IUC UNIVERSITY PRESS İSTANBUL

ORIGINAL ARTICLE
Electrica 2026; 26: 1-13

From Traditional to IoT Based: A Generational Taxonomy and Attack Classification of Supervisory Control and Data Acquisition Systems

Mehmet Yavuz Yağcı, Şafak Durukan-Odabaşı, Muhammed Ali Aydın

Department of Computer Engineering, İstanbul University-Cerrahpaşa Faculty of Engineering, İstanbul, Türkiye

Cite this article as: M. Y. Yağcı, Ş. Durukan-Odabaşı and M. A. Aydın, "From traditional to IoT based: A generational taxonomy and attack classification of supervisory control and data acquisition systems," *Electrica*, 2026, 26, 0173, doi: 10.5152/electrica.2026.25173.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *SCADA systems are critical cyber-physical infrastructures widely used in energy, manufacturing, water, and waste management, where security breaches can cause severe physical, economic, and environmental damage.*
- *The evolution of SCADA systems from isolated, proprietary architectures to IP-based, IoT and cloud-integrated environments has significantly expanded their attack surface.*
- *Existing literature identifies numerous SCADA vulnerabilities and attack taxonomies; however, most studies analyze SCADA systems as a homogeneous class without sufficiently accounting for generational differences and architectural evolution.*

Corresponding author:
Şafak Durukan Odabaşı

E-mail:
safak.odabasi@iuc.edu.tr

Received: June 5, 2025
Revision Requested: July 28, 2025
Last Revision Received: August 25, 2025
Accepted: September 15, 2025
Publication Date: January 30, 2026

DOI: 10.5152/electrica.2026.25173

ABSTRACT

Supervisory control and data acquisition (SCADA) systems play a crucial role in managing vital infrastructures, including power generation, distribution networks, waste management, and smart manufacturing. Initially designed as isolated and closed systems, SCADA architectures have evolved by integrating advanced information technologies, enabling enhanced remote management and interoperability. However, this integration significantly broadens the attack surface, increasing vulnerabilities to sophisticated cyber threats that can lead to severe environmental, human, and economic consequences, thus posing a substantial risk to national security. This study systematically categorizes SCADA systems into distinct generations based on core features, including communication protocols, auditing, and integration levels, and emphasizes the necessity of generation-specific vulnerability analyses. By grouping SCADA systems into two main generational categories, the research provides a structured framework for understanding differing security risks and guiding the development of tailored cybersecurity solutions, such as intrusion detection and prevention systems. This generational approach offers critical insights for both academic inquiry and practical defense strategies, facilitating more effective risk mitigation and resilience building in SCADA systems amid an increasingly complex cyber threat landscape.

***Index Terms*—**Critical infrastructure, cyber-physical systems, industrial internet of things (IIoT), supervisory control and data acquisition (SCADA) systems security, SCADA attacks, vulnerability assessment.

I. INTRODUCTION

Industrial control systems (ICS) are designed to monitor and manage industrial operations over long periods. Among them, supervisory control and data acquisition (SCADA) systems have undergone significant evolution since the 1990s [1]. These cyber-physical systems are widely used in various areas, including manufacturing, energy distribution, waste management, and critical facilities such as nuclear and chemical plants [2].

Initially built as standalone systems using proprietary protocols, SCADA systems have adapted to modern technologies, enabling both vertical (integration with other systems) and horizontal (interoperability among heterogeneous field devices) integration. Their diverse applications and harsh operational environments create unique structural and security requirements, leading to distinct attack vectors.

Supervisory control and data acquisition systems differ fundamentally from information technologies (IT) in terms of operational needs, timing constraints, and risk profiles. While IT disruptions are often tolerable, interruptions in SCADA processes can have serious real-world consequences. National Institute of Standards and Technology (NIST) highlights that SCADA systems prioritize safety and availability over confidentiality [3]. Additionally, their incompatibility with regular software updates complicates vulnerability management, as conventional IT practices such as periodic scanning are ineffective in these specialized environments.

Recent years have seen an increase in cybersecurity threats to SCADA systems, with attackers targeting critical infrastructure. Public vulnerability databases, such as National Vulnerability

WHAT THIS STUDY ADDS ON THIS TOPIC?

- *This study introduces a generation-aware classification framework that systematically categorizes SCADA systems into traditional and IoT-based architectures, highlighting how security risks evolve across four distinct generations.*
- *It provides a comprehensive mapping of SCADA vulnerabilities and attack vectors by jointly leveraging the MITRE ATT&CK for ICS framework and the Purdue Model, enabling clearer alignment between attacker techniques and industrial control layers.*
- *The proposed approach demonstrates that generation-specific vulnerability assessment is essential for accurate risk analysis and for designing effective, tailored cybersecurity strategies in modern SCADA environments, particularly those integrated with IIoT and cloud technologies.*

Database (NVD) [4], Common Vulnerabilities and Exposures (CVE) [5], and Common Weakness Enumeration (CWE) [6], have reported numerous SCADA-related vulnerabilities over the past few decades, highlighting the growing exposure of these systems to cyber threats.

This study analyzes SCADA system vulnerabilities across four generations [7], classified by characteristics such as communication, auditing, integration, and accessibility. It proposes a category-based framework to help vendors, operators, and researchers better understand and secure SCADA environments.

The key contributions include: (i) highlighting generational security differences, (ii) introducing a vulnerability categorization approach, and (iii) linking SCADA characteristics to security challenges. The paper is structured as follows: Section 2 reviews related work, Section 3 introduces SCADA architecture, Section 4 discusses SCADA generations, Section 5 presents SCADA system properties, including operational requirements, device limitations, and communication evolution, and introduces the distinction between traditional and Internet of Things (IoT)–based systems. Section 6 categorizes vulnerabilities, Section 7 proposes a taxonomy for categorizing attacks, and the final sections present conclusions and future directions.

II. RELATED WORK

The security of SCADA systems is crucial because these systems are essential for monitoring and controlling vital infrastructure and industrial processes, such as power plants, water treatment facilities, and manufacturing plants. Protecting SCADA systems is necessary to prevent unauthorized access, data breaches, and potential sabotage, all of which could lead to severe consequences. These may include disruptions to essential services, environmental damage, and threats to public safety. Strong SCADA system security not only ensures the integrity and availability of critical systems but also helps defend against cyberattacks that could exploit vulnerabilities and compromise the stability of essential infrastructure.

Supervisory control and data acquisition systems are vulnerable to several risks that threaten critical infrastructure and industrial processes. One major vulnerability stems from their increasing interconnectivity with the broader internet and corporate networks, which makes them potential targets for cyberattacks. Weak authentication and authorization mechanisms, inadequate encryption practices, and outdated software components can all provide entry points for malicious actors. Additionally, the use of legacy hardware and software, which may no longer receive security updates, leaves SCADA systems exposed to known vulnerabilities. Furthermore, social engineering tactics, such as phishing, can exploit human weaknesses within organizations to gain unauthorized access. Overall, it is essential to address these vulnerabilities to improve the resilience and security of SCADA systems against evolving cyber threats.

Numerous investigations have been conducted regarding SCADA security threats; however, most of these studies have not provided a thorough examination of the vulnerabilities and potential risks involved.

A survey conducted by Sajid et al. [7] focused on the security challenges of IoT-SCADA systems within a cloud environment. However, this survey did not provide a comprehensive analysis of all security vulnerabilities associated with SCADA system functionalities.

Corallo et al. [8] introduced a structural categorization of critical industrial assets within the context of Industry 4.0 and examined the effects of cyberattacks on business operations. Their primary goal was to assess the impact of cybersecurity on the confidentiality, availability, and integrity of data associated with industrial processes conducted through networked manufacturing machines. However, this study did not specifically address the vulnerabilities and attacks related to SCADA systems.

Bartman and Carson [9] discussed the importance of securing communication in SCADA and ICS, highlighting the vulnerabilities these systems face due to legacy protocols and increased connectivity. They proposed practical solutions and best practices, such as encryption, authentication, and network segmentation, to enhance the cybersecurity posture of critical infrastructure systems.

The authors Ghosh and Sampalli [10] built upon the groundwork laid by Sajid et al. [7], with their survey concentrating on contemporary threats to SCADA communication. They also provided a comparative assessment of SCADA security protocols and standards.

Xu et al. [11] offered a taxonomy of cyberattacks on SCADA systems, yet their survey was limited to attacks targeting SCADA communication protocols. Zhu et al. [12] proposed a taxonomy for SCADA that categorized attacks at the network, hardware, and software levels. Software attacks were classified based on the exploitation of embedded operating systems without privileges, while the categories of attacks within the communication stack were similar to those identified by works in [10] and [11].

In [13], the authors introduced a taxonomy that mapped cross-domain attacks on SCADA systems. This taxonomy notably distinguished between an influenced element (e.g., an object manipulated during an attack) and the victim element (e.g., an interaction within a cyber-physical system), which could exist independently in either the physical or cyber domain. However, [14] noted that the proposed taxonomy lacked attack-specific information, and a refined taxonomy has been proposed.

Irmak and Erkek [15] surveyed various attack vectors targeting SCADA systems. While their study shared some similarities with the work of Zhu et al. [12], it did not provide as comprehensive an analysis of SCADA vulnerabilities and attacks as the latter study.

Upadhyay et al. [16] focused on security vulnerabilities and offered recommendations concerning configurations, communication networks, and protocols in SCADA products. They noted that the security approach for SCADA systems should differ from that of typical IT systems. This difference encompasses not only network security but also performance characteristics, reliability requirements, software and hardware architectures, and risk management scenarios. When comparing security metrics, they emphasized that, while data privacy is paramount in IT systems, availability becomes the primary concern for SCADA systems. They identified high network traffic and malware attacks as the most significant sources of vulnerability in SCADA systems.

Asghar et al. [17] drew attention to SCADA systems in industrial facilities and critical infrastructure and their communication over the internet. It has been stated that increasing communication capabilities make SCADA systems more vulnerable than ever. In their work, they grouped the vulnerabilities in SCADA systems into security solutions.

Systems that lack security evaluations and adherence to current standards are vulnerable to cyber threats [3]. The unique nature of ICS requires tailored approaches for maintenance, updates, and security measures [18]. Research shows that well-defined high-level rules enhance security in systems with low-level control mechanisms. The attribute-based access control model facilitates fine-grained authorization, centralized management of access policies, and comprehensive logging [19]. Monitoring data, maintaining records, and assessing traffic security are vital for detecting and preventing attacks [20]. While host-based and network-based methods exist, they often struggle to identify new attack types, especially in ICS, which have unique attack vectors [21]. To address these challenges, multi-layered security strategies are recommended. Risk analyses consider factors such as proximity, accessibility, safety, impact, and value to identify and mitigate risks effectively [22].

The industrial internet of things (IIoT) involves machines, sensors, and actuators communicating to enhance efficiency and monitor costs. While connectivity improves performance, it also exposes systems to vulnerabilities, particularly in SCADA systems used in critical infrastructure. Originally designed for closed networks, SCADA systems did not account for cybersecurity risks, making them susceptible to internal attacks. A. C. Panchal et al. [23] examined vulnerabilities across six layers: the first layer consists of embedded devices and sensors; the second layer includes programmable logic controller (PLC) devices and gateways; the third encompasses human-machine interface (HMI) components. A separating layer distinguishes operational devices from IT systems. The fourth and fifth layers involve classical computing systems and cloud infrastructures. Their study analyzed attack vectors, targets, and effects across these layers.

Hazardous activities and accidents can occur in critical areas like smart grids and chemical facilities where SCADA systems operate, leading to significant environmental and economic damage. While ensuring continuity is essential, the need for preparedness against cyberattacks and systemic errors has gained attention. Research on security mechanisms for critical infrastructures has increased, as illustrated by A. Abou El Kalam et al. [24], who identified SCADA system requirements and proposed a protective approach tailored to their unique characteristics, emphasizing the need for global compliance. Security mechanisms must effectively block attacks and aid in system restoration.

Supervisory control and data acquisition systems, enhanced by computer networks, offer low computing power and complex real-time operations, making traditional IT solutions ineffective. In [2], SCADA vulnerabilities across various system layers, highlighting risks from outdated components and outdated protocols, are analyzed. They recommended simulation and testing to establish defense mechanisms, using attack behaviors modeled mathematically.

Literature reviews categorize SCADA vulnerabilities based on attack stages, system layers, and interaction points. As ICS evolve, vulnerability assessments should consider the generation of SCADA systems, both in live environments and risk analyses, particularly as IoT integration introduces new security risks. For this reason, SCADA systems examined in four generations in [2, 7] are divided into two main topics: traditional and IoT-based, in this study in order to perceive new security risks and attack surfaces more easily. Supervisory control and data acquisition systems, which are examined according to two main headings, have been matched for four different generations and examined in detail according to their features, and new security risks that will be caused by newly added features in IoT-based SCADA systems are emphasized.

III. SUPERVISORY CONTROL AND DATA ACQUISITION ARCHITECTURE

The general architecture of SCADA systems, regardless of their application in different operational areas, can be examined in four layers [2]. The lowest layer consists of sensors and drivers that enable the system to physically interact with the environment. These components are essential for monitoring and activating physical events in the field.Sensors are circuit elements that convert physical changes into analog or digital data, allowing the system to interpret various physical parameters such as temperature, pressure, and speed. Different types of sensors are employed depending on the specific physical changes that need to be detected. The data collected from these sensors, which have varying features, is stored in different data structures.Drivers, on the other hand, are circuit elements that trigger physical events based on decisions made from the evaluated

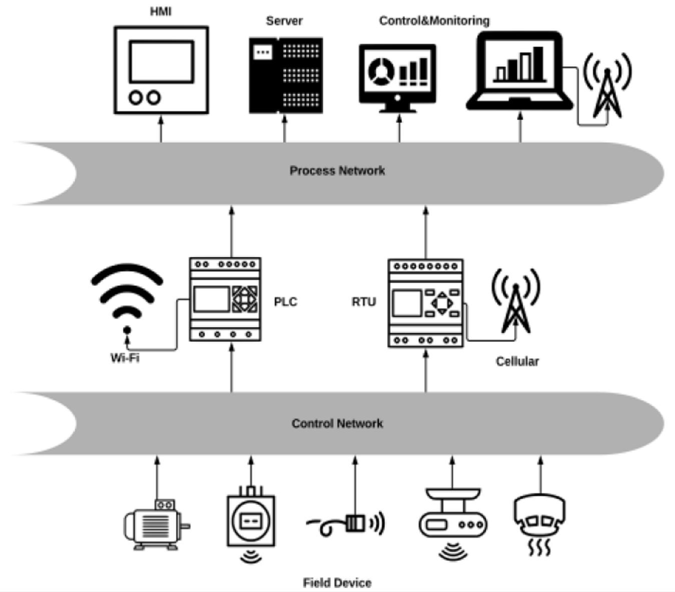


Fig. 1. Supervisory control and data acquisition architecture.

data. They control the power supplied to electrical components like motors, valves, and switches. Since the circuit elements in this layer lack processing power, they operate using control signals received from the upper layer.The medium through which sensors and drivers transmit information to the upper layer, using analog or digital signals, is referred to as the control network. Control information generated in the upper layer, along with data collected from the field, is communicated through this network. A general representation of the SCADA architecture can be seen in Fig. 1.

The lowest layer consists of circuit elements, while the top layer includes computer systems that generally do not communicate directly with each other. An intermediary second layer, comprising components like remote terminal units (RTUs) and PLCs, facilitates communication between incompatible devices through various protocols and control signals. This enables seamless interactions despite differences in device types and communication protocols across layers.Remote terminal units collect digital and analog data from the field and relay it to a central monitoring unit, utilizing a circuit board with various components. In small-scale systems, Beginner's All-purpose Symbolic Instruction Code (BASIC) can be employed, while larger systems may use wireless infrastructures for data collection. Programmable logic controllers, designed for industrial environments, control systems under harsh conditions and are typically programmed using C or ladder logic.The process network layer transmits data from the second layer to the control center, utilizing different communication media based on environmental conditions. Supervisory control and data acquisition systems enable both local and wide-area network connections. Wired connections are favored in closed systems, while Virtual Private Networks (VPNs) and wireless solutions like Wi-Fi and cellular networks cater to broader operations. Variability in protocols across field devices complicates the integration of SCADA systems from different manufacturers.The top layer houses information systems for monitoring, controlling, and reporting field operations. Human-machine interfaces allow operators to interact with field equipment through graphical interfaces. These interfaces can exist as software running on general-purpose operating systems (GPOS) or as dedicated hardware, with each having its vulnerabilities. Human-machine interfaces display real-time data, enabling effective monitoring and control of field operations.

IV. SUPERVISORY CONTROL AND DATA ACQUISITION GENERATIONS

Advancements in IT have led to the development of various communication technologies over the years. The devices that are used daily have enhanced their capabilities by adopting new communication standards and technologies. Once these new standards and technologies demonstrated usability and stability in common devices, they were implemented in industrial applications. These innovations have effectively addressed issues such as access distance and noise within the systems. Supervisory control and data acquisition systems, which integrate changes in communication technologies as part of their infrastructure, are analyzed in four stages [7].

A. First-Generation Supervisory Control and Data Acquisition Systems

Early ICS were designed with communication infrastructures independent of corporate IT networks. Known as first-generation systems, they featured a centralized architecture with a master terminal unit controlling RTUs in the field. Communication relied on point-to-point serial lines, which were considered secure due to their physical isolation.

Protocols such as Modbus [25–27], Profinet [28, 29], and DNP3 [30, 31] were used to transmit compact messages containing only essential elements (transaction code, address, and data). These minimal structures ensured fast response times, which suited the limited bandwidth and latency requirements of the era.

While this architecture was once seen as robust and sufficient, it later revealed challenges in scalability, reliability, and security, particularly as systems evolved toward interconnected and Internet Protocol-based environments. A typical example of such a first-generation SCADA system using serial protocols is shown in Fig. 2.

B. Second-Generation Supervisory Control and Data Acquisition Systems

As the operational area expanded, centralized control in SCADA systems proved inadequate. This limitation led to the emergence of second-generation SCADA systems, which introduced multiple monitoring and control units. While still using serial-based communication with field devices, these systems incorporated communication servers that aggregated data and relayed it to multiple workstations over a local area network (LAN).

The use of LAN enabled several operators to access and control field devices simultaneously through different communication servers, enhancing both scalability and responsiveness. Second-generation systems also began to share networks with IT devices, marking the transition toward distributed control systems by supporting multi-operator environments [32]. A conceptual architecture of a second-generation SCADA system is presented in Fig. 3.

C. Third-Generation Supervisory Control and Data Acquisition Systems

The adoption of modern communication technologies in SCADA systems has significantly reduced communication issues while

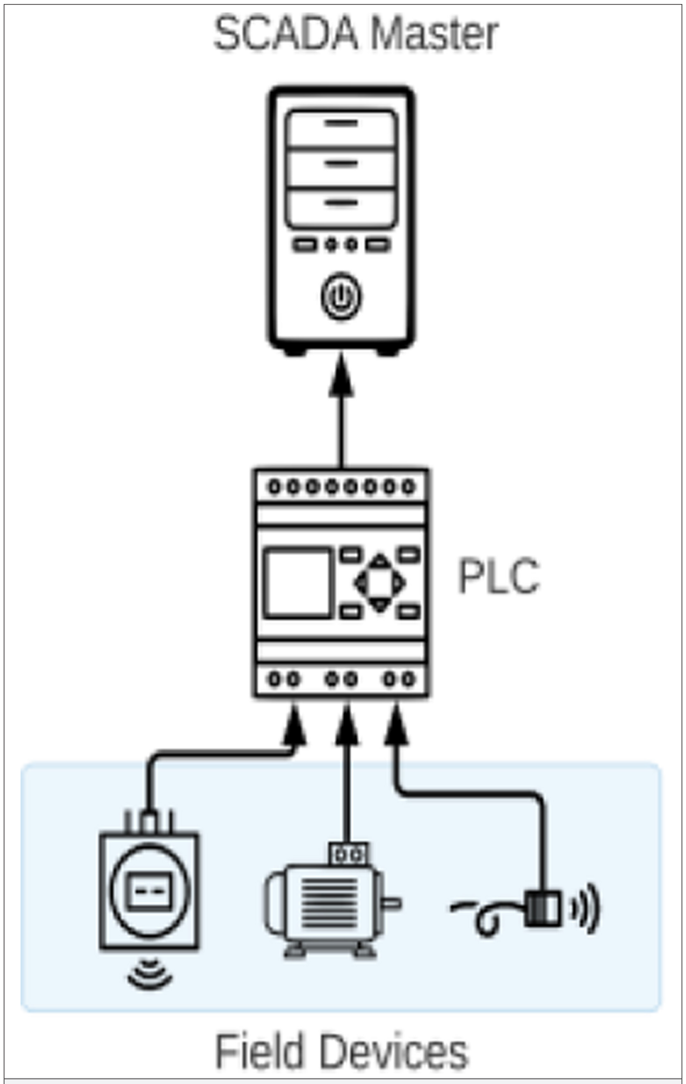


Fig. 2. First-generation supervisory control and data acquisition.

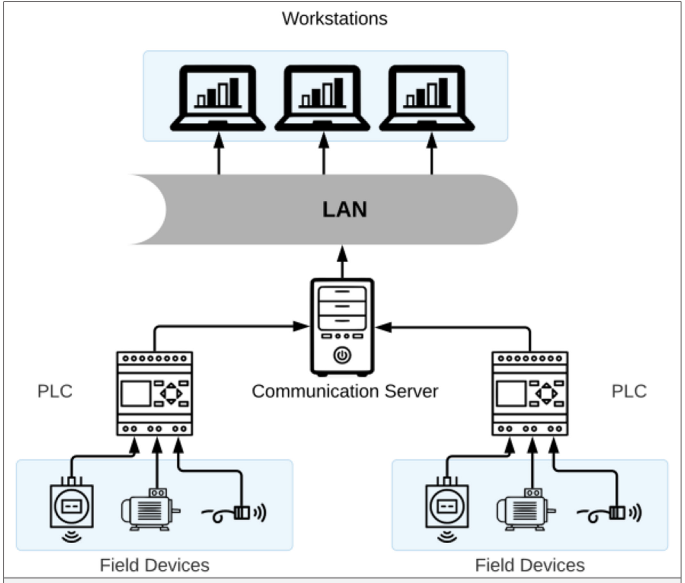


Fig. 3. Second-generation supervisory control and data acquisition.

increasing system functionality. To ensure stable operation in challenging field conditions, such as connectivity, coverage, and environmental constraints, third-generation SCADA systems introduced fundamental changes in their communication architecture.

Unlike earlier generations that relied on isolated serial lines, the third generation utilizes IT-based communication networks, allowing integration with computer networks via Transmission Control Protocol / Internet Protocol (TCP/IP). Importantly, legacy serial communication protocols (e.g., Modbus, DNP3) are still supported over these new infrastructures to ensure backward compatibility, enabling seamless coexistence of old and new components.

This integration has enabled SCADA systems to interface with general-purpose, non-industrial IT systems, improving functions like reporting, planning, and workflow management. However, this increased connectivity also expands the cyberattack surface by exposing critical infrastructure to common IT threats. A high-level overview of third-generation SCADA architecture is shown in Fig. 4.

D. Fourth Generation Supervisory Control and Data Acquisition Systems

The evolution of communication technologies and the widespread adoption of the IoT have led to the emergence of smart systems such as smart homes, cities, grids, and factories. The adaptation of industrial devices to this context introduced the concept of the IIoT [33]. With the Industry 4.0 paradigm, cyber-physical systems gained importance, enabling digital modeling and autonomous control of production processes.

In fourth-generation SCADA systems, cloud and IoT technologies are integrated to overcome the limitations of classical systems. IP-based field devices, introduced in the previous generation, facilitate connectivity, while IoT sensors enhance data collection capabilities. The volume and resolution of collected data make manual operator intervention less practical; instead, cloud-based SCADA systems support autonomous decision-making by processing data and monitoring field parameters in real time.

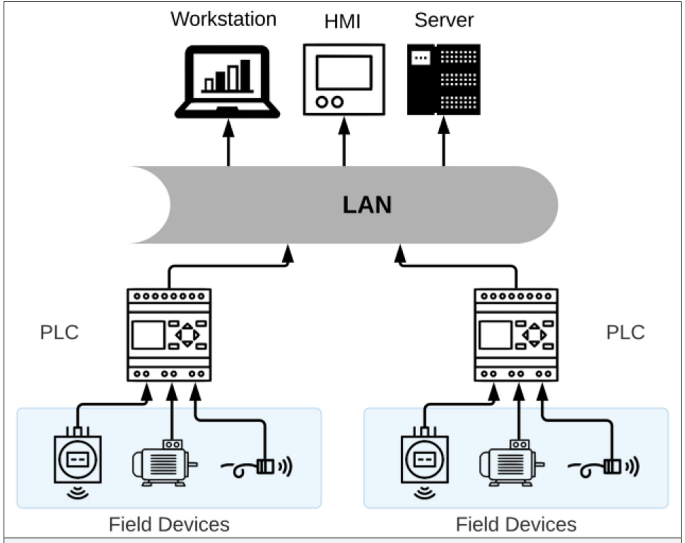


Fig. 4. Third-generation supervisory control and data acquisition.

These systems offer significant advantages in terms of scalability, accessibility, and operational flexibility. However, this openness also introduces new cybersecurity risks. Unlike traditional systems, which benefited from isolated networks, cloud-integrated SCADA environments expose legacy protocols and unpatched systems to external threats. The vulnerabilities inherent in IoT and cloud platforms increase both the attack surface and the impact of potential threats.

A high-level depiction of fourth-generation SCADA architecture is presented in Fig. 5.

Supervisory control and data acquisition systems have evolved in parallel with the needs of industrial automation, transitioning from closed-loop architectures to more accessible, flexible, and powerful IoT- and cloud-based structures. However, this transformation has also introduced new security vulnerabilities that must be carefully addressed.

V. PROPERTIES OF SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

Supervisory control and data acquisition systems differ significantly from IT systems in terms of operational requirements and principles. Commercial off-the-shelf solutions developed for IT environments are often incompatible with SCADA systems due to their unique characteristics. As outlined in NIST SP 800-82 [3], SCADA systems must

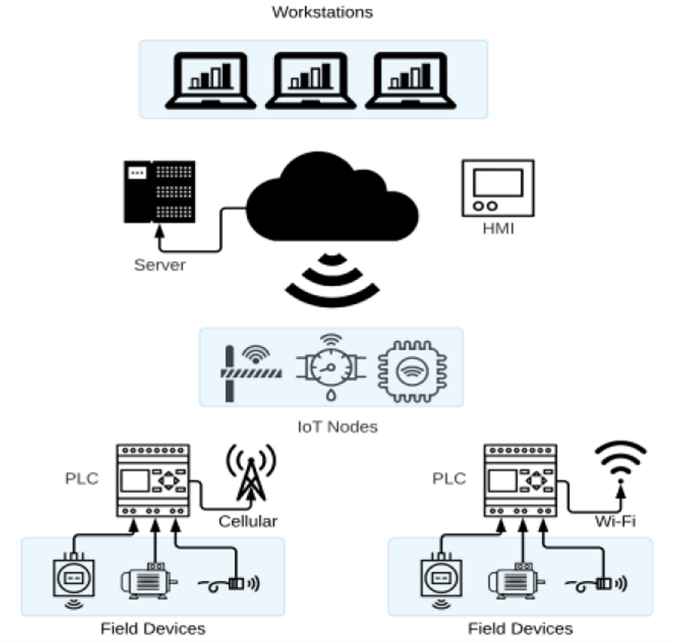


Fig. 5. Fourth generation supervisory control and data acquisition.

TABLE I. SUPERVISORY CONTROL AND DATA ACQUISITION PROPERTIES

		Traditional SCADA Systems			IoT-Based SCADA Systems
Category	**Property**	**1st Gen.**	**2nd Gen.**	**3rd Gen.**	**4th Gen.**
Communication	Serial	✓	✓	✓	✓
	Ethernet		✓	✓	✓
	Cloud				✓
Auditing	Multi-point monitoring		✓	✓	✓
	Multi-point control			✓	✓
	Real-time monitoring			✓	✓
Vertical integration	Reporting tool integration			✓	✓
	OS support (except Windows X)				✓
	Historical data storage			✓	✓
	Historical data analyze				✓
	Enterprise application integration (as Systems, Applications, and Products(SAP))			Partially	✓
	Machine produce data signification				✓
Horizontal integration	Multi-vendor interoperability				✓
	Plug and play capability				✓
Accessibility	Worldwide access			Partially	✓
	Fine-grained data processing				✓
	Multi-level operator authorization			✓	✓
	Non-PLC interoperability				✓

Gen, generation; OS, operating system; PLC, programmable logic controller; SCADA, supervisory control and data acquisition.

maintain long-term stability, fault tolerance, time-critical performance, efficient resource usage, and minimal need for intervention.

These systems are expected to operate continuously at consistent performance levels without error. Their real-time requirements are classified as either complex or soft real-time [18]. While soft real-time disruptions may be tolerable (e.g., video lag), delays in complex real-time systems can lead to severe consequences, such as critical failures in industrial processes.

Supervisory control and data acquisition field devices are typically constrained in terms of processing power and memory, making them unsuitable for computationally intensive tasks such as encryption or data validation. Furthermore, these devices are geographically distributed and often remain in operation for extended periods without updates, leading to legacy hardware and software still being in use.

Technological advancements in communication infrastructures have shaped SCADA system evolution across generations. These developments have improved communication reliability, system functionality, manageability, and stability. Vertically, SCADA systems interact with field-level devices (e.g., PLCs, RTUs) and upper-layer IT systems (e.g., HMIs, reporting tools). Horizontally, they often rely on vendor-specific communication protocols, limiting interoperability.

The classification of SCADA generations reflects fundamental differences in communication technologies and system capabilities. Key features such as real-time monitoring, control, vertical and horizontal integration, and accessibility define the progression of these systems. Table I summarizes these generational distinctions under categories including communication, monitoring, vertical integration, horizontal integration, and accessibility.

In the remainder of this article, SCADA systems are analyzed under two primary categories, traditional and IoT-based, highlighting their fundamental differences in accessibility requirements, communication infrastructures, and vertical and horizontal integration frameworks.

VI. CHARACTERISTICS AND VULNERABILITIES OF SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS

When examining SCADA systems across four generations in terms of cybersecurity vulnerabilities, it is more effective to group attack surfaces and types of attacks. For this reason, SCADA systems are categorized into two main groups to better identify suitable targets during the analysis of current threats. The first group comprises traditional SCADA systems, which operate on networks isolated from the internet. The second group includes IoT-based SCADA systems adapted to IIoT and cloud architectures. Historically, security analyses have focused primarily on traditional SCADA systems. However, assessing vulnerabilities in today's environment requires first determining whether the system is traditional or IoT-based, as this distinction is critical for accurately identifying attack surfaces, system characteristics, and potential weaknesses. Importantly, many considerations relevant to traditional systems remain applicable in the cybersecurity assessment of IoT-based SCADA systems. Therefore, the following section discusses the key characteristics and security vulnerabilities of both traditional and IoT-based SCADA systems.

A. Characteristics and Vulnerabilities of Traditional Supervisory Control and Data Acquisition Systems

In this section, SCADA systems up to the third generation are classified as traditional SCADA systems. The defining characteristics of these systems, along with the vulnerabilities arising from them, are outlined below. Due to the critical nature of the operations they control, the wide geographical distribution of field components, and the use of outdated hardware and software, traditional SCADA systems are highly susceptible to severe physical consequences in the event of system failure or cyberattack. These systems possess multiple contact points that may serve as potential attack surfaces. Given their distinct operational requirements and legacy structures, traditional SCADA systems must be evaluated separately from modern systems when analyzing cybersecurity vulnerabilities.

1) General-Purpose Operating System Usage:

The use of GPOS such as Windows and Linux in industrial environments introduces additional risks, especially when security updates are delayed or ignored. For instance, the WannaCry ransomware attack in 2017 exploited a known vulnerability in unpatched Windows systems and affected various industrial and healthcare infrastructures worldwide. Similarly, many ICS breaches have been linked to outdated or misconfigured operating systems, underscoring the importance of timely patch management in operational technology (OT) environments. Supervisory control and data acquisition systems often rely on GPOS to run HMI components. These systems include many unnecessary services that may contain vulnerabilities not relevant to SCADA, increasing the attack surface.

Since SCADA systems are usually isolated from the internet, security patches are often delayed or skipped. This allows attackers to exploit known weaknesses. For example, the Stuxnet case took advantage of unpatched vulnerabilities for over 2 years [34]. Supervisory control and data acquisition systems typically operate for 7–15 years [35], whereas operating systems like Windows have shorter lifespans—about 5 years of main support and 10 years of extended support [36]. This means SCADA systems often require at least one OS upgrade during their lifetime. Despite the end of support for Windows XP and the existence of many public exploits, it remains in use in SCADA systems due to library incompatibilities, lack of updates, and licensing issues. This highlights the security risks arising from outdated operating systems.

2) Protocol-Based Vulnerabilities:

Many SCADA protocols were designed for closed environments and lack basic security features like encryption and authentication [37]. As communication infrastructures evolved, these insecure protocols remained largely unchanged for compatibility, making them vulnerable to network-based attacks. Attackers can intercept traffic, inject malicious data, or analyze protocol behavior due to the lack of built-in protection [38].

3) Social Engineering Attacks:

Social engineering exploits human vulnerabilities rather than technical ones, often targeting operators using HMI systems [39]. A notable example is the Stuxnet attack, where malware was introduced through a Universal Serial Bus (USB) stick and manipulated PLC code while masking changes with normal-looking data [40, 41]. Phishing emails and unauthorized web use on control computers also increase exposure to social engineering threats [41, 42].

4) Malware:

Malware in SCADA environments can hijack control logic, alter configurations, or establish persistent access through backdoors. Well-known examples like Stuxnet, Flame, and Duqu demonstrate how malware can exploit IT systems' weaknesses to reach SCADA targets

[34, 40, 43, 44]. Once embedded, such malware may remain undetected while executing unauthorized operations, even altering physical processes.

5) Advanced Persistent Threat:

Advanced persistent threat attacks are long-term, stealthy cyber threats, often carried out by state-sponsored groups targeting critical infrastructure [45, 46]. These threats are characterized by advanced techniques, persistence, and tailored strategies that allow them to infiltrate and remain within systems for years. Advanced persistent threats adapt over time, learn system behaviors, and can cause significant disruption while remaining unnoticed [47].

6) Discoverability:

The adoption of cloud technologies has increased SCADA system accessibility, making them easier to discover and potentially attack. The installation process has become more streamlined, but exposed systems may be scanned, identified, and probed by attackers for vulnerabilities [48]. This visibility increases the likelihood of exploitation, especially if security configurations are weak or incomplete.

7) Shared Server Usage:

When SCADA systems share infrastructure with general IT services or use web-based solutions like WebSCADA, the entire environment is exposed to additional risk [7]. A vulnerability in any shared service can compromise the SCADA system, as attackers can identify and exploit connected processes. Security is only as strong as the weakest component, making shared environments particularly dangerous.

8) Configuration Mistakes:

Improper or incomplete configurations during setup or maintenance are a common source of vulnerabilities in SCADA systems [8]. These errors prevent security mechanisms from functioning correctly and may expose sensitive components to unauthorized access. Misconfigured systems fail to meet security policies, leading to potential breaches or system failures [49].

9) Third-Party Library Usage:

In SCADA systems, third-party libraries are often used to manage heterogeneous devices and protocols. However, using unverified or unknown libraries can introduce hidden backdoors and security vulnerabilities [50]. Ensuring the security and stability of all libraries, especially during installation, is essential, as seen in attacks like Stuxnet that exploited software components to access sensitive data.

10) Denial-of-Service Attack:

A denial-of-service (DoS) attack aims to make systems unavailable by overwhelming them with traffic or exploiting system weaknesses. This disrupts services and can result in potential financial loss due to downtime or inaccessibility of critical systems.

11) Authentication Attacks:

These attacks target weaknesses in login mechanisms, aiming to bypass or break authentication controls. They often involve stealing or guessing credentials (like usernames and passwords) to gain unauthorized access to systems.

12) Structured Query Language Injection:

Structured query language (SQL) injection is a type of attack where malicious SQL code is inserted into input fields to manipulate or access a database without authorization. It exploits poor input validation and can result in data theft, modification, or full control over the database.

B. Characteristics and Vulnerabilities of IoT-Based Supervisory Control and Data Acquisition Systems

Today's SCADA systems in the field are increasingly integrated with IoT sensors, creating a new generation of interconnected control systems. This fusion significantly expands the attack surface, making these fourth-generation SCADA systems more vulnerable. Consequently, they inherit both the traditional weaknesses of legacy SCADA and the emerging vulnerabilities of the IoT ecosystem, heightening the risk of exploitation.

1) Brute-Force Attack:

Brute-force attacks involve attackers trying to bypass login systems through trial-and-error methods, often using dictionaries based on leaked data. These attacks are especially effective against systems with default configurations and credentials. Proper security policies and avoiding default passwords reduce their success.

2) Buffer Overflow:

Buffer overflow happens when data exceeding a buffer's size is written, causing memory to overflow into adjacent areas, leading to erratic program behavior and privilege escalation. Attackers can gain control over the operating system layer by exploiting unchecked input sizes [51].

3) Sybil:

Sybil attacks exploit surplus or forgotten devices by assigning them multiple fake identities. The aim is to disrupt data integrity and resource management, thereby degrading network performance. This compromises system availability and causes operational errors [52].

4) Wormhole:

In wormhole attacks, malicious devices exploit routing protocols by advertising low-latency paths, only to drop any packets that pass through them. This disrupts communication and causes real-time system failures [53].

5) Hardware Trojan:

A hardware Trojan is a malicious circuit modification embedded during production that activates via internal counters or external signals, causing data leakage or incorrect operations. These pose significant risks to embedded system security [54].

6) Battery Draining:

Battery-draining attacks rapidly exhaust the energy of battery-powered field devices by flooding them with packets or authentication requests, leading to device unavailability and critical system failures.

7) Sleep Deprivation:

Sleep deprivation attacks prevent resource-limited devices from entering sleep mode, causing rapid battery depletion and shutdown. This results in data collection gaps and system disruptions.

8) Node Replication:

Node replication involves creating counterfeit devices. These devices have stolen device identities. The counterfeit devices flood the network with duplicate transmissions. These duplicate transmissions cause communication failures and confusion [55].

9) Side-Channel Attack:
Side-channel attacks exploit unintended data leaks such as electromagnetic emissions or power consumption patterns to extract sensitive information from IIoT devices, bypassing traditional security measures.

10) Cloud Malware Injection:
This attack injects malicious code into IIoT systems by exploiting vulnerabilities, risking data integrity, operational safety, and causing disruptions in critical industrial processes.

11) Mobile Device Attacks:
Mobile device attacks target portable devices to steal personal and sensitive data, causing privacy breaches and financial losses.

12) Eavesdropping:
Eavesdropping intercepts network traffic between devices and servers to steal sensitive information, often exploiting weak connections [55].

13) Black-Hole Attack:
A black-hole attack selectively drops network packets, disrupting communication and causing DoS, especially in wireless ad-hoc networks.

14) Wireless Jamming:
Wireless jamming blocks communication by interfering with specific frequencies, preventing legitimate data transmission. Frequency hopping techniques can mitigate these attacks.

15) Miscellaneous Attacks:
Various attacks in IIoT environments include malware injection, device hijacking, data theft, DNS poisoning, and botnets, all posing significant threats to operational and IT layers [55].

VII. TAXONOMY

The MITRE ATT&CK Framework constitutes a comprehensive, empirically grounded knowledge base that systematically classifies adversarial behavior through tactics, techniques, and procedures observed in real-world cyber incidents. Serving as a foundational tool in the domain of cyber threat intelligence and attack classification, the framework enables security analysts and researchers to model, detect, and respond to malicious activities in a structured and consistent manner. By mapping attacker behavior across the stages of an intrusion, MITRE ATT&CK facilitates a deeper understanding of threat actor methodologies and supports the development of more effective defense strategies. Its adoption in both academic and operational contexts underscores its significance in advancing proactive cybersecurity practices and threat-informed defense architectures.

The Purdue Enterprise Reference Architecture, commonly known as the Purdue Model, is a hierarchical framework designed to conceptualize the segmentation and control of industrial automation systems across five distinct levels—from physical devices at the lowest level to enterprise systems at the top. Originally developed to support ICS design and management, the model facilitates clear delineation of functional domains, data flow, and trust boundaries within OT environments. By promoting logical isolation between control layers, it supports risk mitigation and enables more effective deployment of cybersecurity controls tailored to each level.

TABLE II. MITRE-BASED ATTACK CLASSIFICATION

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Tactics	Attacks
Initial access	• Social engineering attacks • Protocol-based vulnerabilities • APT • Configuration mistakes • Authentication attacks • Brute-force attack • SQL injection • Cloud malware injection • Mobile device attacks • Miscellaneous attacks
Execution	• General-purpose operating system usage • Protocol-based vulnerabilities • SQL injection • Malware • Cloud malware injection
Persistence	• General-purpose operating system usage • Malware • Third-party library usage • Hardware Trojan • APT
Privilege escalation	• Authentication attacks • Brute-force attack • Buffer overflow • Configuration mistakes
Evasion	• Sybil • Wormhole • Node replication • Side-channel attack
Discovery	• Discoverability • Side-channel attack • Mobile device attacks • Eavesdropping
Lateral movement	• Shared server usage • APT • Node replication • Wormhole
Command and control	• Malware • Cloud malware injection • Mobile device attacks
Inhibit response function	• Protocol-based vulnerabilities • Byzantine • Wireless jamming • Denial-of-service attack
Impair process control	• Hardware Trojan • Battery draining • Sleep deprivation • Black hole

APT, advanced persistent threat; SQL, structured query language.

A review of the literature shows that cyberattacks on SCADA systems are rarely analyzed using both the MITRE ATT&CK framework and the Purdue Model together. The MITRE ATT&CK framework is commonly used to describe attacker behaviors, while the Purdue Model shows the layered structure of industrial systems. In this study, both frameworks have been used to classify attacks in a clearer and more organized way. Table II lists common attack techniques from the MITRE ATT&CK framework. Table III links these techniques to the relevant levels of the Purdue Model. By combining the two, one can better understand which parts of the system are affected and how an attacker might move between layers. This approach helps provide a more complete view of cybersecurity risks and supports better planning for defense strategies.

When combined with the MITRE ATT&CK for ICS framework, the Purdue Model offers a powerful lens through which to map, analyze, and defend against cyber threats targeting industrial systems. The integration of these two models enhances visibility across both IT and OT layers, enabling threat-informed defense strategies that are contextually aligned with the architectural layout of industrial environments.

VIII. CONCLUSION

In this study, SCADA systems were systematically categorized into four distinct generations and evaluated through both generation- and category-based vulnerability analyses, filling a crucial gap in existing research that often treats SCADA systems as a monolithic group despite their significant technological differences. This nuanced approach reveals that understanding the specific vulnerabilities inherent to each generation is vital for developing tailored, robust security architectures and effective prevention mechanisms. As critical infrastructures such as energy distribution, nuclear, and chemical plants face ever-growing cyber threats, the stakes have never been higher: failure to recognize and address generation-specific risks can lead to catastrophic consequences on a national security level. Therefore, aligning vulnerability assessments, security standards, and operational policies explicitly with the SCADA generation in use is not just recommended—it is imperative. Only by doing so can organizations ensure adaptive resilience, protect critical operations, and stay one step ahead of increasingly sophisticated cyberattacks targeting these vital systems.

This study reveals that as field-deployed SCADA systems evolve into interconnected ecosystems leveraging modern technologies, entirely new attack surfaces will inevitably emerge. The critical importance of generation-based analysis has been proven, particularly in identifying and reporting vulnerabilities tied to these expanding attack surfaces. Future research will focus on developing comprehensive test environments categorized into two main types: traditional SCADA systems and IoT-integrated systems. These environments will rigorously analyze the attack vectors unique to each setup, enabling precise identification of vulnerabilities and optimal configuration parameters tailored to the specific SCADA generation deployed in the field.

Moreover, by integrating generation-based attack surface analysis with advanced risk assessment methodologies, forthcoming studies aim to deliver highly accurate, system-specific security evaluations, paving the way for more resilient and adaptive defense strategies against the evolving threat landscape in critical infrastructure cybersecurity.

TABLE III. PURDUE-BASED ATTACK CLASSIFICATION

Purdue Layer	Description	Related Attacks and Vulnerabilities
Layer 5 – Enterprise network	Enterprise IT systems (Enterprise Resource Planning (ERP), email, financial systems)	Social engineering attacks, advanced persistent threat (APT), general-purpose operating system usage, malware, configuration mistakes, shared server usage, third-party library usage, authentication attacks, SQL injection, brute-force attack, cloud malware injection, mobile device attacks, miscellaneous attacks
Layer 4 – Site business planning and logistics	Manufacturing execution system, quality control systems, production planning software	Social engineering attacks, APT, general-purpose operating system usage, malware, configuration mistakes, third-party library usage, authentication attacks, SQL injection, brute-force attack, buffer overflow, cloud malware injection, mobile device attacks, denial-of-service attack, miscellaneous attacks
Layer 3 – Operations/ Demilitarized Zone (DMZ)	SCADA systems, production management, Information Technology – Operational Technology (IT-OT) interface (DMZ)	APT, general-purpose operating system usage, malware, configuration mistakes, shared server usage, protocol-based vulnerabilities, authentication attacks, brute-force attack, buffer overflow, Sybil, node replication, mobile device attacks, discoverability, denial-of-service attack, miscellaneous attacks
Layer 2 – Area supervisory control	SCADA servers, HMIs, process data collection	APT, malware, configuration mistakes, protocol-based vulnerabilities, brute-force attack, buffer overflow, Sybil, wormhole, node replication, side-channel attack, eavesdropping, black-hole, Byzantine, wireless jamming, discoverability, denial-of-service attack, miscellaneous attacks
Layer 1 – Basic control	Basic control devices such as PLC, RTU, DCS	Configuration mistakes, protocol-based vulnerabilities, wormhole, Hardware Trojan, battery draining, sleep deprivation, node replication, side-channel attack, eavesdropping, black-hole, Byzantine, wireless jamming, miscellaneous attacks
Layer 0 – Physical process	Sensors, actuators, physical production processes	Hardware Trojan, battery draining, sleep deprivation, eavesdropping, wireless jamming, miscellaneous attacks

DCS, distributed control system; HMI, human-machine interface; IT, Information Technology; PLC, programmable logic controller; RTU, remote terminal unit; SCADA, supervisory control and data acquisition; SQL, structured query language.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – M.Y.Y., Ş.D.O.; Design – M.Y.Y., Ş.D.O.; Supervision – M.A.A.; Resources – M.Y.Y., Ş.D.O.; Materials – M.Y.Y., Ş.D.O.; Data Collection and/or Processing – M.Y.Y., Ş.D.O.; Analysis and/or Interpretation – M.Y.Y., Ş.D.O.; Literature Search – M.Y.Y., Ş.D.O.; Writing – M.Y.Y., Ş.D.O.; Critical Review – M.Y.Y., Ş.D.O.

Declaration of Interests: The authors have no conflicts of interest to declare.

Funding: The authors declared that this study has received no financial support.

REFERENCES

1. B. Kesler, "The vulnerability of nuclear facilities to cyber attack," *Strateg. Insights*, vol. 10, no. 1, pp. 15–25, 2011.
2. S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Sec.*, vol. 70, pp. 436–454, 2017. [CrossRef]
3. K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, *Guide to Industrial Control Systems (ICS)*. Security, Gaithersburg, MD: National Institute of Standards and Technology, 2015.
4. NIST, *"NVD - Home."* [Online]. Available: https://nvd.nist.gov/. [Accessed: May 25, 2025].
5. MITRE, *"CVE - Common Vulnerabilities and Exposures (CVE)."* [Online]. Available: https://cve.mitre.org/. [Accessed: May 16, 2025].
6. MITRE, *"CWE - Common Weakness Enumeration."* [Online]. Available: https://cwe.mitre.org/. [Accessed: May 25, 2025].
7. A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016. [CrossRef]
8. A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, 103165, 2020. [CrossRef]
9. T. Bartman, and K. Carson, "Securing communications for SCADA and critical industrial systems," in *Proc. 2016 69th Annual Conference for Protective Relay Engineers*. New York: IEEE, 2016, pp.1–10. [CrossRef]
10. S. Ghosh, and S. Sampalli, “A survey of security in scada networks:current issues and future challenges,” *IEEE Access*, vol. 7, pp. 135812–135831, 2019. [CrossRef]
11. Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. 2017 IEEE Conf. Energy Internet and Energy System Integration*, vol. EI2. Beijing, China: IEEE, Nov. 2017, pp. 1–6. [CrossRef]
12. B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. 2011 Int. Conf. Internet of Things and 4th Int. Conf. Cyber, Physical and Social Computing*, Dalian, China. New York: IEEE, 2011, pp. 380–388. [CrossRef]
13. M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on CPS," in *Proc. 2nd ACM Int. Conf. High Confidence Networked Systems (HiCoNS)*, Philadelphia, PA, USA. New York, NY, USA: ACM, 2013, pp. 135–142. [CrossRef]
14. D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *Proc. 2015 13th Annu. Conf. Privacy, Security and Trust (PST)*, Izmir, Turkey. New York: IEEE, 2015, pp. 145–152. [CrossRef]
15. E. Irmak, and I. Erkek, "An overview of cyber-attack vectors on SCADA," in *Proc. 2018 6th Int. Symp. Digital Forensic and Security (ISDFS)*, Antalya, Turkey, 2018, pp. 1–5.
16. D. Upadhyay, and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations," *Comput. Secur.*, vol. 89, p. 101666, 2020. [CrossRef]
17. M. R. Asghar, Q. Hu, and S. Zeadally, "Cybersecurity in industrial control systems: Issues, technologies, and challenges," *Comput. Netw.*, vol. 165, p. 106946, Dec. 2019. [CrossRef]
18. M. Cheminod, L. Durante, L. Seno, and A. Valenzano, "Performance evaluation and modeling of an industrial application-layer firewall," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 2159–2170, 2018. [CrossRef]
19. E. Yalcinkaya, A. Maffei, and M. Onori, "Application of attribute-based access control model for industrial control systems," *IJCNIS*, vol. 9, no. 2, pp. 12–21, 2017. [CrossRef]
20. V. Graveto, L. Rosa, T. Cruz, and P. Simões, "A stealth monitoring mechanism for cyber-physical systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 24, pp. 126–143, 2019. [CrossRef]
21. T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control systems using logical analysis of data," *Comput. Secur.*, vol. 96, p. 101935, 2020. [CrossRef]
22. 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. [CrossRef]
23. A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *Proc. 2018 IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*. New York: IEEE, 2018, pp. 124–130. [CrossRef]
24. A. A. el Kalam, "Securing SCADA and critical industrial systems: From needs to security mechanisms," *Int. J. Crit. Infrastruct. Prot.*, vol. 32, p. 100394, 2021. [CrossRef]
25. B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. 2015 IEEE Int. Workshop Tech, Comm. Qual. Reliab. (CQR)*, pp. 1–6, 2015.
26. J. Luswata, P. Zavarsky, B. Swar, and D. Zvabva, "Analysis of SCADA security using penetration testing: A case study on Modbus TCP protocol," in *Proc. 2018 29th Biennial Symp. Commun. (BSC)*. New York: IEEE, 2018, pp. 1–5. [CrossRef]
27. Modbus Organization, "MODBUS messaging on TCP/IP implementation guide V1.0b," [Online]. Available: https://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf. Accessed: May 15, 2025.
28. T. Müller, and H. D. Doran, "Protecting PROFINET cyclic real-time traffic: A performance evaluation and verification platform," in *Proc. 2018 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2018, pp. 1–4.
29. T. Müller, and H. D. Doran, "PROFINET real-time protection layer: Performance analysis of cryptographic and protocol processing overhead," in *Proc. 2018 IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, Sep. New York: IEEE, 2018, pp. 258–265. [CrossRef]
30. R. Amoah, S. Camtepe, and E. Foo, "Formal modelling and analysis of DNP3 secure authentication," *J. Netw. Comput. Appl.*, vol. 59, pp. 345–360, 2016. [CrossRef]
31. A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer, "Security challenges in control network protocols: A survey," *IEEE Commun. Surv. Tutor.*, Firstquarter 2019, vol. 21, no. 1, pp. 619–639, 2019. [CrossRef]
32. A. Homay, C. Chrysoulas, B. E. El Boudani, M. de Sousa, and M. Wollschlaeger, "A security and authentication layer for SCADA/DCS applications," *Microprocess. Microsyst.*, vol. 87, p. 103479, 2021. [CrossRef]
33. S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–53, 2021. [CrossRef]
34. R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy Mag.*, vol. 9, no. 3, pp. 49–51, 2011. [CrossRef]
35. C. M. Lewandowski et al., “Operating system concepts,” *Wiley Sons*, vol. 1, pp. 40–46, 2013.
36. “Windows life cycle,” *"Windows Life Cycle FAQ,"* [Online]. Available: https://learn.microsoft.com/en-us/lifecycle/faq/windows. [Accessed: May 1, 2025].
37. W. Su, A. Antoniou, and C. Eagle, "Cyber security of industrial communication protocols," in *Proc. 2017 IEEE 22nd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*. New York: IEEE, Sep. 2017, pp. 1–4. [CrossRef].
38. G. Hayes, and K. El-Khatib, “‘Securing Modbus transactions using hash-based message authentication codes and stream transmission control protocol,’ in *Proc. 2013”* 3rd Int. Conf. Commun. Inf. Technol. (ICCIT), 2013, pp. 179–184.
39. J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," *Comput. Secur.*, vol. 83, pp. 354–366, 2019. [CrossRef]
40. Symantec, N. M. Failliere, O. Liam, and E. Chien, *W32.Stuxnet Dossier n.d*, 2011.

41. A. Binks, "The art of phishing: Past, present and future," *Comput. Fraud Secur.*, vol. 2019, no. 4, pp. 9–11, 2019. [CrossRef]

42. “Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks, the henry M.” Jackson School of International Studies. [Online]. Available: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/. [Accessed: May 21, 2025].

43. S. Z. M. Shaid, and M. A. Maarof, "Malware behavior image for malware variant identification," in Int. Symp. Biometrics Secur. Technol. (ISBAST), 2014, pp. 238–243.

44. K. Thakur, M. L. Ali, N. Jiang, and M. Qiu, "Impact of cyber-attacks on critical infrastructure," in *Proc. 2016 IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity)*, IEEE Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS), 2016, pp. 183–186. [CrossRef]

45. L. A. Maglaras *et al.*, "Cyber security of critical infrastructures," *ICT Express*, vol. 4, no. 1, pp. 42–45, 2018. [CrossRef]

46. Y. Qi, R. Jiang, Y. Jia, and A. Li, "An APT attack analysis framework based on self-define rules and MapReduce," in *Proc. 2020 IEEE 5th Int. Conf. Data Sci. Cyberspace (DSC)*. New York: IEEE, 2020, pp. 61–66. [CrossRef]

47. B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, p. 101734, 2020. [CrossRef]

48. D. N. Jones, E. Padilla, S. R. Curtis, and C. Kiekintveld, "Network discovery and scanning strategies and the Dark Triad," *Comput. Hum. Behav.*, vol. 122, p. 106799, 2021. [CrossRef]

49. K. S. Kiangala, and Z. Wang, "An Industry 4.0 approach to develop auto parameter configuration of a bottling process in a small to medium scale industry using PLC and SCADA," *Procedia Manuf.*, vol. 35, pp. 725–730, 2019. [CrossRef]

50. J. Tian, W. Xing, and Z. Li, "BVDetector: A program slice-based binary code vulnerability intelligent detection system," *Inf. Softw. Technol.*, vol. 123, p. 106289, 2020. [CrossRef]

51. Ş. Nicula, and R. D. Zota, "Exploiting stack-based buffer overflow using modern day techniques," *Procedia Comput. Sci.*, vol. 160, pp. 9–14, 2019. [CrossRef]

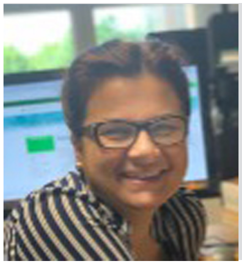
52. P. Kaliyar, W. B. Jaballah, M. Conti, and C. Lal, "LiDL: Localization with early detection of sybil and wormhole attacks in IoT networks," *Comput. Secur.*, vol. 94, p. 101849, 2020. [CrossRef]

53. S. Deshmukh-Bhosale, and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things," *Procedia Manuf.*, vol. 32, pp. 840–847, 2019. [CrossRef]

54. S. Bhasin, and F. Regazzoni, "‘A survey on hardware trojan detection techniques,’ in Proc. IEEE Int. Symp,” *Circuits Syst.. (ISCAS)*, pp. 2021–2024, 2015.

55. J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 280–308, 2023. [CrossRef]

Mehmet Yavuz Yağcı received his B.Sc. degree in Computer Engineering from Karadeniz Technical University in 2017. He completed his M.Sc. at Istanbul University in 2020 and earned his Ph.D. in Cybersecurity from Istanbul University-Cerrahpaşa in 2024. His academic work has primarily focused on operational technology (OT) security, industrial control systems (ICS), SCADA systems, and network traffic analysis. He has participated in various projects involving the analysis of proprietary OT protocols and the detection of cyber threats in industrial environments and has published academic studies in these areas.



Şafak Durukan-Odabaşı received the B.S., M.S., and Ph.D. degrees in Computer Engineering from Istanbul University, Istanbul, Türkiye, in 2005, 2008, and 2013. She worked as a Research Assistant and Assistant Professor of Computer Engineering at Istanbul University and Istanbul University-Cerrahpaşa between 2005-2019. She was a Visiting Assistant Professor at Illinois Wesleyan University, USA, from 2019 to 2021. She is currently working as an Assistant Professor at Istanbul University – Cerrahpaşa. Her research areas are next-generation networks, IoT, and cybersecurity.

Muhammed Ali Aydın received the Ph.D. degree in computer engineering from Istanbul University. He was a Postdoctoral Researcher with the Department of Computer Science, Telecom SudParis. He is currently a Professor with the Department of Computer Engineering, Istanbul University-Cerrahpaşa. His research interests include cyber security, cryptography, network security, and communication-network protocols.