Establishing platforms for sharing information about threats and attacks among organizations would help improve the industry's security posture. Investigating the use of machine learning for real-time anomaly detection tailored to Modbus and HTTP traffic can enhance the ability to detect and mitigate against threats.

Encouraging collaboration between various stakeholder discipline e.g., cybersecurity experts, industrial engineers, and software developers, can facilitate more reliable and well-rounded solutions.

7 Conclusion

In conclusion, the security of Industrial Control Systems, particularly concerning Modbus and HTTP protocols, is a critical area that requires ongoing attention. This paper highlights the diverse threat landscape, existing defense mechanisms, and the importance of cybersecurity frameworks in improving ICS resilience. By identifying research gaps and suggesting future directions, this paper aims to contribute to the ongoing discourse on enhancing the security posture of industrial infrastructures. A proactive, layered defense strategy, coupled with continuous research and adaptation, is essential for safeguarding ICS from evolving cyber threats.

References

- [1] M. U. Ali, M. Akhtar, and H. Durad, "Industrial Control and Building Automation System Penetrating Testing using Modbus TCP Testbed," *VFAST Transactions on Software Engineering*, vol. 10, no. 3, pp. 37–42, Sep. 2022, doi: 10.21015/vtse.v10i3.1113.
- [2] E. Amer, B. A. S. Al-rimy, and S. El-Sappagh, "Strengthening ICS defense: Modbus-NFA behavior model for enhanced anomaly detection," *Journal of Information Security and Applications*, vol. 89, p. 103990, Mar. 2025, doi: 10.1016/J.JISA.2025.103990.
- [3] K. Stouffer et al., "Guide to Operational Technology (OT) security," Sep. 2023. doi: 10.6028/NIST.SP.800-82r3.
- [4] M. Nankya, R. Chataut, and R. Akl, "Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies," *Sensors*, vol. 23, no. 21, p. 8840, Oct. 2023, doi: 10.3390/s23218840.
- [5] F. Katulić, D. Sumina, S. Groš, and I. Erceg, "Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes," *IEEE Access*, vol. 11, pp. 47007–47023, 2023, doi: 10.1109/ACCESS.2023.3275443.
- [6] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems," *Int. J. Distrib. Sens. Netw.*, vol. 14, no. 8, p. 155014771879461, Aug. 2018, doi: 10.1177/1550147718794615.
- [7] Q. Wanying, W. Weimin, Z. Surong, and Z. Yan, "The Study of Security Issues for the Industrial Control Systems Communication Protocols," in *Proceedings of the 2015 Joint International Mechanical, Electronic and Information Technology Conference*, Paris, France: Atlantis Press, 2015. doi: 10.2991/jimet-15.2015.129.
- [8] C. Parian, T. Guldemann, and S. Bhatia, "Fooling the Master: Exploiting Weaknesses in the Modbus Protocol," *Procedia Comput. Sci.*, vol. 171, pp. 2453–2458, 2020, doi: 10.1016/j.procs.2020.04.265.
- [9] A. A. Murthy, P. Mabel John, and R. M. Babu Kasturi Nagappasetty, "Hypertext transfer protocol performance analysis in traditional and software defined networks during Slowloris attack," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 4, p. 4268, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4268-4279.

- [10] D. M. Djekic, "The Industrial Control Systems and The Internet of Things," *Cyber Defense Magazine*, Aug. 27, 2023. Accessed: May 04, 2025. [Online]. Available: <https://www.cyberdefensemagazine.com/the-industrial-control-systems-and-the-internet-of-things/#>
- [11] S. Jaloudi, "Communication protocols of an industrial internet of things environment: A comparative study," *Future Internet*, vol. 11, no. 3, 2019, doi: 10.3390/fi11030066.
- [12] K.-C. Lu, I.-H. Liu, and J.-S. Li, "A Survey of the Offensive and defensive in Industrial Control System." [Online]. Available: www.bncss.org,
- [13] X. Qin, F. Jiang, X. Qin, L. Ge, M. Lu, and R. Doss, "CGAN-based cyber deception framework against reconnaissance attacks in ICS," *Computer Networks*, vol. 251, p. 110655, Sep. 2024, doi: 10.1016/J.COMNET.2024.110655.
- [14] F. J. Folgado, D. Calderón, I. González, and A. J. Calderón, "Review of Industry 4.0 from the Perspective of Automation and Supervision Systems: Definitions, Architectures and Recent Trends," Feb. 01, 2024, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics13040782.
- [15] A. Dima, "The Four Industrial Revolutions: Transforming Manufacturing Across Centuries," K. Factory, Accessed: May 04, 2025. [Online]. Available: <https://kfactory.eu/the-industrial-revolution-short-history-of-manufacturing/>
- [16] C. Urrea, C. Morales, and J. Kern, "Implementation of error detection and correction in the Modbus-RTU serial protocol," *International Journal of Critical Infrastructure Protection*, vol. 15, pp. 27–37, Dec. 2016, doi: 10.1016/J.IJCIP.2016.07.001.
- [17] I. Zagan and V. G. Găitan, "Enhancing the Modbus Communication Protocol to Minimize Acquisition Times Based on an STM32-Embedded Device," *Mathematics*, vol. 10, no. 24, p. 4686, Dec. 2022, doi: 10.3390/math10244686.
- [18] N. C. Găitan, I. Zagan, and V. G. Găitan, "Proposed Modbus Extension Protocol and Real-Time Communication Timing Requirements for Distributed Embedded Systems," *Technologies (Basel)*, vol. 12, no. 10, p. 187, Oct. 2024, doi: 10.3390/technologies12100187.
- [19] D. N. Patel and S. B. Somani, "A Review on Implementation of MODBUS Communication Protocol and its Applications," *International Journal of Electronics Engineering Research*, vol. 9, no. 4, 2017.
- [20] G. Yadav and K. Paul, "Architecture and Security of SCADA Systems: A Review," Jan. 2020.
- [21] Q.-T. Dao, L.-T. Nguyen, T.-K. Ha, V.-H. Nguyen, and T.-A. Nguyen, "Investigation of Secure Communication of Modbus TCP/IP Protocol: Siemens S7 PLC Series Case Study," *Applied System Innovation*, vol. 8, no. 3, p. 65, May 2025, doi: 10.3390/asi8030065.
- [22] A. A. Murthy, P. Mabel John, and R. M. Babu Kasturi Nagappasetty, "Hypertext transfer protocol performance analysis in traditional and software defined networks during Slowloris attack," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 4, p. 4268, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4268-4279.
- [23] CosmasEkoSuharyanto and PastimaSimanjuntak, "Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case) CosmasEkoSuharyanto, PastimaSimanjuntak," 2017, [Online]. Available: <http://www.ijser.org>
- [24] X. Etxezarreta, I. Garitano, M. Iturbe, and U. Zurutuza, "Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey," *International Journal of Critical Infrastructure Protection*, vol. 42, Sep. 2023, doi: 10.1016/j.ijcip.2023.100615.
- [25] A. S. George, "Partners Universal International Innovation Journal (PUIIJ) The Impact of IT/OT Convergence on Digital Transformation in Manufacturing," 2024, doi: 10.5281/zenodo.10895704.
- [26] R. Venanzi, G. Di Modica, L. Foschini, and P. Bellavista, "Towards IT/OT integration in industry digitalization: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 245, p. 104373, Jan. 2026, doi: 10.1016/J.JNCA.2025.104373.
- [27] C. - Clara Morlière, "IT/OT convergence: A fruitful integration of information systems and operational systems."
- [28] T. Martins and S. V. G. Oliveira, "Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions

- Supported,” *Sensors*, vol. 22, no. 20, p. 8024, Oct. 2022, doi: 10.3390/s22208024.
- [29] R. Kumar, R. Kela, S. Singh, and R. Trujillo-Rasua, “APT attacks on industrial control systems: A tale of three incidents,” *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100521, Jul. 2022, doi: 10.1016/j.ijcip.2022.100521.
- [30] R. Buchta, G. Gkoktsis, F. Heine, and C. Kleiner, “Advanced Persistent Threat Attack Detection Systems: A Review of Approaches, Challenges, and Trends,” *Digital Threats: Research and Practice*, vol. 5, no. 4, pp. 1–37, Dec. 2024, doi: 10.1145/3696014.
- [31] V. Pedreira, D. Barros, and P. Pinto, “A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead,” *Sensors*, vol. 21, no. 15, p. 5189, Jul. 2021, doi: 10.3390/s21155189.
- [32] T. J. Olorunlana and H. Mohammed, “Analysis of the Colonial Pipeline Cybersecurity Incident,” *International Journal of Science, Architecture, Technology and Environment*, pp. 9–13, Apr. 2025, doi: 10.63680/jngh0767as.
- [33] W. Alsabbagh, S. Amogbonjaye, D. Urrego, and P. Langendörfer, “A Stealthy False Command Injection Attack on Modbus based SCADA Systems.” [Online]. Available: <http://www.scadabr.com.br/>
- [34] V. Kampurakis, G. Kambourakis, E. Chatzoglou, and C. Zaroliagis, “Revisiting man-in-the-middle attacks against HTTPS,” *Network Security*, vol. 2022, no. 3, Mar. 2022, doi: 10.12968/S1353-4858(22)70028-1.
- [35] C. Singh and A. K. Jain, “A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network,” *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 8, no. 3, p. 100543, Jun. 2024, doi: 10.1016/j.prime.2024.100543.
- [36] I. Odun-Ayo et al., “Evaluating Common Reconnaissance Tools and Techniques for Information Gathering,” *Journal of Computer Science*, vol. 18, no. 2, pp. 103–115, Feb. 2022, doi: 10.3844/jcssp.2022.103.115.
- [37] M. M. Alani and E. Damiani, “XRcon: An Explainable IoT Reconnaissance Attack Detection System Based on Ensemble Learning,” *Sensors*, vol. 23, no. 11, p. 5298, Jun. 2023, doi: 10.3390/s23115298.
- [38] V. Vajrobol et al., “Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms,” *Journal of High Speed Networks*, vol. 31, no. 1, pp. 61–70, Feb. 2025, doi: 10.1177/09266801241295886.
- [39] B. Khaund, “The Evolution of Denial-of-Service Attacks: From DoS to DDoS – Mechanisms, Impacts, and Defensive Strategies,” *European Journal of Computer Science and Information Technology*, vol. 13, no. 47, pp. 134–146, Jun. 2025, doi: 10.37745/ejcsit.2013/vol13n47134146.
- [40] P. Radoglou-Grammatikis, I. Siniosoglou, T. Liatifis, A. Kourouniadis, K. Rompolos, and P. Sarigiannidis, “Implementation and Detection of Modbus Cyberattacks,” in *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCASST)*, IEEE, Sep. 2020, pp. 1–4. doi: 10.1109/MOCASST49295.2020.9200287.
- [41] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, “Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications,” *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.
- [42] F. Trungadi et al., “Securing Modbus in legacy industrial control systems: A decentralized approach using proxies, Post-Quantum Cryptography and Self-Sovereign Identity,” *Journal of Information Security and Applications*, vol. 94, p. 104199, Nov. 2025, doi: 10.1016/J.JISA.2025.104199.
- [43] D. Upadhyay, S. Ghosh, H. Ohno, M. Zaman, and S. Sampalli, “Securing industrial control systems: Developing a SCADA/IoT test bench and evaluating lightweight cipher performance on hardware simulator,” *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100705, Dec. 2024, doi: 10.1016/J.IJCIP.2024.100705.
- [44] V. Varadharajan, U. Tupakula, and K. K. Karmakar, “Techniques for Enhancing Security in Industrial Control Systems,” *ACM Transactions on Cyber-Physical Systems*, vol. 8, no. 1, pp. 1–36, Jan. 2024, doi: 10.1145/3630103.
- [45] A. Fielder, T. Li, and C. Hankin, “Defense-in-depth vs. Critical Component Defense for Industrial Control Systems,” Oct. 2016. doi: 10.14236/ewic/ICS2016.1.
- [46] Y. Li, S. Wu, and Q. Pan, “Network Security in the Industrial Control System: A Survey,” Aug. 2023, [Online]. Available: <http://arxiv.org/abs/2308.03478>

- [47] E. Wai and C. K. M. Lee, "Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0," in *Science and Technology: Recent Updates and Future Prospects Vol. 2*, B P International, 2024, pp. 124–144. doi: 10.9734/bpi/strufp/v2/12542F.
- [48] Z. Yang et al., "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," *Comput. Secur.*, vol. 116, p. 102675, May 2022, doi: 10.1016/J.COSE.2022.102675.
- [49] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," *Computers*, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.
- [50] S. Dilshan Ranwadana, "Anomaly Detection in Intrusion Detection and Prevention Systems."
- [51] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," *Comput. Secur.*, vol. 114, p. 102598, Mar. 2022, doi: 10.1016/J.COSE.2021.102598.
- [52] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, "A Zero Trust approach for the cybersecurity of Industrial Control Systems," in *2022 IEEE 21st International Symposium on Network Computing and Applications (NCA)*, IEEE, Dec. 2022, pp. 1–7. doi: 10.1109/NCA57778.2022.10013559.
- [53] W. Yeoh, M. Liu, M. Shore, and F. Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework," *Comput. Secur.*, vol. 133, p. 103412, Oct. 2023, doi: 10.1016/J.COSE.2023.103412.
- [54] A. Pigola and F. de S. Meirelles, "Zero trust in cybersecurity: managing critical challenges for effective implementation," *Journal of Systems and Information Technology*, Apr. 2025, doi: 10.1108/JSIT-08-2024-0326.
- [55] A. Elmarkez, S. Mesli-Kesraoui, P. Berruet, and F. Oquendo, "Security by Design for Industrial Control Systems from a Cyber–Physical System Perspective: A Systematic Mapping Study," *Machines*, vol. 13, no. 7, p. 538, Jun. 2025, doi: 10.3390/machines13070538.
- [56] X. Niu, M. M. Cook, and D. Pezaros, "Examining the Suitability of Stream Ciphers for Modbus-TCP Encryption on Resource Constrained Devices," in *Proceedings of the 17th European Workshop on Systems Security*, New York, NY, USA: ACM, Apr. 2024, pp. 51–57. doi: 10.1145/3642974.3652287.
- [57] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach," *Sensors (Basel)*, vol. 19, no. 20, Oct. 2019, doi: 10.3390/s19204455.
- [58] A. Dehlaghi-Ghadim, A. Balador, M. H. Moghadam, H. Hansson, and M. Conti, "ICSSIM — A framework for building industrial control systems security testbeds," *Comput. Ind.*, vol. 148, p. 103906, Jun. 2023, doi: 10.1016/J.COMPIND.2023.103906.
- [59] Y. Jiang et al., "MITRE ATT&CK Applications in Cybersecurity and The Way Forward," Feb. 2025, [Online]. Available: <http://arxiv.org/abs/2502.10825>
- [60] B. Al-Sada, A. Sadighian, and G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database," *IEEE Access*, vol. 12, pp. 1217–1234, 2024, doi: 10.1109/ACCESS.2023.3344680.
- [61] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors (Basel)*, vol. 21, no. 9, May 2021, doi: 10.3390/s21093267.
- [62] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the Art and Way Forward," *ACM Comput. Surv.*, vol. 57, no. 1, pp. 1–37, Jan. 2025, doi: 10.1145/3687300.
- [63] A.-S. Bader, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the Art and Way Forward." doi: XXXXXXXX.XXXXXXX.
- [64] A. F. Syifa and M. Salman, "Cyber Kill Chain Framework Approach to Map Potential Attack Vectors on Windows-based OS," *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 3, no. 1, May 2025, doi: 10.62146/ijecbe.v3i1.107.
- [65] X. Qin, F. Jiang, M. Cen, and R. Doss, "Hybrid cyber defense strategies using Honey-X: A survey," *Computer Networks*, vol. 230, p. 109776, Jul. 2023, doi: 10.1016/J.COMNET.2023.109776.
- [66] M. Sprengers and J. van Haaster, "Organization of #operations," *Cyber Guerilla*, pp. 41–109, 2016, doi: 10.1016/B978-0-12-805197-9.00003-6.
- [67] S. M. Khalil, H. Bahsi, and T. Korötko, "Threat modeling of industrial control systems: A systematic literature review," *Comput.*

- Secur., vol. 136, p. 103543, Jan. 2024, doi: 10.1016/J.COSE.2023.103543.
- [68] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, Dec. 2022, doi: 10.4218/etrij.2021-0181.
- [69] Z. Nadifi, M. Ouaisa, M. Ouaisa, M. Alhyan, and A. Kartit, "STRIDE-Based Threat Modeling and Risk Assessment Framework for IoT-enabled Smart Healthcare Systems," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 21, no. 09, pp. 63–80, Jul. 2025, doi: 10.3991/ijoe.v21i09.55517.
- [70] S. A. Khan and R. A. Khan, "Confidentiality Quantification Model at Design Phase," *International Journal of Information and Education Technology*, pp. 535–537, 2012, doi: 10.7763/ijiet.2012.v2.199.
- [71] J. De and L. Cruz, "Security Chaos Engineering and the Application of Threat Modeling."
- [72] M. Pendleton and J.-H. Cho, "A Survey on Systems Security Metrics 1."
- [73] A. Z. Zaidi, C. Y. Chong, Z. Jin, R. Parthiban, and A. S. Sadiq, "Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 191, p. 103162, Oct. 2021, doi: 10.1016/J.JNCA.2021.103162.
- [74] L. Song, X. Ju, Z. Zhu, and M. Li, "An access control model for the Internet of Things based on zero-knowledge token and blockchain," *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13638-021-01986-4.
- [75] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korötko, K. McLaughlin, and V. Kotkas, "Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System," *Comput. Secur.*, vol. 124, p. 102950, Jan. 2023, doi: 10.1016/J.COSE.2022.102950.
- [76] L. Mauri and E. Damiani, "Modeling Threats to AI-ML Systems Using STRIDE," *Sensors*, vol. 22, no. 17, p. 6662, Sep. 2022, doi: 10.3390/s22176662.
- [77] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 6, 2025, doi: 10.14569/IJACSA.2025.0160672.
- [78] "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [79] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39–50, Dec. 2015, doi: 10.1016/J.IJCIP.2015.08.003.
- [80] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, and J. Porcel-Bustamante, "Implementation and Evaluation of Physical, Hybrid, and Virtual Testbeds for Cybersecurity Analysis of Industrial Control Systems," *Symmetry (Basel)*, vol. 13, no. 3, p. 519, Mar. 2021, doi: 10.3390/sym13030519.
- [81] H. Cui, F. Li, and K. Tomsovic, "Cyber-physical system testbed for power system monitoring and wide-area control verification," *IET Energy Systems Integration*, vol. 2, no. 1, pp. 32–39, Mar. 2020, doi: 10.1049/iet-esi.2019.0084.
- [82] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues," Feb. 01, 2023, Elsevier Ltd. doi: 10.1016/j.cose.2022.103028.
- [83] M. S. Abdelrahman, I. Kharchouf, T. L. Nguyen, and O. A. Mohammed, "A Hybrid Physical Co-Simulation Smart Grid Testbed for Testing and Impact Analysis of Cyber-Attacks on Power Systems: Framework and Attack Scenarios," *Energies (Basel)*, vol. 16, no. 23, p. 7771, Nov. 2023, doi: 10.3390/en16237771.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US