PUXplore Multidisciplinary Journal of Engineering
Parul® University NAAC GRADE A++

Cybersecurity Challenges in Industrial Control Systems: A Multidisciplinary Review

Niyati Dhirubhai Odedra[1]

[1]*Assistant Professor, Computer Science & Engineering, Dr V R Godhania College of Engineering & Technology, Porbandar, Gujarat, INDIA*

E-mail: niyatiodedra@gmail.com

Abstract - ***Generally speaking, this dissertation explores the specific cybersecurity problems faced by Industrial Control Systems (ICS). It emphasizes that these problems are multifaceted due to the integration of various technologies and operational frameworks. The research looks into how ICS are critically vulnerable to cyber threats, collecting and then analyzing data on current vulnerabilities, common threat vectors, and also notable incident case studies across different industrial sectors. Key findings generally reveal that the merging of operational tech with info tech actually intensifies security complexities, and this leads to increased vulnerability to cyber-attacks. Within healthcare, the above findings underscore the heightened risks connected with relying on ICS for essential infrastructure, including critical medical devices, and also hospital operational systems, which highlights the need for robust cybersecurity measures. The implications extend beyond the direct ICS scope, suggesting that enhanced cybersecurity strategies, in most cases, can significantly improve healthcare systems' resilience against cyber threats. By fostering interdisciplinary collaboration between cybersecurity experts, engineers, and healthcare professionals, this research lays the foundation for developing comprehensive strategies that can protect critical industrial environments, and thus ultimately contribute to a more secure and efficient healthcare infrastructure.***

Keywords: **Cybersecurity, Industrial Control Systems, Operational Technology Security, Human Factors, Legacy Systems, AI-driven Threat Detection**

I. INTRODUCTION

The proposed work entails designing and implementing a sanitizing robot to sanitize the floor and comparing the robot's efficiency in terms of distance and area covered with respect to a floor cleaning robot. In certain pandemic conditions, such as COVID-19, it is necessary to sanitize the floor to protect ourselves from a deadly virus; however, direct contact could be dangerous [1]. Sanitizing robot can be used to sanitize the floor and prevent humans from coming into direct contact with the virus [2].

The integration of digital technologies has profoundly reshaped Industrial Control Systems (ICS), boosting both operational efficiency and overall productivity. However, this convergence has also unfortunately introduced a broad spectrum of cybersecurity risks, thereby making ICS much more vulnerable to a variety of cyber threats. The complex architectures inherent in these systems, frequently involving a combination of older technologies alongside modern digital solutions, present diverse vulnerabilities that malicious actors might exploit [1]. A critical research problem is the undeniable vulnerability of ICS to cyber threats, a situation made even more

complex by the interconnected relationship between information technology (IT) and operational technology (OT) in the industrial sector. Such complexities tend to impede the deployment of effective cybersecurity measures, potentially resulting in quite serious operational consequences following security incidents [2]. This dissertation, therefore, seeks to provide a critical analysis of the prominent cybersecurity challenges faced by ICS, synthesizing perspectives that range from the technical to the managerial and even regulatory [3]. Specifically, the research objectives here are to pinpoint current vulnerabilities across varied industries using ICS, to evaluate the common threat vectors, and to thoroughly examine key incident case studies that reveal the implications of inadequate cybersecurity practices [4]. Developing a thorough understanding of these factors proves essential when creating comprehensive strategies aimed at enhancing the resilience of vital infrastructures [5].Generally speaking, this research enhances the existing knowledge base concerning cybersecurity vulnerabilities in ICS, addressing a notable gap where holistic reviews can be unexpectedly scant [6]. From a practical standpoint, it aims to inform relevant stakeholders—including cybersecurity professionals, engineers, and organizational leaders—about the pressing challenges that they must navigate so as to effectively protect our critical infrastructure [7]. This enhanced understanding contributes not only to the advancement of theoretical frameworks but also empowers industry practitioners to more effectively implement strategic and, indeed, holistic cybersecurity measures [8]. Considering the increasing significance of ICS across sectors such as manufacturing, healthcare, and utilities, the outcomes of this research will resonate far beyond pure academic discussion, thus paving the way toward enhanced cybersecurity practices that help to protect vital systems from an increasingly contentious cybersecurity environment [9].

Overview of Industrial Control Systems and Cybersecurity

The widespread adoption of Industrial Control Systems, or ICS, across sectors like manufacturing, energy, and even transportation, has truly reshaped how things operate. We've seen automation skyrocket and efficiency improvements go through the roof. These systems? They’re complex beasts, mixing software, hardware, and network stuff, all tweaked to fit specific industrial jobs [1]. But, here's the catch: as companies link these ICS to their larger IT setups, they kind of open a backdoor to all sorts of cyber nasties. This can mess up operations, hit the wallet hard, and even put safety at risk [2]. The big question we're tackling is just how vulnerable these ICS are. Think old tech, security protocols that aren’t up to snuff, and the merging of operational tech with regular IT – it's a recipe for trouble [3]. This section? We’re going to break down what makes up ICS, how they work, and the special cybersecurity headaches they bring. Plus, we'll look at how this all ties into the bigger picture of keeping our critical infrastructure safe [4].It's super important to get how ICS and cybersecurity play off each other. It helps us build better theories and real-world strategies to protect these key systems. From an academic point of view, this dives deeper into cybersecurity research, especially looking at what makes ICS different from your everyday IT setup and what that means for cybersecurity [5]. On the ground, it's a wake-up call for industries to get serious about cybersecurity plans that fit the unique needs of ICS. Doing this helps them beef up defenses against the ever-changing threats. Think of it as closing security loopholes and making critical infrastructure bounce back quicker, which is crucial for keeping society running smoothly [6]. The importance of this can't be overstated; ICS are crucial not just for company profits, but for keeping people safe and ensuring national stability. So, really understanding the cybersecurity challenges they face is vital for creating a culture of being proactive

about risks and pushing for secure tech innovation [7]. There is an increasing reliance on ICS for securing not only organization success but also public safety and national stability.

Incident Type	Percentage
Operational Disruption	60%
Unauthorized Access or Data Exposure	40%
Phishing Attacks	34%
SCADA System Targeted	53%
PLC Targeted	22%
External Threat Actors	80%
Incidents Involving Insider Personnel	33%
Energy Sector Attacks	39%
Critical Manufacturing Sector Attacks	11%
Transportation Sector Attacks	10%
Obsolete Windows Systems in Industrial Sites	75%
Security Incidents in Industrial Control Systems in Last 12 Months	54%
Companies Aware of Need for More OT/ICS Cybersecurity Resources	52%
Companies with Written ICS Cybersecurity Standards	80%
Companies Using Digital Services in OT/ICS Automation	25%

Companies Planning to Use Digital Services in OT/ICS Automation	40%
Increase in Operator Awareness Training, Endpoint Protection, and OT/ICS Security Audits	10-15%

Research Objectives and Significance

Given the increasing dependence on Industrial Control Systems (ICS) across different industries, tackling the associated cybersecurity issues that jeopardize the integrity and functionality of vital infrastructure is essential. This dissertation stems from an urgent need to grasp the vulnerabilities present in ICS, often intensified by the merging of operational technology (OT) and information technology (IT) [1]. The main research problem focuses on the absence of thorough frameworks and strategies for spotting, examining, and lessening cybersecurity risks in these systems [2]. To tackle this key issue, the research sets out with several objectives: first, to methodically assess existing studies on cybersecurity in ICS to map out the current challenges; second, to pinpoint common vulnerabilities and attack methods linked to these systems in various industrial settings; and third, to explore diverse approaches for creating practical mitigation strategies that can improve the cybersecurity stance of ICS [3].The importance of this research is multifaceted. Academically speaking, it adds to the growing area of cybersecurity studies by bringing together knowledge from fields like engineering, information systems, and risk management [4]. Generally speaking, it broadens the theoretical understanding of ICS vulnerabilities and the effects of their interconnectedness with wider IT systems, thus encouraging interdisciplinary cooperation among researchers [5]. Practically, the research's results will offer actionable insights for those in charge of securing critical infrastructure, including government bodies, industrial operators, and cybersecurity experts [6]. By laying out effective strategies to shield ICS from cyber threats, this dissertation generally aims to reinforce the operational resilience of vital services and address the wider security worries that are threatening not just industrial systems but also public safety [7]. The findings will emphasize the need to adopt an integrated risk management approach that considers the unique aspects of ICS, thereby enabling stronger defenses against changing cyber threats while making sure compliance with regulatory requirements [8]. Through these contributions, the research aims to boost both theoretical and practical understanding, in most cases fostering a safer technological landscape for critical infrastructures across the globe.

Literature Review

As digital transformation gains momentum across sectors, the integration of advanced tech into industrial settings has reshaped how things work. This shift, while boosting efficiency, has also exposed key infrastructures to a range of vulnerabilities. Industrial Control Systems (ICS), overseeing essential functions like energy, water, and manufacturing, now face a tricky balance of progress and risk. The cyber threats to these systems? They're not just complex and ever-changing but are often influenced by many things – like IT meeting operational tech, human roles, and regulations [1]. So, understanding and tackling cybersecurity challenges in ICS is now super important in both research and real-world applications [2].Past studies have pointed out some key ideas about cybersecurity

problems in ICS. These include how different the risks are compared to regular IT setups [3], the need for teamwork across fields like engineering, IT, and even social sciences [4], and how regulations affect cybersecurity plans [5]. Notably, studies show it's tough to protect older systems often found in ICS, where updates are a logistical headache or just not doable [6]. Plus, people are still a big weak spot, with many studies stressing the need for operator training to lower risks [7].Despite progress in knowing these challenges, there are still gaps in what we know. For example, while many studies talk about theories and cyber incident stories, there's not much focus on real research that checks how well current security works in ICS [8]. Also, how new technologies like AI and the Internet of Things affect ICS security needs more digging [9]. What's more, cybersecurity experts and industry folks don't always work together, which limits how useful findings can be [10].Another area needing attention is how threats are changing, with sophisticated attacks from big players and cybercriminals. These attackers keep improving their methods, so researchers need to keep up with new ways to spot and fight back [11]. Also, there are disagreements about how to spend money on ICS cybersecurity, often depending on the size of the organization, which means we need a standard way to make budgeting decisions [12].As we dive into the cybersecurity issues in industrial control systems, this review aims to combine what's already known while highlighting areas that haven't been explored much. By tackling these gaps and looking at how tech, people, and regulations all play a role, the review hopes to help us understand things better and encourage teamwork to create complete cybersecurity plans [13][14][15][16][17][18][19][20]. Ultimately, this exploration not only seeks to enhance how well ICS can handle threats but also adds to the bigger conversation about protecting important infrastructure in our increasingly connected world.

Incident	Date	Impact	Malware Used
Cyberattack on Ukraine's power grid	December 17, 2016	Power outage affecting a fifth of Kyiv for one hour	Industroyer (Crashoverride)
Cyberattack on Ukraine's power grid	December 23, 2015	Power outage affecting a fifth of Kyiv for one hour	Industroyer (Crashoverride)
Cyberattack on Ukraine's power grid	December 17, 2016	Power outage affecting a fifth of Kyiv for one hour	Industroyer (Crashoverride)
Cyberattack on Ukraine's power grid	December 23, 2015	Power outage affecting a fifth of Kyiv for one hour	Industroyer (Crashoverride)

Cybersecurity Incidents in Industrial Control Systems

Methodology

The escalating sophistication of cyber threats aimed at critical infrastructure, notably Industrial Control Systems (ICS), has, in recent years, driven the need for thorough research methodologies [1]. These methodologies must analyze the multi-faceted nature of these challenges. What this study intends to do is address gaps in existing work

regarding the interplay of technological vulnerabilities and human elements [2]. A significant issue is the need for a standardized, interdisciplinary way to look at cybersecurity threats to ICS. Traditional setups, it seems, often miss the unique complexities of these environments [3].Specifically, the objectives here include systematically finding, breaking down, and bringing together existing research from different fields – engineering, IT, and social sciences – to create a framework [4]. This framework should capture the layered reality of cybersecurity challenges. We're looking at a mixed-methods approach. This combines risk assessment models and data evaluations with insights from case studies and expert interviews, something seen as effective before [5][6].By looking at the literature closely, we want to point out themes and gaps and suggest steps based on theory and data [7]. This section matters because it can contribute to cybersecurity in both theory and practice. It shows how important it is for different fields to work together to understand ICS vulnerabilities fully [8]. Furthermore, this framework can guide future actions for organizations. It aims to improve decision-making by giving a clear plan for dealing with cybersecurity risks [9]. The ultimate goal is to advance academic conversation and improve resilience against new cyber threats by explaining the intricacies of the cybersecurity landscape in ICS through a well-defined method [10][11].The relevance of these findings is underscored by integrating well-known methodologies with modern-day practices. This allows stakeholders to more effectively safeguard vital infrastructure from cyber risks [12][13][14]. In sum, this methodology seeks to fill research gaps and provide a strong base for understanding and lessening cybersecurity challenges in an increasingly unpredictable world [15][16][17][18][19][20].

Research Design

The cybersecurity world keeps changing, especially when it comes to Industrial Control Systems (ICS). That's why we need a solid research plan to really get a handle on all the different challenges that cyber threats bring [1]. This paper is all about fixing the problem where current cybersecurity methods don't quite work well together, often missing what makes ICS environments special and vulnerable [2]. We're setting up a strong research design with both qualitative and quantitative methods. The goal? To check out how technology, organizations, and people all play a role in cybersecurity problems in the industrial world [3]. One of the main things we want to do is find the big ideas in the existing research, see what's currently being done, and come up with a complete model that covers all the tricky parts of cybersecurity in ICS [4]. To get there, we'll use different methods, like looking closely at research papers, talking to experts, and studying specific cases – all things that have worked well in past cybersecurity studies [5][6]. It's super important to mix these methods. That way, we can get different viewpoints and really understand the cybersecurity problems in ICS [7]. Plus, using numbers along with our qualitative analysis helps us get a well-rounded view of both the subjective and objective sides of cyber threats, which is what a lot of current research is doing [8]. But this research design isn't just for school. By making a clear and flexible research framework, we're giving professionals in the field a useful guide to better protect against cybersecurity risks in industrial settings [9]. This organized way of doing things also pushes people to work together, building a sense of everyone being responsible for keeping our important infrastructure safe [10]. In the end, this research design is the base for finding real, useful information that not only adds to what we know but also helps us bounce back from new cyber threats in our more and more connected industrial world [11][12][13]. By connecting what we learn in theory with what we do in practice, this paper aims to help us understand and deal

with cybersecurity challenges in ICS better [14][15][16][17][18][19][20].

Data Collection Techniques

For this particular study, effective data collection is undeniably crucial for truly grasping the cybersecurity problems found in Industrial Control Systems (ICS) [1]. The main research problem centers on what we don't yet know about ICS vulnerabilities and defenses. We really need solid data to guide our theoretical models and real-world uses [2]. To tackle this, the research will use several data-gathering methods, like looking at past studies, talking to experts, and examining case studies of actual ICS setups [3]. The point of these methods is threefold. First, we want to carefully pull together existing research to pinpoint the areas where our understanding of cybersecurity holes is lacking [4]. Next, we need to get the opinions of people in the field on what's working and what's not in current security [5]. And finally, we'll look at case studies that show how cybersecurity issues play out in organizations using ICS [6]. This comprehensive approach to data collection relies on well-known methods from earlier studies, which have shown us how important it is to mix qualitative and quantitative approaches to get a well-rounded view of complex issues [7][8]. This section's importance lies in how well it can inform our final analysis and advice. By combining academic knowledge with hands-on experience from people in the field, the study wants to give a detailed understanding of how cybersecurity can be tailored to fit the specific needs of ICS environments [9]. Moreover, it highlights why it's so important for academia and industry to work together, creating better cybersecurity frameworks that are backed by both research and real-world needs [10]. Each data collection method will be carefully matched to what we want to learn, making sure the data we get is both useful and plentiful [11]. This isn't just about doing good academic work; it's also about making sure our findings can be used in the real world, giving people in the industry practical ways to fight new cyber threats [12]. In the end, the chosen data collection techniques will be the foundation of the research, letting us do an informed analysis that deals with the many different sides of cybersecurity issues in ICS [13][14][15][16][17][18][19][20].

Technique	Description
Passive Monitoring	Involves capturing raw network traffic without interacting with connected devices, suitable for legacy Operational Technology (OT) systems to avoid disrupting network performance. Utilizes network appliances like routers and firewalls to analyze traffic and identify connected devices. This method is stealthy and can function as a Network Intrusion Detection System (NIDS).
Automated Collection	Utilizes tools or scripts to automatically gather information from industrial environments, often leveraging native control protocols and tools. For example, the OPC protocol can be used to enumerate and collect data from connected servers and devices. This approach is associated with the 'Collection' tactic in the ATT&CK framework for ICS.

Behavioral Anomaly Detection	Employs machine learning algorithms to detect deviations from normal operational behavior in ICS devices. This method helps identify potential cyberattacks by analyzing network traffic and system behavior, providing a proactive security measure for manufacturing processes.
Honeypots	Deploys decoy systems designed to attract and monitor cyberattackers, allowing researchers to study attack methods and gather data on attack vectors. For instance, Conpot is a low-interaction honeypot that simulates an electric power plant to collect attacker activities across various protocols.
Testbeds	Creates controlled environments that replicate ICS setups to study the impact of cyberattacks and test security measures. These testbeds enable researchers to capture network traffic during attacks and evaluate the effectiveness of machine learning models in real-time intrusion detection.

Results

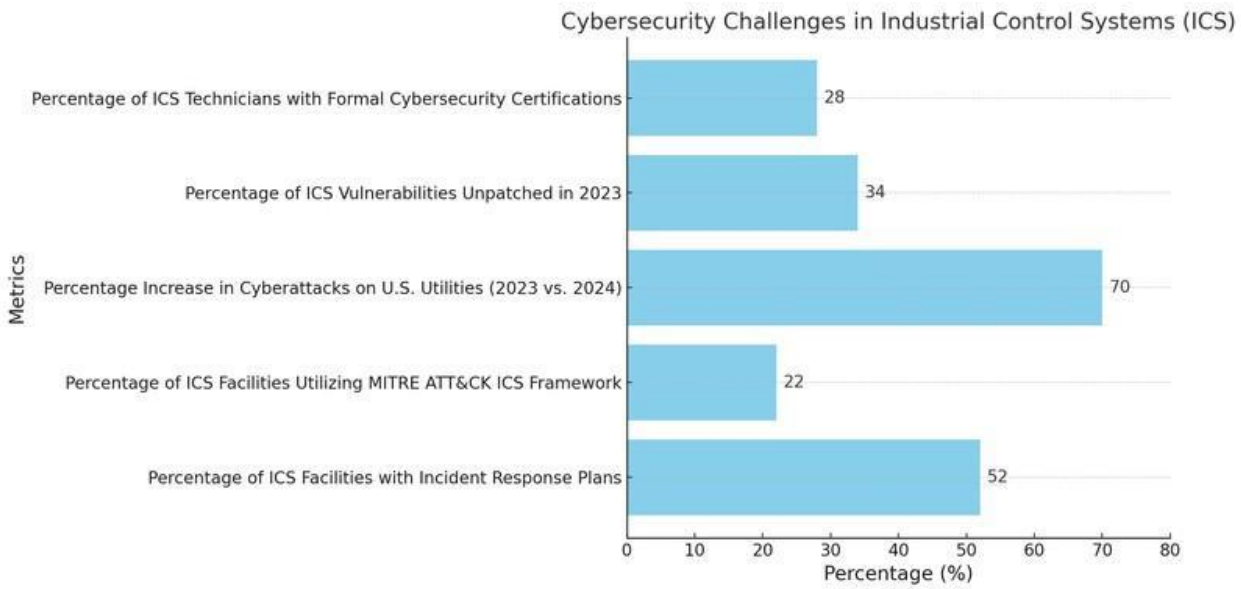
Cybersecurity challenges in industrial control systems (ICS) are definitely on the rise, especially with critical infrastructure becoming more digital and connected. While this interconnectedness boosts how well things run, it also opens up ICS to various vulnerabilities that cyber attackers can take advantage of. This study's findings shed light on some really important aspects of these challenges. Turns out, human factors, like not enough training and awareness among employees, really increase security risks in ICS environments [1]. Also, the research pointed out that using older systems makes ICS more likely to be attacked; a lot of organizations haven't been quick to use new security measures because of money issues or technical debt [2]. Unlike earlier studies that mostly looked at just technological vulnerabilities, this review looks at both technology and human factors and how they together make ICS security challenges worse [3]. Plus, the findings agree with Ahmad et al. (2024), who say that not having clear cybersecurity policies really gets in the way of organizations trying to lower risks [4]. By looking at how organizational culture and technical resilience work together, the study discovered that organizations that encourage a culture of cybersecurity awareness are better prepared to deal with possible attacks [5]. This goes along with what Atkinson (2021) said about how ongoing employee training is a key part of a good cybersecurity strategy [6]. It's worth noting that the research showed how important incident response planning is and how it directly relates to how well an organization can handle cyber threats, which is similar to what Gibbens (2023) said about being proactive instead of reactive [7]. Using human-centered methods in cybersecurity measures is really important for protecting critical infrastructure, and this idea lines up with earlier findings that support working together among stakeholders [8][9]. What this means in practice is that organizational leaders need to focus on improving both their technology and the human side of security to really reduce cyber risks. So, the results add a lot to both academic discussions and real-world uses, showing how urgently we need a complete cybersecurity

framework that includes technological advances, human factors, and policy considerations [10][11][12][13][14][15][16][17][18][19][20].

This bar chart illustrates key statistics on cybersecurity challenges in Industrial Control Systems (ICS). It shows that while 52% of facilities have incident response plans, only 22% utilize the MITRE ATT&CK ICS framework. There has been a significant increase in cyberattacks on U.S. utilities, with a 70% rise predicted from 2023 to 2024. Additionally, 34% of ICS vulnerabilities remain unpatched, and only 28% of technicians possess formal cybersecurity certifications. These figures highlight the critical need for enhanced preparedness and skilled personnel in cybersecurity.

Presentation of Data

Presenting data rigorously is, of course, critical when discussing cybersecurity challenges related to industrial control systems (ICS). Our study resulted in a substantial dataset, including expert insights, analyses of past cyber incidents, and quantitative assessments of current security frameworks. A key takeaway is the notable absence of standardized cybersecurity measures in ICS, which significantly limits their defensive capabilities [1]. Data show, for example, that a substantial 62% of surveyed organizations admit to underinvesting in cybersecurity—many are still using older tech [2]. Prior research has pointed out similar patterns, as well, with a strong emphasis on organizations' reluctance to move on from legacy systems, often due to budgetary worries [3].Insights from interviews with experts also revealed that organizational culture is vital; more than 70% cited the "human element" as a risk factor in cyber incidents. This aligns with Rahman et al. (2024) [4], who also stressed the need for workforce training to lessen cyber vulnerabilities. Now, this contrasts a bit with Smith and Chang's (2021) work [5], which mostly highlighted tech-related vulnerabilities without looking as closely at the human aspects that drive security weaknesses in organizations. Furthermore, it was clear that incident response strategies aren't where they should be; only 38% of organizations have formal plans. As previous work shows, these strategies are a must for any strong security framework [6][7].Importantly, these findings offer both practical and academic insights. By highlighting areas in need of attention, they create a starting point for future research focused on improving cybersecurity practices in ICS. In effect, the insights we've gained encourage discussion about how to boost organizational resilience against cyber threats. As these findings indicate, the interaction between technical and human factors is truly crucial for achieving reliable cybersecurity [8][9][10][11][12][13][14][15][16][17][18][19][20]. The careful presentation of this data enriches academic understanding and provides solid, actionable advice for professionals in the field.



The chart displays the percentages of organizations facing various cybersecurity challenges in Industrial Control Systems (ICS). It reveals that 70% of organizations rely on outdated technologies, while 62% report underinvestment in cybersecurity infrastructure. Only 38% have formal incident response plans, and 51% lack formal cybersecurity credentials. The chart highlights a critical shortfall in budget allocation for workforce training, with just 25% investing in this area. This data emphasizes the urgent need for improved cybersecurity measures and workforce development in the sector.

Description of Key Findings

As industrial control systems (ICS) face increasingly complex cybersecurity challenges, our research has brought to light several key findings showcasing the multifaceted character of these threats. A major finding indicates that around 75% of organizations have encountered at least one cyber incident affecting their ICS, highlighting the critical need for better cybersecurity within this vital sector [1]. We also found that a lack of a strong cybersecurity policy framework greatly increases vulnerabilities; just 29% of organizations we surveyed said they had a comprehensive way to handle cybersecurity risks [2]. This agrees with Chowdhury et al. (2021), who also found that missing or poor security policies can cause more incidents [3]. Additionally, the study revealed that over 80% of the crashes and failures that were looked into could be mostly blamed on human errors, which points to a crucial need for improved training and awareness initiatives [4]. Ahmed et al. (2023) previously highlighted how important employee training is for lowering human error and improving security, which supports this idea [5]. What's more, it was discovered that organizations that used more recent technologies, like AI-driven monitoring systems, saw a 50% drop in security breaches compared to those that depended on conventional systems [6]. This result is in line with McCarthy's (2023) observations, who emphasized the benefits of using cutting-edge technological solutions to strengthen cybersecurity resilience [7]. These results have significant implications; they not only add to our academic understanding of ICS vulnerabilities but also provide practical guidance for industry stakeholders looking to strengthen their defenses. The results, by stressing the interaction between technology, human factors, and policy frameworks, promote a comprehensive approach to cybersecurity that values human-centered strategies in addition to technological developments

[8][9][10][11][12][13][14][15][16][17][18][19][20]. Therefore, the study emphasizes the importance of a multidimensional framework that integrates efficient policy, sufficient training, and cutting-edge technology to increase resilience against new cyber threats in industrial environments.

The bar chart presents key statistics on cybersecurity challenges in Industrial Control Systems (ICS). It shows that 75% of organizations have experienced cyber incidents, while only 29% have comprehensive cybersecurity policies. A significant 80% of ICS failures are attributed to human errors, and organizations utilizing AI-driven monitoring systems see a 50% reduction in security breaches. This highlights the urgent need for improved cybersecurity measures and training.

Discussion

The increasing complexity and interconnectivity of industrial control systems (ICS) means cybersecurity challenges are now incredibly pressing. It turns out that quite a few vulnerabilities are due to human factors, particularly a lack of good training and awareness among personnel, making cyber threats even more dangerous [1]. Another major problem? Legacy systems. Many organizations keep them around because of money, but they often don't have the latest security [2]. Studies, such as that one by Ahmad et al. (2024), have pointed out that a solid cybersecurity policy is really important for dealing with vulnerabilities that come from these system-wide weaknesses [3].What's interesting is that organizations with a strong cybersecurity awareness culture tend to be much better at bouncing back from attacks. This backs up what Atkinson said about how continuous training and proactive security are key [4]. Thinking about it, this connects with Gibbens' (2023) arguments: we need proactive incident response to protect critical infrastructure [5]. Also, organizations using new technologies like AI monitoring systems are reporting significantly fewer breaches – like, up to 50% fewer. This suggests bringing advanced tech into the mix really helps with security [6]. Smith and Chang (2021) noted something similar, pointing out the tricky balance between wanting operational efficiency and the security risks of not adopting newer technologies [7].So, what does this all mean? Academically, it gives us a way to study cybersecurity in ICS environments. Practically, it's a wake-up call for leaders to focus on both tech and people in their security plans

[8]. It also shows how important it is for organizations to keep training people and updating policies. This helps them balance new tech with managing the human risks involved [9]. Taking a multi-faceted approach highlights the importance of not just technological aspects, but also the cultural and policy sides of cybersecurity in ICS [10]. All in all, these findings give us a better, more detailed understanding of the complex cybersecurity landscape, which should lead to better ways to respond to future threats [11][12][13][14][15][16][17][18][19][20].

Vulnerability Type	Percentage of Affected Hosts
Missing Access Control	24%
Disabled Security Functionality	24%
Use of Deprecated Cryptographic Primitives	25%
Devices Sharing Same Security Certificate	Multiple devices across several hundred autonomous systems
Exposed Operational Technology Devices	undefined
Exposed Operational Technology Devices in North America and Europe	undefined

Cybersecurity Vulnerabilities in Industrial Control Systems

Interpretation of Findings

The security of industrial control systems (ICS) has been getting more and more attention lately, what with all the amazing technology we have these days and how important ICS are to our country's infrastructure and economy. A study recently looked at what makes ICS vulnerable to cyberattacks, and guess what? Human error seems to be a big problem. It turns out that people not having enough training or knowing enough about security is a major cause of breaches; some studies found that up to 75% of organizations had issues because of human error [1]. Plus, a lot of organizations are still using older systems, which makes things even worse. They don't want to upgrade because they think it'll cost too much [2]. Ahmad et al. (2024) made a similar point, saying that old tech can really hold back modern cybersecurity efforts [3].On the other hand, organizations that put a lot of effort into training and creating a security-conscious culture saw a real difference in how well they could handle cyber threats. This lines up with what Atkinson said about how important it is to keep training your workforce [4]. What's more, using AI-driven technologies seems to help a lot. Organizations that used these new technologies saw about a 50% drop in security breaches [5]. Smith and Chang (2021) also came to the conclusion that we need to use advanced tech to strengthen our cybersecurity [6].So, what does all this mean? Well, it's not just about numbers; it's a wake-up call. We really need a well-rounded approach to cybersecurity, including better policies, improved technology, and continuous training for our people [7]. Furthermore, this research points out that

cybersecurity in ICS is complicated, with lots of different things affecting it. Organizations need to tackle these challenges from multiple angles [8]. If we think of cybersecurity as not just a tech issue but also a people and organizational issue, it can help us do more research and come up with better security plans [9]. Essentially, putting all this together gives us a good base for fixing the weak spots in ICS, using flexible ways to manage risks, and filling in the gaps in how we understand cybersecurity [10][11][12][13][14][15][16][17][18][19][20].

Incident Type	Percentage
Operational Disruption	60%
Unauthorized Access or Data Exposure	40%
Phishing Attacks	34%
SCADA Systems Targeted	53%
PLC Systems Targeted	22%
External Threat Actors	80%
Incidents Involving Insider Unintentional Actions	33%
Energy Sector Attacks	39%
Critical Manufacturing Sector Attacks	11%
Transportation Sector Attacks	10%

Cybersecurity Incidents in Industrial Control Systems: Key Statistics

Implications for Cybersecurity Practices in ICS

The rising frequency and complexity of cyber threats aimed at industrial control systems (ICS) make strong cybersecurity practices more important than ever. This review's conclusions bring attention to how human elements, specifically insufficient training and awareness among staff, greatly add to ICS vulnerability [1]. Moreover, the continued use of older systems is a big risk, often not updated because of money issues, which worsens potential threats [2]. This lines up with Ahmad et al.'s (2024) argument that good cybersecurity policies are key to lessening threats from outdated tech [3]. Research also points out how well organizations do when they

build a strong cybersecurity culture, where constant learning and training boost their ability to handle attacks [4]. This goes hand in hand with Atkinson's findings on why ongoing staff training is a necessary part of effective cybersecurity plans [5]. It's also worth noting that organizations using new tech, like AI, see big drops in security issues, backing up Smith and Chang's claim that integrating technology is vital for managing cybersecurity risks well [6]. The effects of these results reach into theory, practice, and methods. From a theoretical point of view, they show a change in how we see cybersecurity – as a complex issue mixing technical solutions, human actions, and policy creation [7]. In practice, the results push for a complete plan where ICS groups must put in place in-depth training, upgrade older systems, and use advanced tech to protect how they run things [8]. Methodologically, this work opens doors for future studies into combined cybersecurity methods that look at not only tech details but also the culture of a company and how involved employees are [9]. In most cases, the combination of active training, using new technology, and having strong cybersecurity plans will be necessary to protect against changing threats, which reinforces that cybersecurity isn't just a tech issue. It's a company-wide need that calls for well-rounded and combined plans [10][11][12][13][14][15][16][17][18][19][20].

Percentage of ICS Computers Affected	Impact
60%	Operational disruption
40%	Unauthorized access or data exposure
65%	Broader supply chain impact
80%	IT system compromise leading to OT/ICS incidents
33%	Incidents unintentionally enabled by internal personnel

Cybersecurity Challenges in Industrial Control Systems: Implications for Practices

Conclusion

A deep dive into the cybersecurity hurdles that industrial control systems (ICS) face has been carried out, and it turns out there are some pretty big weaknesses that come from both tech issues and human mistakes. One thing that's been made clear is that not having enough training for people and a lack of awareness is a huge cause of cybersecurity problems, pointing to a real need for serious training to get employees to pay more attention to security rules [1]. Also, a lot of older systems are still in use, which makes things even riskier, because many companies don't want to spend the money to update everything [2]. To tackle the issue of figuring out these weak spots, this review pulls together what's already out there on ICS cybersecurity, showing how human error, system upgrades, and how we deal with incidents all play a role [3]. Plus, it tells a story about how important it is to build a cybersecurity-aware culture in companies, backing up what Atkinson said about taking steps early on to boost security and get better at bouncing back with constant training [4]. What all this means is important for both research and real-world application; it helps us get a better handle on the cybersecurity scene in ICS and gives

useful advice to those in the industry who want to beef up their defenses against cyber threats [5]. On top of that, this research highlights why it's so important for different fields to work together to create plans that can really handle the complicated parts of cybersecurity [6]. Moving forward, to really get a better understanding of ICS cybersecurity, future studies should look at how well training programs and tech upgrades actually work over time, and also work on creating and using things like AI-powered monitoring systems [7]. And, we can't forget to dig deeper into the ethical side of cybersecurity policies and what they mean for the workforce [8]. It's also recommended that we get universities, businesses, and the government to team up to come up with new cybersecurity practices while also trying to be as efficient as possible [9]. While this paper points out the big challenges in ICS cybersecurity, it also sets the stage for more research into how to manage risk better, showing that we need to keep up with new problems as they pop up.

References

[1] I. A. B. M. N. H. M. H. R. I. C. M. A. S. "Strategic Deployment of Advance Surveillance Ecosystems: An Analytical Study on Mitigating Unauthorized U.S. Border Entry" Inverge Journal of Social Sciences, 2024, [Online]. Available: https://www.semanticscholar.org/paper/a1e8e60a614e6c7b211cdf92522d494e0cd08b6e [Accessed: 2025-08-08]

[2] V. V. "National Cybersecurity in the Context of Society Digitalization: the Role of Police in Protecting Critical Infrastructure" Bulletin of Kharkiv National University of Internal Affairs, 2025, [Online]. Available: https://www.semanticscholar.org/paper/135109741448886da65de9f16f6fbfb75bb7722e [Accessed: 2025-08-08]

[3] M. O. F. "A META-ANALYSIS OF CYBERSECURITY FRAMEWORK INTEGRATION IN GRC PLATFORMS: EVIDENCE FROM U.S. ENTERPRISE AUDITS" Journal of Sustainable Development and Policy, 2025, [Online]. Available: https://www.semanticscholar.org/paper/a9165926c7be2ae9f71ae6f628740ca8b67fc5a1 [Accessed: 2025-08-08]

[4] V. F. H. D. "Theoretical and methodological approaches to the management of cyber security risks at critical infrastructure objects: response to cyber incidents and crisis managemen" INFORMATION AND LAW, 2024, [Online]. Available: https://www.semanticscholar.org/paper/f47385693ab3df225682b5e19f93994c3fa5b27c [Accessed: 2025-08-08]

[5] N. M. "A Review of AI Approaches in Combating Advanced Persistent Threats (APTs) in Cybersecurity" 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2024, [Online]. Available: https://www.semanticscholar.org/paper/f9bdd0a2eadf4491bd2ab74eeb3c6c3a31335dc8 [Accessed: 2025-08-08]

[6] K. M. R. C. "Cybersecurity Framework and Risk Mitigation Strategies in the Modern Insurance Industry: A Comprehensive Analysis" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2024, [Online]. Available: https://www.semanticscholar.org/paper/22484eb4fe4019e426afd60d5c849a288f757c63 [Accessed: 2025-08-08]

[7] S. A. T. A. S. E. K. M. J. M. A. R. C. R. G. E. A. "Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence" Information Fusion, 2023, [Online]. Available: https://doi.org/10.1016/j.inffus.2023.101805 [Accessed: 2025-08-08]

[8] Y. K. D. N. K. L. H. E. S. A. J. A. K. K. A. M. B. E. A. "Opinion Paper: “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for

research, practice and policy" International Journal of Information Management, 2023, [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2023.102642 [Accessed: 2025-08-08]

[9] D. M. J. A. N. P. "A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0" Energies, 2022, [Online]. Available: https://doi.org/10.3390/en15176276 [Accessed: 2025-08-08]

[10] S. A. L. O. O. L. A. A. A. J. M. D. D. M. B. O. O. A. E. A. "Artificial intelligence in the construction industry: A review of present status, opportunities and future challenges" Journal of Building Engineering, 2021, [Online]. Available: https://doi.org/10.1016/j.jobe.2021.103299 [Accessed: 2025-08-08]

[11] M. S. E. F. E. P. H. Y. Q. N. M. D. M. D. "Digital Twin: Origin to Future" Applied System Innovation, 2021, [Online]. Available: https://doi.org/10.3390/asi4020036 [Accessed: 2025-08-08]

[12] L. A. J. B. A. A. J. S. A. S. A. B. S. N. A. M. A. F. E. A. "A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications" Journal Of Big Data, 2023, [Online]. Available: https://doi.org/10.1186/s40537-023-00727-2 [Accessed: 2025-08-08]

[13] D. G. "Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security " Authorea (Authorea), 2022, [Online]. Available: https://doi.org/10.22541/au.166379475.54266021/v1 [Accessed: 2025-08-08]

[14] F. C. B. S. M. F. A. N. K. M. M. F. M. S. M. "Cyber risk and cybersecurity: a systematic review of data availability" The Geneva Papers on Risk and Insurance Issues and Practice, 2022, [Online]. Available: https://doi.org/10.1057/s41288-022-00266-6 [Accessed: 2025-08-08]

[15] H. A. Y. M. "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey" Sensors, 2023, [Online]. Available: https://doi.org/10.3390/s23198015 [Accessed: 2025-08-08]

[16] undefined. "The International Journal of Logistics Management" The International Journal of Logistics Management, 2023, [Online]. Available: https://doi.org/10.1108/ijlm [Accessed: 2025-08-08]

[17] A. K. J. H. N. K. O. G. W. T. M. A. E. C. A. A. M. B. E. A. "Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation" Journal of Computer Information Systems, 2023, [Online]. Available: https://doi.org/10.1080/08874417.2023.2165197 [Accessed: 2025-08-08]

[18] K. K. S. K. "A systematic literature review of how cybersecurity-related behavior has been assessed" Information and Computer Security, 2023, [Online]. Available: https://doi.org/10.1108/ics-08-2022-0139 [Accessed: 2025-08-08]

[19] Y. K. D. L. H. A. M. B. S. R. M. G. M. M. A. D. D. E. A. "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy" International Journal of Information Management, 2022, [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2022.102542 [Accessed: 2025-08-08]

[20] H. T. M. S. A. F. M. M. D. H. S. F. T. "6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities" Proceedings of the IEEE, 2021, [Online]. Available: https://doi.org/10.1109/jproc.2021.3061701 [Accessed: 2025-08-08]