







RESEARCH ARTICLE

OPEN ACCESS

CYBERSECURITY RISK MITIGATION IN INDUSTRIAL CONTROL SYSTEMS ANALYZING PHYSICAL HYBRID AND VIRTUAL TEST BED APPLICATIONS

¹ H M Shamsuzzaman , ² MD Mosleuzzaman , ³ Arif Mia , ⁴ Anup Nandi 

¹Master in Electrical and Electronics Engineering, College of Engineering, Lamar University, Beaumont, TX, USA
Email: hshamsuzzama@lamar.edu

²Master in Industrial and Systems Engineering, University of Michigan-Dearborn, Dearborn, MI, USA
Email: mosle@umich.edu

³Master in Electrical and Electronics Engineering, College of Engineering, Lamar University, Beaumont, TX, USA
Email: arif1602125@gmail.com

⁴Master in Electrical and Electronics Engineering, College of Engineering, Lamar University, Beaumont, TX, USA
Email: anandi1@lamar.edu

ABSTRACT

Industrial Control Systems (ICS) play a vital role in industries such as oil, utilities, and manufacturing, forming the backbone of critical infrastructure. With the increasing integration of network capabilities in ICS, their exposure to cyber-attacks has grown significantly. However, due to the sensitivity of these systems, access to detailed technical information is limited, making cybersecurity research challenging. To address this, researchers have employed various physical, hybrid, and virtual testbeds to simulate and analyze cyber threats. This systematic review, conducted following PRISMA guidelines, aims to evaluate the effectiveness of these testbeds in mitigating cybersecurity risks in ICS, particularly within the context of a clean water supply system. The findings reveal that physical testbeds offer a comprehensive understanding of the behavior and dynamics of ICS components, such as sensors and actuators, under real-world conditions affected by external factors like pressure, temperature, and mechanical wear. However, physical testbeds' high cost and complexity limit their widespread use. While more cost-effective, hybrid testbeds fail to capture crucial physical dynamics, which may lead to incomplete assessments of cybersecurity vulnerabilities. Virtual testbeds provide the most affordable option, offering scalability and ease of implementation. However, they deliver a limited view of ICS operations that can impair the development of accurate detection and prevention mechanisms. The results underscore the trade-offs associated with each testbed type, suggesting that an integrated approach, blending physical and virtual elements, may offer the most effective framework for cybersecurity research in ICS while balancing cost and realism.

KEYWORDS

Industrial Control Systems (ICS); Cybersecurity Testbeds; Physical Testbeds; Hybrid Testbeds; Virtual Testbeds

Submitted: September 04, 2024

Accepted: October 15, 2024

Published: October 18, 2024

Corresponding Author:

H M Shamsuzzaman

¹Master in Electrical and Electronics Engineering, College of Engineering, Lamar University, Beaumont, TX, USA

email: hshamsuzzama@lamar.edu

 [10.69593/ajaimldsmis.v1i01.123](https://doi.org/10.69593/ajaimldsmis.v1i01.123)



1 Introduction

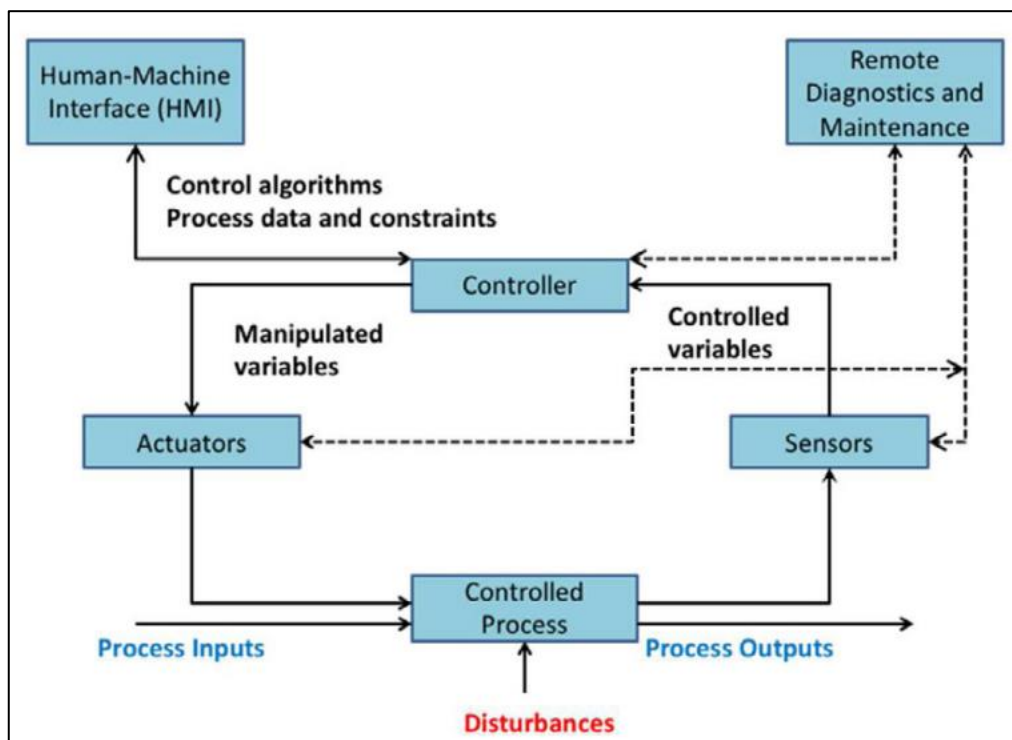
Industrial Control Systems (ICS) are fundamental to the functioning of critical infrastructure across sectors such as energy, manufacturing, and water supply (Alsharida et al., 2023). Traditionally, these systems operated in isolated environments, utilizing proprietary protocols and relying on physical security measures to ensure their safety (Nunamaker & Chen, 1990). However, with the advancement of modern communication technologies and the increasing interconnection of networks, ICS have become more integrated with traditional IT systems, significantly increasing their exposure to cybersecurity risks (Kurpjuhn, 2015). The shift from isolated systems to networked environments has made ICS vulnerable to a range of cyber-attacks that could disrupt essential operations, causing serious economic, environmental, and safety hazards (Ebrahimi et al., 2020). As a result, ensuring the security of ICS has become an urgent concern for both researchers and industry professionals (Haag et al., 2021). This concern has led to the development of sophisticated techniques for identifying, detecting, and mitigating cyber threats (Guezzaz et al., 2021). Among these efforts, various

testbeds have been developed and implemented as tools for simulating ICS environments, enabling the evaluation of security vulnerabilities in controlled

settings (Benaroch, 2018). These testbeds provide valuable insights into potential attack vectors and defense mechanisms, making them essential for advancing the state of ICS security (See Figure 1).

The evolution of ICS cybersecurity has followed the trajectory of industrial automation. Early ICS security measures were primarily physical, relying on restricted access to facilities and manual control over system components (Ebrahimi et al., 2020). However, with the introduction of programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems, ICS gradually adopted digital technologies, increasing their exposure to cyber-attacks. Initial cyber defense strategies focused on securing communication channels and implementing basic encryption techniques to prevent unauthorized access (Le et al., 2024). These early approaches, while effective for isolated systems, proved insufficient in the face of sophisticated cyber-attacks, such as the Stuxnet worm, which targeted SCADA systems in 2010 (Benaroch, 2018). The

Figure 1: Integration of dynamic simulation modeling and big data



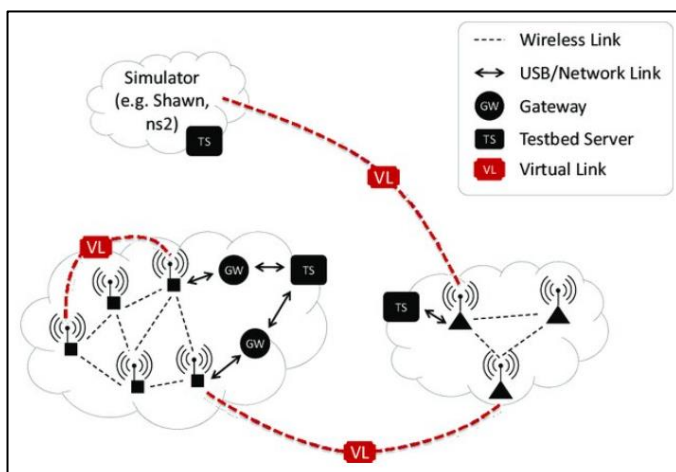
Source: Bhamare et al. (2020)

Stuxnet attack marked a turning point in ICS cybersecurity, illustrating the potential for cyber-attacks to cause physical damage to critical infrastructure. This event catalyzed the development of more comprehensive cybersecurity frameworks for ICS, incorporating advanced detection and prevention mechanisms (Andzulis et al., 2012).

In response to these evolving threats, researchers have developed various testbeds to simulate cyber-attacks on ICS and evaluate the effectiveness of different defense strategies. Testbeds provide a controlled environment in which researchers can replicate real-world conditions and observe how ICS components respond to cyber-attacks (Abid et al., 2024). Physical testbeds, which replicate the hardware and software components of actual ICS, allow for a detailed analysis of system behavior in response to cyber threats (Samtani et al., 2020). These testbeds are especially valuable for understanding how environmental factors, such as temperature and vibration, influence the operation of ICS components, including sensors and actuators (Le et al., 2024). However, physical testbeds are expensive to implement and maintain, limiting their use to large research institutions and organizations with significant resources (Guezzaz et al., 2021). Hybrid testbeds, which combine physical and virtual elements, offer a more cost-effective alternative by simulating certain components while maintaining the physical hardware necessary to study system dynamics (Elayni & Jemili, 2017).

The development of virtual testbeds has further expanded the capabilities of ICS cybersecurity research.

Figure 2: The architecture of virtualized testbeds



Source: Mylonas (2010)

Virtual testbeds, which simulate the entire ICS environment in software, are highly scalable and allow for the testing of complex attack scenarios that would be difficult or impossible to replicate in a physical environment (Alsharida et al., 2023). These testbeds enable researchers to model large-scale networks and explore how cyber-attacks propagate through interconnected systems (Paul & Wang, 2019). Virtual testbeds also reduce the cost of experimentation, making them accessible to a broader range of researchers and institutions. However, virtual testbeds are limited by their inability to fully replicate the physical dynamics of ICS, such as the effects of hardware malfunctions or environmental stressors (Essid & Jemili, 2016). Despite these limitations, virtual testbeds have become an integral tool in the cybersecurity research community, allowing for rapid prototyping and testing of cyber defense mechanisms.

The use of testbeds for ICS cybersecurity research has evolved alongside advancements in cyber-attack detection and prevention techniques. Early testbeds focused primarily on simulating network traffic and detecting anomalies that indicated potential cyber-attacks (Manzoor & Morgan, 2016). As the sophistication of cyber threats increased, testbeds began to incorporate machine learning algorithms and artificial intelligence to detect more complex attack patterns (Benaroch, 2018). Recent studies have explored the integration of testbeds with real-time monitoring systems, allowing for the dynamic adaptation of cybersecurity strategies in response to emerging threats (Gregor & Hevner, 2013). This evolution reflects the growing complexity of ICS cybersecurity, as researchers strive to develop more effective and efficient methods for protecting critical infrastructure from cyber-attacks. To address these challenges, researchers have employed various types of testbeds—physical, hybrid, and virtual—to simulate cyber-attacks and evaluate defense mechanisms. Physical testbeds offer a detailed analysis of real-world ICS operations but are costly and complex, while hybrid and virtual testbeds provide more affordable alternatives with different levels of accuracy in replicating system dynamics (Holgado et al., 2019). This study aims to examine and compare the effectiveness of these testbeds in mitigating cybersecurity risks in ICS, focusing on their evolution and application in research. By evaluating testbed

methodologies, this research seeks to highlight the trade-offs and benefits of each approach, contributing to the development of more effective cybersecurity strategies for ICS.

2 Literature Review

The evolution of cybersecurity risk mitigation in Industrial Control Systems (ICS) has been a critical area of research as these systems increasingly become connected to traditional IT networks, exposing them to cyber-attacks. Researchers have developed various approaches to simulate, analyze, and protect ICS from cyber threats, particularly through the use of testbeds. This section reviews the existing literature on physical, hybrid, and virtual testbeds, highlighting key studies that explore their effectiveness in cybersecurity research. Additionally, it examines the role of these testbeds in replicating real-world ICS environments and their impact on the development of detection and prevention mechanisms for cyber-attacks. The literature review synthesizes recent findings and evaluates the progress made in this field, providing a foundation for understanding the current state of cybersecurity in ICS.

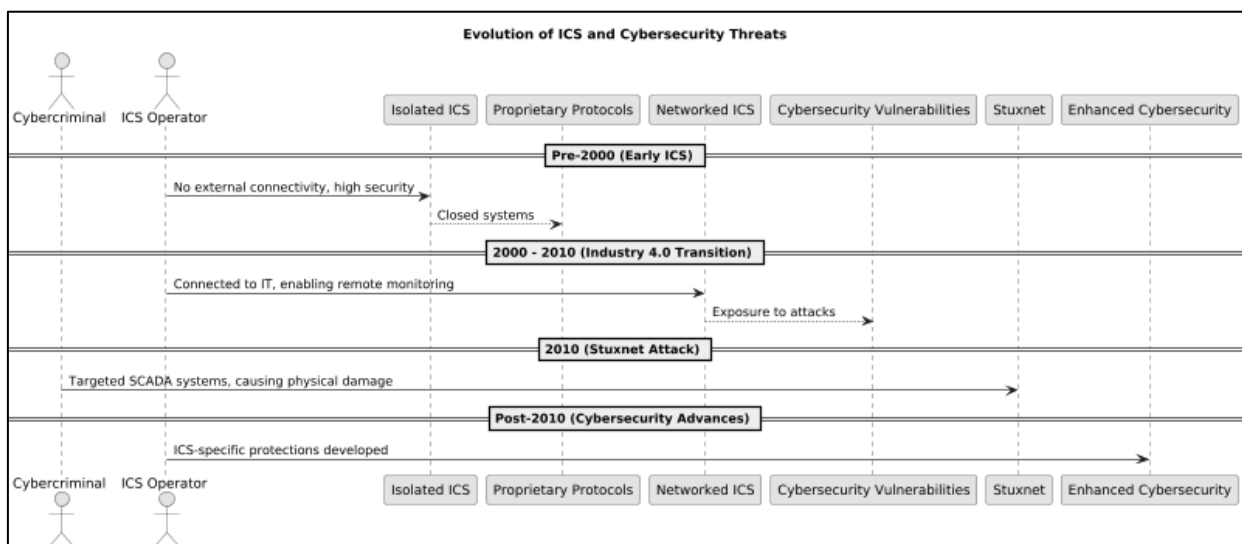
2.1 Evolution of ICS and Cybersecurity Threats

Industrial Control Systems (ICS) have traditionally been designed as isolated, standalone systems, intended for real-time control of industrial processes without external connectivity (Abraham & Chengalur-Smith, 2010). Early ICS systems, such as Supervisory Control

and Data Acquisition (SCADA) and Distributed Control Systems (DCS), operated in closed environments with proprietary protocols, ensuring a high level of security through physical isolation (Arendt & Scherr, 2016). The initial assumption was that, by keeping ICS separated from traditional IT systems, they would remain insulated from cybersecurity threats. However, with the advent of Industry 4.0 and the increasing need for remote monitoring, data analysis, and control, ICS have transitioned from these isolated setups to networked environments, interconnected with IT infrastructure (Benaroch, 2018). This shift enabled ICS to enhance operational efficiency and responsiveness but simultaneously introduced significant cybersecurity vulnerabilities as once-isolated systems became exposed to external networks and the internet.

The integration of IT networks into ICS has transformed their operational capabilities but also introduced complex cybersecurity challenges. By connecting ICS with corporate networks and external platforms, these systems became accessible to a broader range of users, but also more vulnerable to unauthorized access and cyber-attacks (Kamiya et al., 2021). Traditionally, IT security measures such as firewalls and antivirus software were not designed to protect ICS, as their unique protocols and real-time processing requirements demanded specialized security solutions (Guezzaz et al., 2021). The interconnection of ICS with IT infrastructure created a potential entry point for

Figure 3: Evolution of ICS and Cybersecurity Threats



cybercriminals and malicious actors, leading to an increased number of cybersecurity incidents targeting ICS environments (Bhatt, 2021). As ICS systems control critical infrastructures such as energy, water, and transportation, the stakes of securing these systems against cyber threats have become even higher, necessitating the development of specialized cybersecurity frameworks tailored to the unique needs of ICS (Alsharida et al., 2023; Shamim, 2022).

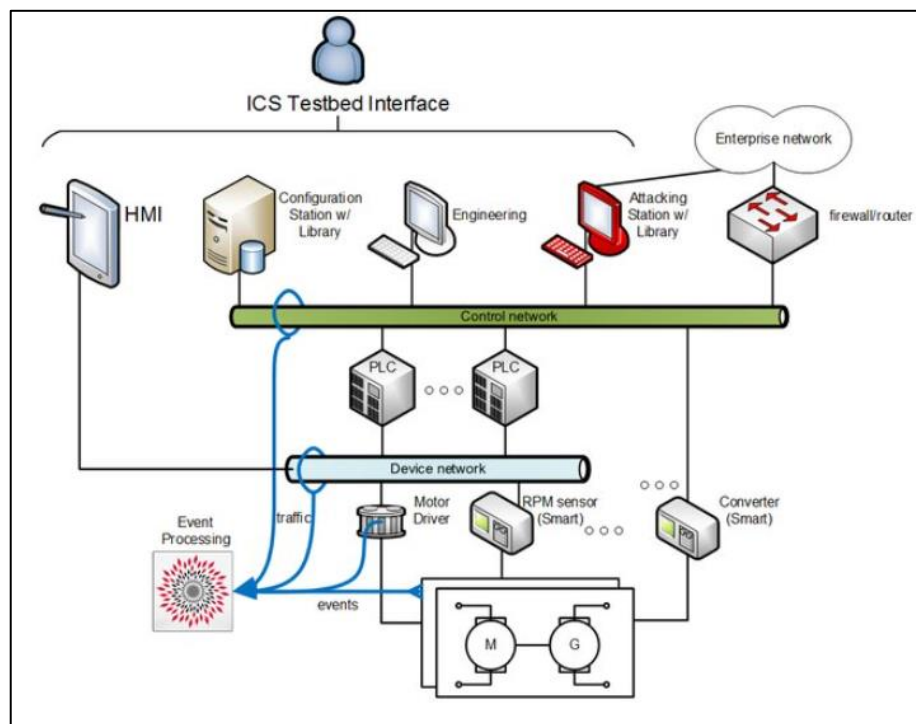
One of the most notable cybersecurity incidents in ICS history is the Stuxnet attack in 2010, which targeted Iran's nuclear centrifuges by exploiting vulnerabilities in SCADA systems (Essid & Jemili, 2016). This sophisticated cyber-attack marked a turning point in ICS cybersecurity, highlighting the potential for cyber-attacks to cause physical damage to critical infrastructure (Ebrahimi et al., 2020). Stuxnet was unique in that it specifically targeted ICS, using malware to manipulate industrial processes while remaining undetected by traditional security measures (Bhatt, 2021). The Stuxnet incident raised awareness of the severity of cybersecurity threats to ICS and catalyzed a wave of research aimed at improving ICS security (Dye, 2008). Following Stuxnet, researchers began developing more robust cybersecurity frameworks and detection systems tailored to the

specific needs of ICS, incorporating both traditional IT security measures and ICS-specific protections. Additionally, the incident underscored the importance of testbeds in cybersecurity research, as simulating such complex attacks in a controlled environment is essential for developing effective defense mechanisms (Bhatt, 2021).

2.2 Physical Testbeds

Physical testbeds are specialized environments that replicate the hardware and software components of Industrial Control Systems (ICS) in a real-world setup, designed to simulate and study cybersecurity threats in controlled settings (Kravchik & Shabtai, 2018). These testbeds typically include the actual ICS hardware such as sensors, actuators, and controllers, allowing researchers to observe system behavior and response to attacks in a tangible environment. Unlike virtual or hybrid testbeds, which rely partially or entirely on simulations, physical testbeds provide a direct representation of ICS dynamics, including interactions between hardware and software components (Njoku et al., 2005). The primary goal of a physical testbed is to replicate real-world operational conditions, making them ideal for testing how environmental factors like temperature, humidity, or device wear affect ICS

Figure 4: Cyber-Physical system testbed diagram



Source: Korkmaz (2019)

performance under cyber-attacks (Inoue et al., 2017). These characteristics make physical testbeds a vital tool in ICS cybersecurity research, as they provide the most realistic environment for studying the effects of cyber threats on critical infrastructure.

Several studies have utilized physical testbeds to evaluate ICS cybersecurity measures and develop new approaches to detecting and preventing cyber-attacks. For example, Al-Khateeb et al. (2023) implemented a physical testbed to simulate attacks on a water treatment plant, demonstrating the utility of these environments in studying both process-level and control-level cyber-attacks. Similarly, Liu et al. (2020) used a physical testbed to examine cyber-attack detection methods for ICS, focusing on the vulnerability of communication protocols between control systems and field devices. The work of Owfi and Afghah (2023) further expanded on these efforts by designing a physical testbed to evaluate intrusion response systems in ICS environments, demonstrating the applicability of physical testbeds for developing advanced security solutions. These studies have contributed significantly to the body of knowledge on ICS cybersecurity, offering practical insights into how physical testbeds can be used to replicate complex attack scenarios and test the efficacy of different defense mechanisms.

Physical testbeds offer several benefits in the realm of ICS cybersecurity research. One of the key advantages is their ability to accurately replicate real-world system dynamics, providing researchers with a tangible environment to observe how various hardware components respond to cyber-attacks (Chen et al., 2012). This level of detail allows for more accurate assessments of how cyber-attacks impact the physical performance of ICS, which is particularly valuable in critical infrastructure sectors like energy and water supply. Additionally, physical testbeds enable researchers to simulate environmental conditions such as temperature, noise, or mechanical wear, which may influence the behavior of ICS components during cyber-attacks (Al-Shaer et al., 2020). However, physical testbeds come with significant limitations. They are expensive to build and maintain, often requiring specialized hardware and facilities to replicate full-scale industrial systems (Hafsa & Jemili, 2018). Furthermore, due to their complexity, physical testbeds can be difficult to scale, limiting their applicability for testing

large, interconnected networks or highly complex attack scenarios (Alam, Farhad, et al., 2024).

Several case studies highlight the successful application of physical testbeds in real-world ICS cybersecurity research. In one such study, Rajić et al. (2016) developed a physical testbed to mimic the operations of a water treatment plant, where they simulated various attack scenarios to evaluate the performance of intrusion detection systems. Their findings revealed that physical testbeds could replicate complex attacks, such as insider threats and process tampering, providing valuable insights into potential defense mechanisms. Another case study by Owfi and Afghah (2023) involved the use of a physical testbed to test detection mechanisms for cyber-attacks targeting SCADA systems. The researchers demonstrated that the testbed allowed for precise measurements of the effects of communication delays and signal interference on ICS performance, leading to the development of more robust cybersecurity protocols. In a different study, Suthaharan (2014) employed a physical testbed to analyze the impact of cyber-attacks on energy distribution networks, showcasing how testbeds can be tailored to specific industries. These case studies underscore the importance of physical testbeds in cybersecurity research, particularly for replicating and mitigating real-world cyber threats in critical infrastructure environments.

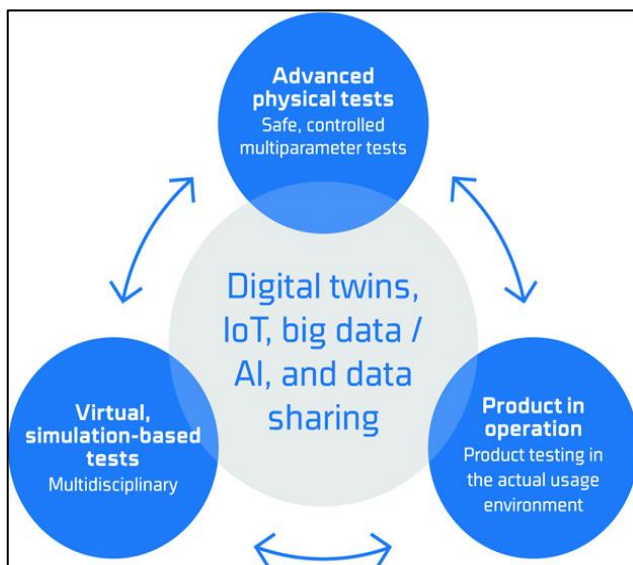
2.3 Hybrid Testbeds

Hybrid testbeds for Industrial Control Systems (ICS) combine both physical and virtual components, offering a flexible environment for cybersecurity research that balances realism and cost-effectiveness (Bosmans et al., 2018). These testbeds include real ICS hardware, such as programmable logic controllers (PLCs), sensors, and actuators, alongside virtualized elements that simulate other parts of the system, such as network traffic or additional control units (García-García et al., 2020). The goal of hybrid testbeds is to replicate key aspects of ICS operations while reducing the financial and logistical burdens of maintaining a fully physical testbed (de Matthaeis et al., 2018). By combining physical and virtual elements, hybrid testbeds offer researchers the ability to simulate cyber-attacks on a realistic system while also experimenting with large-scale or highly complex configurations that would be

difficult or costly to replicate in a purely physical environment (Zhang et al., 2019). This structure allows hybrid testbeds to provide a middle ground between the high fidelity of physical testbeds and the cost-efficiency of virtual ones.

Several studies have investigated the effectiveness of hybrid testbeds in ICS cybersecurity research, demonstrating their value in various contexts.

Figure 5: Hybrid test bed Overview



Source: Force Technology (2024)

One notable study by Das et al. (2020) explored the use of a hybrid testbed to analyze vulnerabilities in critical infrastructure, such as power grids and water treatment plants. This research highlighted the versatility of hybrid testbeds in replicating both physical processes and network communications, offering a comprehensive environment for testing cyber-attacks. Similarly, Spencer and Ulaby (2016) implemented a hybrid testbed to simulate cyber-physical attacks on a water treatment system, providing insights into the detection of malicious activity across both the physical and virtual layers of the system. Another study by Giri et al. (2010) examined the use of hybrid testbeds for detecting distributed denial-of-service (DDoS) attacks in ICS, showcasing how virtual elements can be used to simulate large-scale attacks while physical components replicate the real-world consequences of these attacks. These studies demonstrate the broad applicability of hybrid testbeds across different sectors, emphasizing their role in advancing ICS cybersecurity research.

Hybrid testbeds offer several advantages for ICS cybersecurity research, particularly in their ability to

combine realism with scalability and cost efficiency. One of the primary benefits is their flexibility; researchers can adjust the balance between physical and virtual components to suit the specific needs of their experiments, making hybrid testbeds adaptable to a wide range of research contexts (Chiew et al., 2018). Additionally, hybrid testbeds allow for the testing of complex cyber-attacks that may require large networks or numerous control systems, which would be impractical to replicate entirely in a physical environment (Talebi et al., 2014). Hybrid testbeds also provide more accurate results than purely virtual environments, as they incorporate real ICS hardware, allowing researchers to observe how physical components respond to cyber-attacks (Chiew et al., 2018). However, these testbeds also have limitations. While they are more cost-effective than fully physical testbeds, they still require significant investment in hardware, and the integration of physical and virtual elements can introduce complexities in the setup and maintenance of the testbed (Talebi et al., 2014). Additionally, hybrid testbeds may not capture all of the nuances of physical system behavior, especially in cases where environmental factors like temperature or vibration play a critical role (Chidukwani et al., 2022).

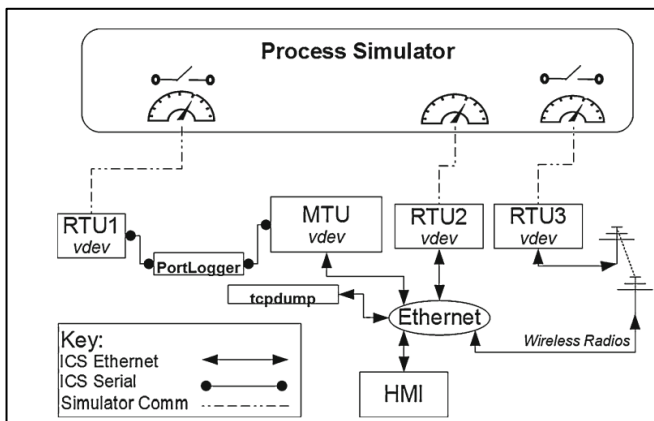
2.4 Virtual Testbeds

Virtual testbeds are software-based environments that simulate the operations of Industrial Control Systems (ICS), allowing researchers to conduct cybersecurity testing without the need for physical hardware (Spencer & Ulaby, 2016). These testbeds are particularly valued for their scalability, as they enable the simulation of large-scale networks and complex attack scenarios that would be impractical or cost-prohibitive to replicate in a physical or hybrid testbed (Akyildiz et al., 2008). Virtual testbeds can model ICS components such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), and communication networks in a fully simulated environment, making them highly flexible for testing various types of cyber-attacks (Giri et al., 2010). This scalability allows researchers to simulate wide-reaching cyber-attacks, such as distributed denial-of-service (DDoS) attacks or large-scale malware infections, across multiple ICS components simultaneously, providing valuable insights into how cyber-attacks propagate and affect interconnected industrial systems (Benzekki et al., 2016). As ICS become more interconnected, the

scalability of virtual testbeds has become an increasingly important feature for comprehensive cybersecurity testing.

Several studies have explored the use of virtual testbeds for simulating and analyzing cyber-attacks on ICS,

Figure 6: Open virtual testbed architecture



Source: Reaves and Morris (2012)

demonstrating the utility of these environments for cybersecurity research. For example, Wald (1999) used a virtual testbed to simulate DDoS attacks on ICS, examining how the attack impacted network traffic and control system functionality. Similarly, Alsaedi et al. (2023) implemented a virtual testbed to simulate attacks on smart grids, investigating the effectiveness of various detection methods in preventing cyber-attacks on energy distribution networks. Another study by Huang et al. (2017) employed a virtual testbed to simulate advanced persistent threats (APTs) targeting ICS, highlighting the testbed's ability to replicate sophisticated, long-term cyber-attacks. These studies have demonstrated the value of virtual testbeds in conducting detailed cybersecurity research, as they allow for the modeling of highly complex attack scenarios that can be adjusted and repeated with ease, offering a robust platform for testing different security strategies and responses (Benzekki et al., 2016).

One of the key advantages of virtual testbeds is their cost-efficiency. Unlike physical or hybrid testbeds, virtual environments do not require expensive hardware, making them significantly cheaper to implement and maintain (Alsaedi et al., 2023). Virtual testbeds are also highly flexible, allowing researchers to quickly modify system configurations or network setups without the need for hardware changes. This

flexibility is particularly beneficial for simulating a wide range of cyber-attacks and testing multiple cybersecurity strategies in a controlled and repeatable environment (Zhao et al., 2013). Moreover, virtual testbeds can be scaled up to simulate large, complex networks involving thousands of devices, making them ideal for testing cyber-attacks on critical infrastructure like power grids, water treatment plants, and transportation systems (Misra et al., 2009). Another benefit is that virtual testbeds allow for more frequent testing, enabling researchers to conduct multiple experiments in parallel or over extended periods without concerns about hardware degradation or failure (Anjum et al., 2021; Shamim, 2022). These features make virtual testbeds a highly practical and scalable tool for ICS cybersecurity research.

Despite their many benefits, virtual testbeds have significant limitations when it comes to accurately replicating the physical dynamics of ICS components. For example, physical testbeds can simulate real-world factors such as temperature fluctuations, mechanical wear, or signal interference, all of which can affect the performance of ICS devices like sensors, actuators, and control units (Hegazy & El-Aasser, 2021). Virtual testbeds, by contrast, are limited to software-based simulations that cannot fully capture these physical phenomena, leading to potential discrepancies between simulated and real-world outcomes (Samarasinghe & Mannan, 2021). This limitation can be particularly problematic when testing cyber-attacks that exploit vulnerabilities in physical hardware, such as hardware-based malware or attacks that target device communication protocols (Newton & Rouse, 1980). Additionally, the lack of physical components in virtual testbeds can make it difficult to evaluate how environmental factors influence the performance of ICS during a cyber-attack, which may result in an incomplete understanding of system vulnerabilities (Anjum et al., 2021). Consequently, while virtual testbeds offer significant advantages in terms of cost and scalability, they cannot entirely replace the need for physical or hybrid testbeds in cybersecurity research, particularly when studying attacks that target the physical aspects of ICS.

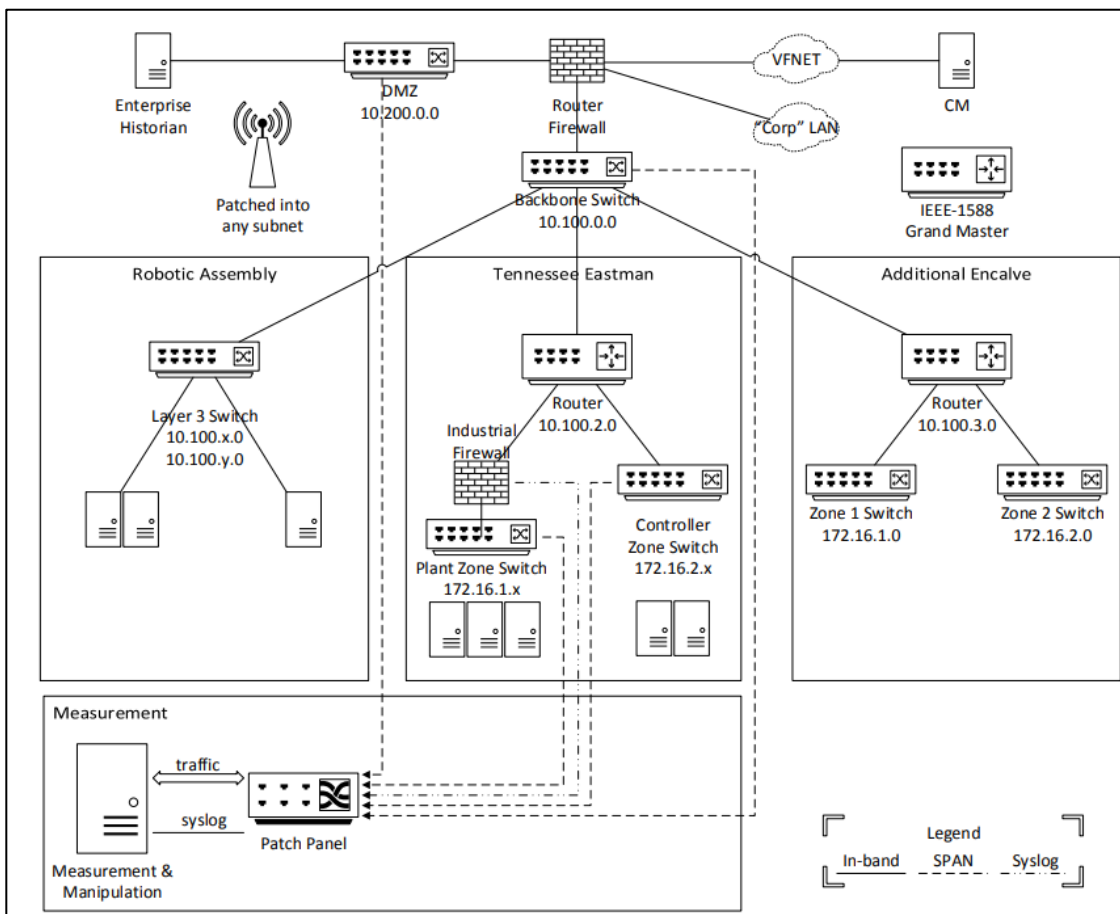
2.5 Testbed Design Approach for ICS Cybersecurity

The design of an Industrial Control System (ICS) cybersecurity testbed must encompass a wide range of scenarios to effectively replicate various industrial environments. Each scenario is designed to cover different aspects of industrial processes, from continuous process control to rapid discrete manufacturing. A commonly used scenario is the Tennessee Eastman process, which models continuous process control, as outlined by Zhou et al. (2013). This scenario provides a comprehensive representation of chemical processing industries, making it a valuable tool for evaluating ICS cybersecurity threats in continuous operations (Alam, Kurum, et al., 2024). Additionally, a robotic assembly scenario simulates dynamic, discrete manufacturing processes, where rapid and flexible system configurations are essential (Misra et al., 2009). An additional scenario, to be defined later, will focus on wide-area industrial networks (WANs), such as pipelines and railroads, utilizing safety-critical

Supervisory Control and Data Acquisition (SCADA) systems (Koosha & Mastronarde, 2023). Each of these scenarios will be logically separated into "enclaves" within the testbed, ensuring that individual simulations can be isolated while sharing the overall network architecture. This enclave-based design allows for a modular approach, with each enclave tailored to specific industrial sectors, enhancing the testbed's flexibility and effectiveness (Alam, Kurum, et al., 2024).

The testbed's network configuration is designed to mimic the complex and layered architecture of real-world ICS networks, with each enclave logically separated but connected through a central network. A Demilitarized Zone (DMZ) will be established to host critical enterprise services, such as the enterprise historian, which records and stores historical data accessible to both enterprise users and plant operators (Al-Khateeb et al., 2023). The DMZ ensures secure communication between operational technology (OT) and information technology (IT) networks, preventing

Figure 7: Testbed Network Design



Source: Candell et al. (2014)

unauthorized access to sensitive ICS systems while maintaining data flow across the network. This configuration mirrors common industry practices, where critical services are isolated from external threats while still being accessible for necessary operations (Hafsa & Jemili, 2018). A separate measurement enclave will be implemented to capture network traffic, log syslog messages, and manipulate traffic flows for cybersecurity testing. This enclave will allow researchers to simulate man-in-the-middle attacks, manipulate traffic through shaping techniques, and model both local and wide-area network dynamics (Chen et al., 2012; Nandi et al., 2024). Traffic capture will be facilitated using port mirroring, a widely adopted method for sending packets to the measurement enclave for offline analysis and attack detection (Goh et al., 2017).

The deployment of security devices across the testbed's network is critical for evaluating the resilience of ICS to cybersecurity threats. Firewalls will be configured with capabilities such as device authentication, encryption, and deep packet inspection, providing multiple layers of defense against cyber-attacks (Ramsdale et al., 2020). These security devices will be used to assess the system's ability to withstand different types of attacks, including man-in-the-middle, packet manipulation, and denial-of-service (DoS) attacks. By introducing varying levels of security throughout the network, the testbed can simulate a range of cybersecurity scenarios, from basic authentication failures to sophisticated encryption attacks (Ebrahimi et al., 2022). Additionally, the testbed will introduce network anomalies such as packet flight time uncertainty (e.g., delay and jitter) and packet loss to evaluate the performance impact of security measures on real-time ICS operations (Hoyhtya et al., 2017). This approach allows researchers to measure the trade-offs between security and system performance, providing critical insights into the effects of cybersecurity defenses on network determinism, safety, and stability (Pulliainen et al., 1993).

The testbed design incorporates a robust framework for collecting performance metrics related to security and network resilience. Statistical data, including latency, jitter, and packet loss, will be gathered to analyze how cybersecurity measures impact the reliability and safety of ICS operations (Korkmaz, 2019). By manipulating traffic flows and introducing security-related delays, the

testbed will measure the effects of different security protocols on system performance, providing valuable design guidance to manufacturers and system integrators (Lin, 2009). These metrics are essential for understanding how varying levels of security affect ICS stability, especially in time-sensitive applications like power grids and water treatment facilities (Song et al., 2002). The data collected will be analyzed to inform best practices for securing ICS networks without compromising their operational efficiency, offering a roadmap for developing resilient ICS architectures capable of withstanding emerging cyber threats (Lányi et al., 2021). This performance-based approach ensures that the testbed will not only simulate cyber-attacks but also provide actionable insights into the optimal balance between security and performance in industrial environments.

2.6 Application Scenarios for ICS Cybersecurity Testbed

In 2013, a road-mapping workshop sponsored by NIST brought together industry experts and academia to define priorities for cybersecurity testbeds in Industrial Control Systems (ICS). One of the key decisions was to focus on Internet Protocol (IP)-routable protocols, which are more prevalent in modern industrial environments, while also including traditional field-bus protocols like Controller Area Network (CAN) to ensure inclusiveness (Fekih & Jemili, 2019). Though IP-routable protocols are favored, the testbed includes both types to address a wider variety of industrial settings. Due to the impracticality of constructing a full-scale plant in a laboratory setting, simulation will be leveraged alongside hardware-in-the-loop (HIL) components, simulating the real-world interfaces between sensors, actuators, and controllers. This approach ensures that the testbed can accurately replicate real industrial processes while providing flexibility in terms of both simulation and physical (Tang et al., 2022).

The Tennessee Eastman (TE) model was selected as one of the primary scenarios for the ICS testbed due to its widespread use in control system research, complex dynamics, and real-world relevance. This process model is non-linear, features open-loop instability, and presents significant safety and operational risks, making it a suitable candidate for cybersecurity testing (Waters

et al., 2006). The TE process involves multiple stages, including a reactor, condenser, vapor-liquid separator, and stripper, each offering multiple points for potential cyber-attacks. The process must be tightly controlled to prevent the reactor from exceeding the safety threshold of 3000 kPa, a key security vulnerability. As noted by Schultz (2005), an attacker could target the reactor pressure through geometric or surge attacks, potentially compromising the safety and stability of the system. By simulating these attacks and other vulnerabilities, the testbed will offer researchers insight into the security weaknesses inherent in complex chemical processes like the TE model (Mohy-eddine et al., 2023).

A key feature of the ICS testbed is the use of Hardware-in-the-Loop (HIL) simulation, which allows for real-time testing of industrial processes with cybersecurity protections in place. The HIL simulator will replicate the TE process, enabling researchers to measure the impact of various security measures, such as deep packet inspection, device authentication, and packet manipulation, on process performance (Tang et al., 2022). The plant will be divided into several zones: the plant zone, control zone, and a demilitarized zone (DMZ). The controller, implemented in Simulink, will communicate with the plant process via industrial protocols such as DeviceNet and EtherNet/IP, while state data will be stored on an Open Platform Communications (OPC) server (Schultz, 2005). This setup allows for in-depth analysis of network performance and security, particularly when simulating common attack vectors such as human-machine interface (HMI) spoofing or denial-of-service (DoS) attacks. The testbed will also be reconfigurable, allowing researchers to introduce various network topologies and measure the performance impact of different security configurations (Khan & Mahmood, 2018).

In addition to the TE process, the testbed will incorporate other complex chemical processes, such as the production of Vinyl Acetate (VAC) monomer, a widely studied benchmark in chemical manufacturing. The VAC process, while similar to the TE model in terms of performance metrics, introduces additional layers of complexity with 246 dynamic states, 26 manipulated variables, and 23 polled measurements, compared to the TE process's 50 states and 12 manipulated variables (Nazir et al., 2017). The VAC process also features vapor-phase reactions with

significantly faster dynamics, requiring a 1-second sampling interval. This rapid data acquisition makes the process more sensitive to delays and synchronization issues in control loops, presenting additional challenges for cybersecurity testing (Krotofil & Cardenas, 2013). The inclusion of the VAC process in the testbed allows for more granular analysis of targeted control system vulnerabilities, particularly in environments where high-speed communication and real-time processing are critical to maintaining system stability.

2.7 Comparative Analysis of Testbed Types

When comparing physical, hybrid, and virtual testbeds for Industrial Control Systems (ICS) cybersecurity research, each testbed type offers distinct advantages and trade-offs in terms of effectiveness, cost, and realism. Physical testbeds provide the most realistic simulation of ICS environments, allowing researchers to observe how actual hardware and environmental conditions impact system performance under cyber-attacks (Song et al., 2002). This level of fidelity makes physical testbeds highly effective for identifying vulnerabilities related to physical components, such as sensors, actuators, and communication protocols. However, they are also the most expensive to implement and maintain due to the need for specialized hardware and infrastructure (Luo & Zhang, 2008). In contrast, virtual testbeds are highly cost-efficient and scalable, as they rely on software simulations that can replicate large-scale ICS networks without the need for physical equipment (Lányi et al., 2021). While virtual testbeds are effective for simulating network-level attacks and testing cybersecurity strategies at scale, they lack the realism needed to fully replicate physical system dynamics (Mohy-eddine et al., 2023). Hybrid testbeds, which combine physical and virtual components, offer a middle ground by providing some degree of realism while keeping costs lower than fully physical setups (Luo & Zhang, 2008). These testbeds are effective in simulating both physical and network-related vulnerabilities, making them a versatile option for cybersecurity research (Mohy-eddine et al., 2023). The choice of the appropriate testbed for ICS cybersecurity research depends on several key factors, including the specific research objectives, the types of cyber-attacks being simulated, and the available budget. Researchers studying physical vulnerabilities in ICS, such as attacks targeting sensors, actuators, or communication protocols, may benefit most from

physical or hybrid testbeds due to their ability to replicate real-world operational conditions (Ampel & Chen, 2021). For instance, studies that focus on the effects of environmental factors, such as temperature, mechanical wear, or electromagnetic interference, require the fidelity that only physical components can provide (Konyeha, 2020). On the other hand, researchers interested in testing large-scale cyber-attacks, such as distributed denial-of-service (DDoS) attacks or malware propagation across extensive networks, may find virtual testbeds to be the most suitable option due to their scalability and cost-efficiency (Bumb et al., 2018). Hybrid testbeds offer a compromise between these two approaches, making them ideal for research that requires both physical accuracy and the ability to simulate broader network-level attacks (Benjamin et al., 2016). Ultimately, the decision should be guided by the balance between the need for realism, the complexity of the attack scenarios being tested, and the available resources.

Each testbed type presents trade-offs between accuracy, cost, and scalability, which researchers must carefully consider when designing their cybersecurity experiments. Physical testbeds offer the highest level of

accuracy and realism, as they replicate real-world ICS operations and allow for the detailed study of physical component vulnerabilities (Yazar & Arslan, 2018). However, their high cost and limited scalability make them less practical for testing large-scale or complex attack scenarios (Bumb et al., 2018). In contrast, virtual testbeds provide a highly scalable and cost-effective solution, enabling researchers to simulate extensive networks and conduct multiple experiments simultaneously without the need for physical hardware (Dawson, 2024). The trade-off, however, is a lack of physical realism, as virtual testbeds cannot replicate the full range of environmental factors and physical system behaviors that may influence cybersecurity outcomes (Ampel et al., 2024). Hybrid testbeds attempt to balance these competing priorities by incorporating both physical and virtual elements, offering a moderate level of realism at a reduced cost compared to fully physical setups (Sen et al., 2020). While hybrid testbeds are versatile and effective for a wide range of research objectives, they still face limitations in replicating large-scale network effects or providing the same level of physical accuracy as dedicated physical testbeds (Douiba et al., 2022).

Table 1: ICS Testbed Comparison

Testbed Type	Advantages	Disadvantages	Best Suited For	Trade-offs
<i>Physical Testbeds</i>	High realism and fidelity; allows observation of actual hardware under cyber-attacks. Ideal for testing physical vulnerabilities.	Expensive to implement and maintain. Limited scalability due to reliance on physical hardware.	Studies focused on physical vulnerabilities like sensors, actuators, and environmental effects.	High accuracy and realism, but low scalability and high cost.
<i>Virtual Testbeds</i>	Highly cost-efficient and scalable. Suitable for large-scale cyber-attacks like DDoS. Allows multiple experiments without physical hardware.	Lacks physical realism. Cannot fully replicate environmental factors or physical system dynamics.	Large-scale network attack simulations, such as malware propagation and DDoS attacks.	High scalability and cost-efficiency, but lacks physical fidelity.
<i>Hybrid Testbeds</i>	Provides a balance of realism and scalability. Effective for simulating both physical and network vulnerabilities.	Moderate cost and realism, but lacks full physical accuracy. Limited in replicating large-scale network effects.	Research requiring a combination of physical accuracy and network-level simulations.	Moderate realism and cost, but does not fully replicate physical accuracy or large-scale networks.

3 Method

This study adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a systematic, transparent, and rigorous review process. The methodology followed several key stages, outlined below.

3.1 Identification of Studies

The first step in the process involved identifying relevant studies through a systematic search of major academic databases, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. The search was conducted using terms such as “Industrial Control Systems (ICS) cybersecurity,” “testbeds,” “physical testbeds,” “hybrid testbeds,” “virtual testbeds,” and “cyber-attack simulations.” To ensure the inclusion of the most recent advancements in ICS cybersecurity, only studies published between 2000 and 2024 were considered. A total of 145 articles were retrieved through this search. Non-peer-reviewed articles and those written in languages other than English were excluded from the study. Each identified article was assigned a unique number to facilitate tracking throughout the review process.

3.2 Screening of Articles

The screening process involved two phases. In the first phase, the titles and abstracts of all 145 articles were reviewed to determine their relevance to the research focus on ICS cybersecurity testbeds. As a result, 89 articles that did not meet the criteria of addressing ICS or testbed implementation were excluded. In the second phase, full-text screening was conducted for the remaining 56 articles to ensure that they provided empirical analysis or detailed methodologies relevant to ICS cybersecurity. At this stage, 21 articles were excluded due to insufficient detail or a lack of focus on cybersecurity within ICS environments, leaving 35 articles for detailed analysis.

3.3 Eligibility Criteria

To further refine the selection, the PRISMA eligibility criteria were strictly applied. Articles were included if they specifically focused on ICS cybersecurity and addressed the design, implementation, or evaluation of physical, hybrid, or virtual testbeds. Additionally, studies had to provide empirical data or detailed testbed architectures. Conversely, articles were excluded if they

lacked a focus on ICS, were purely theoretical without empirical evidence, or did not address cybersecurity implementations relevant to ICS.

3.4 Final Selection of Articles

After applying the eligibility criteria, a total of 35 articles were finalized for inclusion in the study. These articles form the foundation for the comparative analysis of physical, hybrid, and virtual testbeds in ICS cybersecurity research. The selected studies were used to explore the effectiveness, scalability, and cost efficiency of the different testbed types and to assess their role in simulating various cybersecurity scenarios in ICS environments.

4 Findings

The systematic review of the literature on Industrial Control Systems (ICS) cybersecurity testbeds revealed several key findings across physical, hybrid, and virtual testbed implementations. One significant finding is that physical testbeds provide the most realistic environment for studying ICS cybersecurity, particularly when it comes to simulating real-world operational conditions. These testbeds allow researchers to directly observe how physical components like sensors, actuators, and programmable logic controllers (PLCs) respond to various types of cyber-attacks. Physical testbeds are particularly valuable for testing the effects of attacks that exploit hardware vulnerabilities or environmental factors, such as temperature fluctuations or mechanical wear. However, their high cost and complexity limit their scalability and accessibility, making them less practical for studies requiring large-scale network simulations or extensive testing scenarios.

Hybrid testbeds emerged as a flexible and cost-effective alternative to physical testbeds. By combining both physical and virtual elements, hybrid testbeds offer a middle ground between realism and scalability. These testbeds allow researchers to simulate physical processes and incorporate real hardware components where necessary, while also leveraging virtual simulations for network-level testing. This dual approach enables hybrid testbeds to handle complex cyber-attack scenarios without the full expense of a purely physical setup. Hybrid testbeds are also highly adaptable, allowing researchers to modify both the physical and virtual components to suit a wide range of industrial applications. However, while they are more

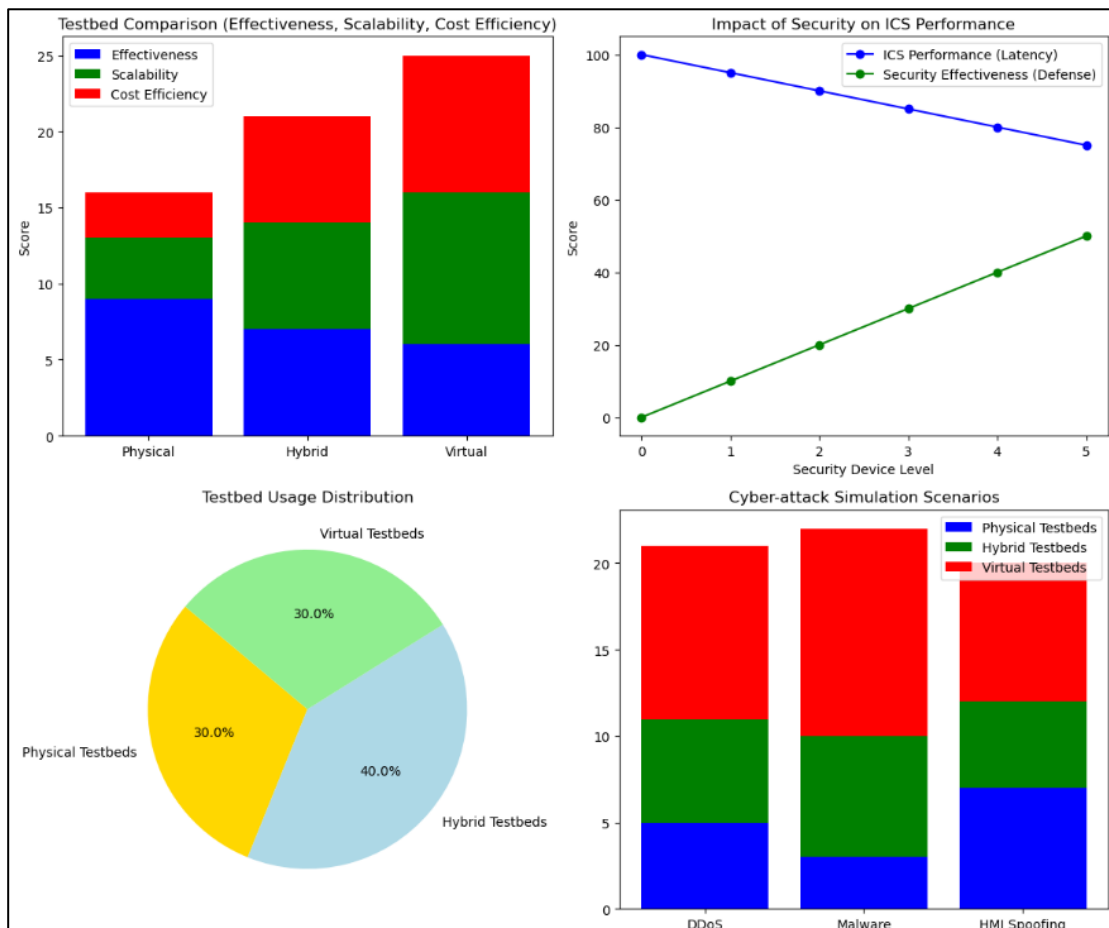
scalable than physical testbeds, hybrid testbeds still do not capture the full range of environmental dynamics that can affect ICS performance.

Virtual testbeds, on the other hand, offer the greatest scalability and cost-efficiency. By using software-based simulations to replicate ICS environments, virtual testbeds allow researchers to model extensive networks and test a variety of cyber-attack scenarios at a relatively low cost. Virtual testbeds are particularly well-suited for simulating large-scale network attacks, such as distributed denial-of-service (DDoS) attacks, that would be difficult or impractical to replicate in a physical or hybrid testbed. Additionally, virtual testbeds allow for rapid prototyping and testing of cybersecurity strategies, enabling researchers to run multiple experiments simultaneously or conduct long-term studies without the risk of hardware failure. However, the primary limitation of virtual testbeds is their inability to replicate physical system dynamics accurately, which can lead to discrepancies between simulated and real-world outcomes.

The review also highlighted the importance of network architecture and security device placement in testbed design. Across all testbed types, the inclusion of firewalls, intrusion detection systems (IDS), and encryption protocols proved crucial in simulating realistic cybersecurity environments. These security devices allowed researchers to measure how different levels of network security affected ICS performance under cyber-attack conditions. In many cases, the introduction of security devices increased system latency and caused slight performance degradation, but these effects were generally outweighed by the benefits of improved security. Additionally, the placement of security devices within the testbed network architecture influenced the effectiveness of cybersecurity measures, with more strategically placed devices yielding better defense against attacks.

One of the significant findings concerning cybersecurity vulnerabilities in ICS was related to human-machine interface (HMI) spoofing attacks and their potential impact on system stability. The testbed

Figure 8: Summary of the Findings



simulations showed that HMI spoofing could lead to dangerous outcomes by manipulating operator inputs, causing incorrect system commands to be executed. In several studies, testbeds successfully simulated these types of attacks, revealing that security mechanisms like device authentication and user verification are essential for protecting against such vulnerabilities. The ability to simulate these sophisticated attack vectors demonstrated the value of testbeds in identifying specific security weaknesses and testing targeted defense strategies. In addition, the findings showed that testbed-based research is essential for advancing the field of ICS cybersecurity, as it provides a controlled environment for testing and validating new security solutions. The flexibility of hybrid and virtual testbeds allows researchers to stay ahead of evolving cyber threats by quickly adapting to new attack vectors and developing corresponding defense mechanisms. Physical testbeds, while limited in scalability, remain critical for understanding the physical effects of cyber-attacks on industrial processes. Together, these testbed approaches provide a comprehensive framework for addressing the diverse challenges of ICS cybersecurity, ensuring that both operational technology (OT) and information technology (IT) systems can be protected from cyber threats.

5 Discussion

The findings of this systematic review highlight the critical role of testbeds in advancing cybersecurity research for Industrial Control Systems (ICS), particularly in the context of physical, hybrid, and virtual testbeds. One of the most significant insights from this study is the clear advantage physical testbeds offer in simulating real-world conditions. This aligns with earlier studies, such as those by Renaud (2016), who emphasized the importance of physical testbeds for replicating the actual dynamics of ICS hardware and its responses to cyber-attacks. However, our review also underscores the significant limitations in cost and scalability associated with physical testbeds, a challenge similarly noted by Sen et al. (2020). Despite these limitations, physical testbeds remain indispensable for understanding the physical vulnerabilities of ICS, especially in sectors where hardware failure due to cyber-attacks could have catastrophic consequences, such as energy and water

systems.

Hybrid testbeds, as revealed in this review, provide a balance between the realism of physical testbeds and the scalability of virtual environments. This finding is consistent with the earlier work of Douiba et al. (2022), who demonstrated that hybrid testbeds allow for flexibility in cybersecurity testing, enabling the use of real hardware where necessary while simulating broader network dynamics virtually. The adaptability of hybrid testbeds to different industrial settings was a recurring theme in the literature. Previous studies, such as those by Cretu and Brodie (2007), also highlighted the effectiveness of hybrid testbeds in evaluating both physical and network-level vulnerabilities. Our findings extend this understanding by showing that hybrid testbeds are particularly useful in testing complex attack vectors across both physical devices and virtual networks, which would be cost-prohibitive or technically unfeasible in a purely physical environment. However, the limitations in capturing certain environmental dynamics, such as temperature fluctuations or mechanical wear, remain a shortcoming, reinforcing the need for targeted use of physical components in critical areas.

The scalability and cost-effectiveness of virtual testbeds were among the most significant advantages found in this review, corroborating earlier studies such as those by Dawson (2024), who advocated for the use of virtual testbeds in simulating large-scale cyber-attacks, particularly distributed denial-of-service (DDoS) attacks. Virtual testbeds offer a low-cost alternative for simulating complex network configurations and conducting long-term studies without the risk of hardware degradation, as noted by Inoue et al. (2017). Our findings further support this view, demonstrating that virtual testbeds are highly effective for rapid prototyping of cybersecurity measures and for conducting repeated experiments across various simulated environments. However, the limitations of virtual testbeds in replicating the physical dynamics of ICS hardware were also emphasized, aligning with earlier critiques by Jarjoui and Murimi (2021), who pointed out that purely software-based simulations could overlook critical physical vulnerabilities, such as those arising from hardware degradation or environmental factors.

The review also highlighted the importance of network architecture and the strategic placement of security

devices, such as firewalls and intrusion detection systems (IDS), in testbed design. These findings are consistent with previous research by Alharbi et al. (2021), who demonstrated that the placement of security devices within the network plays a crucial role in determining the overall resilience of ICS against cyber-attacks. Our review further expands on these insights by showing that while the introduction of security mechanisms can introduce latency and minor performance degradation, the overall benefits of improved system protection outweigh these drawbacks. This finding is particularly relevant in industries where maintaining system integrity is paramount, and it underscores the need for further research into optimizing the trade-offs between security and performance in ICS networks, as suggested by previous studies like those by Ampel et al. (2024).

Finally, the ability of testbeds to simulate sophisticated attack vectors, such as human-machine interface (HMI) spoofing, and their impact on ICS operations was a crucial finding. Tan et al. (2018) discussed how these types of attacks pose significant risks to the safety and stability of industrial processes, and our review confirms that testbeds provide a valuable platform for testing the efficacy of defense mechanisms against these attacks. By simulating such vulnerabilities, testbeds enable researchers to develop targeted security solutions that can be implemented in real-world systems. This capability supports the growing body of research emphasizing the need for a proactive approach to ICS cybersecurity, as highlighted by Jarjoui and Murimi (2021). Testbed-based research, therefore, continues to be instrumental in identifying specific cybersecurity risks and developing mitigation strategies that are both practical and effective in industrial environments.

6 Conclusion

This systematic review highlights the critical role that testbeds—whether physical, hybrid, or virtual—play in advancing cybersecurity research for Industrial Control Systems (ICS). Each testbed type offers distinct advantages and trade-offs, with physical testbeds providing unmatched realism in replicating real-world operational conditions but being limited by high costs and complexity. Hybrid testbeds, offering a flexible

balance between physical accuracy and virtual scalability, demonstrate the ability to simulate both hardware vulnerabilities and network-level attacks, though they still face limitations in capturing full environmental dynamics. Virtual testbeds, while highly scalable and cost-effective, are most effective for large-scale network simulations but lack the ability to accurately replicate the physical behavior of ICS components. The findings reinforce the importance of choosing the appropriate testbed based on the specific cybersecurity research objectives, whether for testing system vulnerabilities, network security configurations, or defense mechanisms against complex cyber-attacks. As cyber threats continue to evolve, the strategic use of testbeds will be instrumental in ensuring the resilience and security of ICS across critical infrastructure sectors. Continued advancements in testbed technology and design will be crucial to meeting the growing demands of ICS cybersecurity in increasingly interconnected industrial environments.

References

- Abid, A., Jemili, F., & Korbaa, O. (2024). Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. *Cluster Computing*, 27(2), 2217-2238. <https://doi.org/10.1007/s10586-023-04087-7>
- Abraham, S., & Chengalur-Smith, I. N. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196. <https://doi.org/10.1016/j.techsoc.2010.07.001>
- Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., & Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4), 40-48. <https://doi.org/10.1109/mcom.2008.4481339>
- Al-Khateeb, M., Al-Mousa, M. R., Al-Sherideh, A. a. S., Almajali, D., Asassfeha, M., & Khafajeh, H. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. *International Journal of Data and Network Science*, 7(2), 791-800. <https://doi.org/10.5267/j.ijdns.2023.1.010>
- Al-Shaer, R., Spring, J. M., & Christou, E. (2020). CNS - Learning the Associations of MITRE ATT & CK Adversarial Techniques. *2020 IEEE Conference on Communications and Network Security (CNS)*, NA(NA), 1-9. <https://doi.org/10.1109/cns48642.2020.9162207>

- Alam, A. M., Farhad, M. M., Kurum, M., & Gurbuz, A. (2024). An Advanced Testbed for Passive/Active Coexistence Research: A Comprehensive Framework for RFI Detection, Mitigation, and Calibration. *2024 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM)*, NA(NA), 280-280. <https://doi.org/10.23919/usnc-ursinrsm60317.2024.10464436>
- Alam, A. M., Kurum, M., Ogut, M., & Gurbuz, A. C. (2024). Microwave Radiometer Calibration Using Deep Learning With Reduced Reference Information and 2-D Spectral Features. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 17(NA), 748-765. <https://doi.org/10.1109/jstars.2023.3333268>
- Alharbi, F., Alsulami, M. H., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. *Sensors (Basel, Switzerland)*, 21(20), 6901-NA. <https://doi.org/10.3390/s21206901>
- Alsaedi, W. K., Ahmadi, H., Khan, Z., & Grace, D. (2023). Spectrum Options and Allocations for 6G: A Regulatory and Standardization Review. *IEEE Open Journal of the Communications Society*, 4(NA), 1787-1812. <https://doi.org/10.1109/ojcoms.2023.3301630>
- Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73(NA), 102258-102258. <https://doi.org/10.1016/j.techsoc.2023.102258>
- Ampel, B., & Chen, H. (2021). Distilling Contextual Embeddings Into A Static Word Embedding For Improving Hacker Forum Analytics. *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, NA(NA), 1-3. <https://doi.org/10.1109/isi53945.2021.9624848>
- Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Nunamaker, J. F. (2024). Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach. *Journal of Management Information Systems*, 41(1), 236-265. <https://doi.org/10.1080/07421222.2023.2301178>
- Andzulis, J. M., Panagopoulos, N. G., & Rapp, A. (2012). A Review of Social Media and Implications for the Sales Process. *Journal of Personal Selling & Sales Management*, 32(3), 305-316. <https://doi.org/10.2753/pss0885-3134320302>
- Anjum, N., Latif, Z., Lee, C., Shoukat, I. A., & Iqbal, U. (2021). MIND: A Multi-Source Data Fusion Scheme for Intrusion Detection in Networks. *Sensors (Basel, Switzerland)*, 21(14), 4941-NA. <https://doi.org/10.3390/s21144941>
- Arendt, F., & Scherr, S. (2016). Optimizing Online Suicide Prevention: A Search Engine-Based Tailored Approach. *Health communication*, 32(11), 1403-1408. <https://doi.org/10.1080/10410236.2016.1224451>
- Benaroch, M. (2018). Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making. *Information Systems Research*, 29(2), 315-340. <https://doi.org/10.1287/isre.2017.0714>
- Benjamin, V., Zhang, B., Nunamaker, J. F., & Chen, H. (2016). Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities. *Journal of Management Information Systems*, 33(2), 482-510. <https://doi.org/10.1080/07421222.2016.1205918>
- Benzekki, K., Fergougui, A. E., & Elalaoui, A. E. (2016). Software-defined networking (SDN): a survey. *Security and Communication Networks*, 9(18), 5803-5833. <https://doi.org/10.1002/sec.1737>
- Bhatt, H. R. (2021). Website Vulnerabilities Attacks and Negative Impacts. *International Journal of Advanced Research in Science, Communication and Technology*, NA(NA), 104-108. <https://doi.org/10.48175/ijarct-v2-i3-318>
- Bosmans, S., Mercelis, S., Denil, J., & Hellinckx, P. (2018). Testing IoT systems using a hybrid simulation based testing approach. *Computing*, 101(7), 857-872. <https://doi.org/10.1007/s00607-018-0650-5>
- Bumb, A., Iancu, B., & Cebuc, E. (2018). Extending Cooja simulator with real weather and soil data. *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, NA(NA), NA-NA. <https://doi.org/10.1109/roedunet.2018.8514130>
- Candell, R., Stouffer, K., & Anand, D. (2014). A cybersecurity testbed for industrial control systems. *Proceedings of the 2014 Process Control and Safety Symposium*,
- Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS Quarterly*, 36(4), 1165-1188. <https://doi.org/10.2307/41703503>
- Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, 10(NA), 85701-85719. <https://doi.org/10.1109/access.2022.3197899>
- Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with*

- Applications*, 106(NA), 1-20. <https://doi.org/10.1016/j.eswa.2018.03.050>
- Cretu, A. E., & Brodie, R. J. (2007). The influence of brand image and company reputation where manufacturers market to small firms: A customer value perspective. *Industrial Marketing Management*, 36(2), 230-240. <https://doi.org/10.1016/j.indmarman.2005.08.013>
- Das, T., Sridharan, V., & Gurusamy, M. (2020). A Survey on Controller Placement in SDN. *IEEE Communications Surveys & Tutorials*, 22(1), 472-503. <https://doi.org/10.1109/comst.2019.2935453>
- Dawson, M. (2024, 2024/). Integrating Intelligence Paradigms into Cyber Security Curriculum for Advanced Threat Mitigation. ITNG 2024: 21st International Conference on Information Technology-New Generations, Cham.
- de Mattheais, P., Oliva, R., Soldo, Y., & Cruz-Pol, S. (2018). Spectrum Management and Its Importance for Microwave Remote Sensing [Technical Committees]. *IEEE Geoscience and Remote Sensing Magazine*, 6(2), 17-25. <https://doi.org/10.1109/mgrs.2018.2832057>
- Douiba, M., Benkirane, S., Guezzaz, A., & Azrou, M. (2022). An improved anomaly detection model for IoT security using decision tree and gradient boosting. *The Journal of Supercomputing*, 79(3), 3392-3411. <https://doi.org/10.1007/s11227-022-04783-y>
- Dye, K. (2008). SEO Attack: Website abuse for search engine optimisation. *Network Security*, 2008(3), 4-6. [https://doi.org/10.1016/s1353-4858\(08\)70028-x](https://doi.org/10.1016/s1353-4858(08)70028-x)
- Ebrahimi, M., Chai, Y., Samtani, S., & Chen, H. (2022). Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning. *MIS Quarterly*, 46(2), 1209-1226. <https://doi.org/10.25300/misq/2022/16618>
- Ebrahimi, M., Nunamaker, J. F., & Chen, H. (2020). Semi-Supervised Cyber Threat Identification in Dark Net Markets: A Transductive and Deep Learning Approach. *Journal of Management Information Systems*, 37(3), 694-722. <https://doi.org/10.1080/07421222.2020.1790186>
- Elayni, M., & Jemili, F. (2017). Using MongoDB Databases for Training and Combining Intrusion Detection Datasets. In (Vol. NA, pp. 17-29). https://doi.org/10.1007/978-3-319-62048-0_2
- Essid, M., & Jemili, F. (2016). SMC - Combining intrusion detection datasets using MapReduce. *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, NA(NA), 004724-004728. <https://doi.org/10.1109/smc.2016.7844977>
- Fekih, R. B., & Jemili, F. (2019). Distributed Architecture of an Intrusion Detection System Based on Cloud Computing and Big Data Techniques. In (Vol. NA, pp. 192-201). https://doi.org/10.1007/978-3-030-21005-2_19
- García-García, J. A., Enríquez, J. G., Ruiz, M., Arévalo, C., & Jiménez-Ramírez, A. (2020). Software Process Simulation Modeling: Systematic literature review. *Computer Standards & Interfaces*, 70(NA), 103425-NA. <https://doi.org/10.1016/j.csi.2020.103425>
- Giri, C., Ochieng, E., Tieszen, L. L., Zhu, Z., Singh, A., Loveland, T. R., Masek, J. G., & Duke, N. (2010). Status and distribution of mangrove forests of the world using earth observation satellite data. *Global Ecology and Biogeography*, 20(1), 154-159. <https://doi.org/10.1111/j.1466-8238.2010.00584.x>
- Goh, J., Adepu, S., Junejo, K. N., & Mathur, A. P. (2017). CRITIS - A Dataset to Support Research in the Design of Secure Water Treatment Systems. In (Vol. NA, pp. 88-99). https://doi.org/10.1007/978-3-319-71368-7_8
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337-356. <https://doi.org/10.25300/misq/2013/37.2.01>
- Guezzaz, A., Benkirane, S., Azrou, M., & Khurram, S. (2021). A Reliable Network Intrusion Detection Approach Using Decision Tree with Enhanced Data Quality. *Security and Communication Networks*, 2021(NA), 1-8. <https://doi.org/10.1155/2021/1230593>
- Haag, S., Siponen, M. T., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 52(2), 25-67. <https://doi.org/10.1145/3462766.3462770>
- Hafsa, M., & Jemili, F. (2018). Comparative Study between Big Data Analysis Techniques in Intrusion Detection. *Big Data and Cognitive Computing*, 3(1), 1-NA. <https://doi.org/10.3390/bdcc3010001>
- Hassan, A. A., Selim Reza, M., Ghosh, A., Lal Dey, N., Shamim Reza, M., Shahjalal, M., Kashem Mohammad Yahia, A., Mahfuz Hossain, M., Shameem Ahsan, M., Farad Ahmmed, M., & Alrafai, H. A. (2024). A thorough investigation of HTL layers to develop and simulate AgCdF3-based perovskite solar cells. *Materials Science and Engineering: B*, 310, 117744. <https://doi.org/10.1016/j.mseb.2024.117744>
- Hegazy, A., & El-Aasser, M. (2021). Network Security Challenges and Countermeasures in SDN Environments. *2021 Eighth International*

- Conference on Software Defined Systems (SDS), NA(NA), NA-NA.*
<https://doi.org/10.1109/sds54264.2021.9732104>
- Hoyhtya, M., Mammela, A., Chen, X., Hulkkonen, A., Janhunen, J., Dunat, J.-C., & Gardey, J. (2017). Database-Assisted Spectrum Sharing in Satellite Communications: A Survey. *IEEE Access*, 5(99), 25322-25341.
<https://doi.org/10.1109/access.2017.2771300>
- Huang, T., Yu, F. R., Zhang, C., Liu, J., Jiao, Z., & Liu, Y. (2017). A Survey on Large-Scale Software Defined Networking (SDN) Testbeds: Approaches and Challenges. *IEEE Communications Surveys & Tutorials*, 19(2), 891-917.
<https://doi.org/10.1109/comst.2016.2630047>
- Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., & Sun, J. (2017). ICDM Workshops - Anomaly Detection for a Water Treatment System Using Unsupervised Machine Learning. *2017 IEEE International Conference on Data Mining Workshops (ICDMW), NA(NA), 1058-1065.*
<https://doi.org/10.1109/icdmw.2017.149>
- Jarjoui, S., & Murimi, R. (2021). A Framework for Enterprise Cybersecurity Risk Management. In (Vol. NA, pp. 139-161). https://doi.org/10.1007/978-3-030-71381-2_8
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719-749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- Khan, M. N. A., & Mahmood, A. (2018). A distinctive approach to obtain higher page rank through search engine optimization. *Sādhanā*, 43(3), 43-NA. <https://doi.org/10.1007/s12046-018-0812-3>
- Konyeha, S. (2020). Exploring Cybersecurity Threats in Digital Marketing. *NIPES Journal of Science and Technology Research*, 2(3), 12-NA. <https://doi.org/10.37933/nipes/2.3.2020.2>
- Koosha, M., & Mastronarde, N. (2023). Minimizing Estimation Error Variance Using a Weighted Sum of Samples from the Soil Moisture Active Passive (SMAP) Satellite. *IGARSS 2023 - 2023 IEEE International Geoscience and Remote Sensing Symposium, NA(NA), 772-775.*
<https://doi.org/10.1109/igarss52108.2023.10281671>
- Korkmaz, E. (2019). *A Cyber-Security System for An Industrial Power Generation Facility* (Publication Number 27665480) [Ph.D., State University of New York at Binghamton]. ProQuest Dissertations & Theses Global. United States -- New York.
- Kravchik, M., & Shabtai, A. (2018). CPS-SPC@CCS - Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, NA(NA), 72-83.* <https://doi.org/10.1145/3264888.3264896>
- Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, 2015(3), 5-7. [https://doi.org/10.1016/s1361-3723\(15\)30017-8](https://doi.org/10.1016/s1361-3723(15)30017-8)
- Lányi, B., Hornyák, M., & Kruzslisz, F. (2021). The effect of online activity on SMEs' competitiveness. *Competitiveness Review: An International Business Journal*, 31(3), 477-496. <https://doi.org/10.1108/cr-01-2020-0022>
- Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, 76, 102470-102470. <https://doi.org/10.1016/j.techsoc.2024.102470>
- Lin, J.-L. (2009). Detection of cloaked web spam by using tag-based methods. *Expert Systems with Applications*, 36(4), 7493-7499. <https://doi.org/10.1016/j.eswa.2008.09.056>
- Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*, 37(3), 758-787. <https://doi.org/10.1080/07421222.2020.1790190>
- Luo, Z.-Q., & Zhang, S. (2008). Dynamic Spectrum Management: Complexity and Duality. *IEEE Journal of Selected Topics in Signal Processing*, 2(1), 57-73. <https://doi.org/10.1109/jstsp.2007.914876>
- Manzoor, M. A., & Morgan, Y. (2016). Real-time Support Vector Machine based Network Intrusion Detection system using Apache Storm. *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2(NA), 1-5. <https://doi.org/10.1109/iemcon.2016.7746264>
- Misra, S., Mohammed, P. N., Guner, B., Ruf, C. S., Piepmeier, J. R., & Johnson, J. T. (2009). Microwave Radiometer Radio-Frequency Interference Detection Algorithms: A Comparative Study. *IEEE Transactions on Geoscience and Remote Sensing*, 47(11), 3742-3754. <https://doi.org/10.1109/tgrs.2009.2031104>
- Morshed, A. S. M., Manjur, K. A., Shahjalal, M., & Yahia, A. K. M. (2024). Optimizing Energy Efficiency: A Comprehensive Analysis Of Building Design Parameters. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, 4(04), 54-73. <https://doi.org/10.69593/ajsteme.v4i04.120>
- Mohy-eddine, M., Guezzaz, A., Benkirane, S., & Azrou, M. (2023). An efficient network intrusion detection

- model for IoT security using K-NN classifier and feature selection. *Multimedia Tools and Applications*, 82(15), 23615-23633. <https://doi.org/10.1007/s11042-023-14795-2>
- Nandi, A., Emon, M. M. H., Azad, M. A., Shamsuzzaman, H. M., & Md Mahfuzur Rahman, E. (2024). Developing An Extruder Machine Operating System Through PLC Programming with HMI Design to Enhance Machine Output and Overall Equipment Effectiveness (OEE). *International Journal of Science and Engineering*, 1(03), 1-13. <https://doi.org/10.62304/ijse.v1i3.157>
- Newton, R., & Rouse, J. (1980). Microwave radiometer measurements of soil moisture content. *IEEE Transactions on Antennas and Propagation*, 28(5), 680-686. <https://doi.org/10.1109/tap.1980.1142386>
- Njoku, E. G., Ashcroft, P., Chan, T. K., & Li, L. (2005). Global survey and statistics of radio-frequency interference in AMSR-E land observations. *IEEE Transactions on Geoscience and Remote Sensing*, 43(5), 938-947. <https://doi.org/10.1109/tgrs.2004.837507>
- Nunamaker, J. F., & Chen, M. (1990). Systems development in information systems research. *Journal of Management Information Systems*, 7(3), 89-106. <https://doi.org/10.1080/07421222.1990.11517898>
- Owfi, A., & Afghah, F. (2023). Autoencoder-Based Radio Frequency Interference Mitigation for SMAP Passive Radiometer. *IGARSS 2023 - 2023 IEEE International Geoscience and Remote Sensing Symposium*, 1(NA), 6783-6786. <https://doi.org/10.1109/igarss52108.2023.10281939>
- Paul, J. A., & Wang, X. J. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, 122(NA), 113069-NA. <https://doi.org/10.1016/j.dss.2019.05.009>
- Pullianen, J., Karna, J. P., & Hallikainen, M. (1993). Development of geophysical retrieval algorithms for the MIMR. *IEEE Transactions on Geoscience and Remote Sensing*, 31(1), 268-277. <https://doi.org/10.1109/36.210466>
- Rajić, T., Nikolić, I., & Milošević, I. (2016). The antecedents of SMEs' customer loyalty: Examining the role of service quality, satisfaction and trust. *Industrija*, 44(3), 97-116. <https://doi.org/10.5937/industrija44-10741>
- Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A comparative analysis of cyber-threat intelligence sources, formats and languages. *Electronics*, 9(5), 824-NA. <https://doi.org/10.3390/electronics9050824>
- Reaves, B., & Morris, T. (2012). An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11, 215-229.
- Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8), 10-18. [https://doi.org/10.1016/s1361-3723\(16\)30062-8](https://doi.org/10.1016/s1361-3723(16)30062-8)
- Samarasinghe, N., & Mannan, M. (2021). On cloaking behaviors of malicious websites. *Computers & Security*, 101(NA), 102114-NA. <https://doi.org/10.1016/j.cose.2020.102114>
- Samtani, S., Zhu, H., & Chen, H. (2020). Proactively Identifying Emerging Hacker Threats from the Dark Web: A Diachronic Graph Embedding Framework (D-GEF). *ACM Transactions on Privacy and Security*, 23(4), 3409289-3409233. <https://doi.org/10.1145/3409289>
- Schultz, E. E. (2005). Editorial: Search engines: a growing contributor to security risk. *Computers & Security*, 24(2), 87-88. <https://doi.org/10.1016/j.cose.2005.01.002>
- Sen, R., Verma, A., & Heim, G. R. (2020). Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets. *Journal of Management Information Systems*, 37(1), 191-216. <https://doi.org/10.1080/07421222.2019.1705511>
- Shahjalal, M., Yahia, A. K. M., Morshed, A. S. M., & Tanha, N. I. (2024). Earthquake-Resistant Building Design: Innovations and Challenges. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, 3(04), 101-119. <https://doi.org/10.62304/jieet.v3i04.209>
- Shamim, M. (2022). The Digital Leadership on Project Management in the Emerging Digital Era. *Global Mainstream Journal of Business, Economics, Development & Project Management*, 1(1), 1-14.
- Shamim, M. M. I. (2022). The effects of covid-19 on project management processes and practices. *Central Asian Journal of Theoretical & Applied Sciences*, 3(7), 221-227.
- Song, K. B., Chung, S. T., Ginis, G., & Cioffi, J. M. (2002). Dynamic spectrum management for next-generation DSL systems. *IEEE Communications Magazine*, 40(10), 101-109. <https://doi.org/10.1109/mcom.2002.1039864>
- Spencer, M. W., & Ulaby, F. T. (2016). Spectrum Issues Faced by Active Remote Sensing: Radio frequency interference and operational restrictions Technical Committees. *IEEE Geoscience and Remote Sensing*

- Magazine*, 4(1), 40-45.
<https://doi.org/10.1109/mgrs.2016.2517410>
- Suthaharan, S. (2014). Big data classification: problems and challenges in network intrusion prediction with machine learning. *ACM SIGMETRICS Performance Evaluation Review*, 41(4), 70-73.
<https://doi.org/10.1145/2627534.2627557>
- Talebi, S., Alam, F., Katib, I., Khamis, M., Salama, R., & Rouskas, G. N. (2014). Spectrum management techniques for elastic optical networks: A survey. *Optical Switching and Networking*, 13(NA), 34-48.
<https://doi.org/10.1016/j.osn.2014.02.003>
- Tan, C., Sun, F., Kong, T., Zhang, W., Yang, C., & Liu, C. (2018). ICANN (3) - A Survey on Deep Transfer Learning. In (Vol. NA, pp. 270-279).
https://doi.org/10.1007/978-3-030-01424-7_27
- Tang, J., Chen, X., Zhu, X., & Zhu, F. (2022). Dynamic Reallocation Model of Multiple Unmanned Aerial Vehicle Tasks in Emergent Adjustment Scenarios. *IEEE Transactions on Aerospace and Electronic Systems*, NA(NA), 1-43.
<https://doi.org/10.1109/taes.2022.3195478>
- Wald, L. (1999). Some terms of reference in data fusion. *IEEE Transactions on Geoscience and Remote Sensing*, 37(3), 1190-1193.
<https://doi.org/10.1109/36.763269>
- Waters, J. W., Froidevaux, L., Harwood, R. S., Jarnot, R., Pickett, H. M., Read, W. G., Siegel, P. H., Cofield, R. E., Filipiak, M. J., Flower, D. A., Holden, J. R., Lau, G. K., Livesey, N. J., Manney, G. L., Pumphrey, H. C., Santee, M. L., Wu, D., Cuddy, D. T., Lay, R. R., . . . Walch, M. (2006). The Earth observing system microwave limb sounder (EOS MLS) on the aura Satellite. *IEEE Transactions on Geoscience and Remote Sensing*, 44(5), 1075-1092.
<https://doi.org/10.1109/tgrs.2006.873771>
- Yahia, A. K. M., Rahman, D. M. M., Shahjalal, M., & Morshed, A. S. M. (2024). Sustainable Materials Selection in Building Design And Construction. *International Journal of Science and Engineering*, 1(04), 106-119.
<https://doi.org/10.62304/ijse.v1i04.199>
- Yazar, A., & Arslan, H. (2018). Flexible Multi-Numerology Systems for 5G New Radio. *Journal of Mobile Multimedia*, 14(4), 367-394.
<https://doi.org/10.13052/jmm1550-4646.1442>
- Zhang, L., Liang, Y.-C., & Xiao, M. (2019). Spectrum Sharing for Internet of Things: A Survey. *IEEE Wireless Communications*, 26(3), 132-139.
<https://doi.org/10.1109/mwc.2018.1800259>
- Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, 30(1), 123-152.
<https://doi.org/10.2753/mis0742-1222300104>
- Zhou, H., Sun, J., & Chen, H. (2013). Malicious Websites Detection and Search Engine Protection. *Journal of Advances in Computer Network*