**Cyber-Physical Security in Electromechanical Human-Machine Systems (EPICS): The Future of Protection**

**VISWANADHA RAJU BYRRAJU (4236949)**

**Masters in Cybersecurity, Webster University**

**CSSS 6000: Practical Research in Cybersecurity**

**Instructor: Dr. Adewale Ashogbon**

**RESEARCH PAPER**

**May 11th, 2025**

**ABSTRACT**

Modern industries and critical infrastructure systems benefit from **cyber-physical systems** because they use these **CPS** to automate operations and increase operational efficiency. However, these new electromechanical systems experience rising cyber threats that endanger their operational safety standards, and accessibility along with data privacy protection. This research evaluates the essential role of cyber-physical security within **electromechanical human-machine systems (EPICS)** which functions as a primary subcategory of CPS to connect humans with machines through robotic systems and automated equipment. It evaluates the security weaknesses in EPICS that involve **data tampering**, **unauthorized control system entry**, and **system failures** triggered by cyberattacks. Also, this paper discusses comprehensive details about consequences from such attacks, including safety dangers and operational disruptions. The present security techniques such as **encryption** along with **intrusion detection systems** and **secure communication protocols** are examined through their vulnerabilities in this investigation. Looking into the future, emerging technologies like **AI**, **ML**, and **quantum computing** are the solutions that can make security stronger by using **predictive analysis**, **detecting unusual patterns**, and **improving encryption**. Finally, the paper shows the establishment of **standardized policies** and **operational rules** for EPICS development alongside specific guidelines to produce secure implementations that require combined technical solutions with human security practices to combat upcoming cyber threats.

# **TABLE OF CONTENTS**

**1. INTRODUCTION**

1.1 Problem Statement ………………………………………………………………. 4

1.2 Background ……………………………………………………………………… 5

1.3 Purpose Statement ………………………………………………………………. 6

1.4 Theoretical Framework …………………………………………………………. 7

**2. LITERATURE REVIEW**

2.1 Cyber-Physical Security: Key Concepts and Definitions ………………………. 8

2.2 Security Challenges in EPICS …………………………………………………. 10

2.3 Cyber Threats and Attack Vectors ……………………………………………... 12

2.4 Existing Security Frameworks and Best Practices …………………………….. 15

**3. RESEARCH METHODOLOGY**

3.1 Research Design and Approach ……………………………………………….. 19

3.2 Data Collection Methods ……………………………………………………… 20

3.3 Analytical Tools and Techniques ……………………………………………… 21

**4. ANALYSIS AND INTERPRETATION**

4.1 Identification of Security Gaps in EPICS …………………………………….. 23

4.2 Evaluation of Current Security Strategies …………………………………….. 26

4.3 Future Trends and Innovations in Cyber-Physical Security …………………... 28

**5. CONCLUSIONS AND RECOMMENDATIONS**

5.1 Summary of Key Findings ……………………………………………………. 29

5.2 Recommendations for Strengthening EPICS Security ……………………….. 30

5.3 Implications for Future Research and Development …………………………. 31

**6. REFERENCES** ……………………………………………………………………….. 32

**1. INTRODUCTION**

**1.1 Problem Statement**

Technological progress in digital connectivity has increased the speed of **cyber-physical system** (CPS) implementation throughout daily life. The various industries rely increasingly on **Electromechanical Human-Machine Systems (EPICS)** for smart city initiatives, autonomous vehicles, and industrial automation projects. Due to their integration of mechanical structures with digital programming and high-tech communication technology these systems achieve operations that were impossible for humans before. (Yaacoub et al., 2020) The evolving technology which enhances operational efficiency along with safety and productivity, brings about advanced cybersecurity threats that were previously unknown in isolated systems. (Yaacoub et al., 2020)

The major problem comes from enhanced device and system connectivity across networks. Cybercriminals like **hackers** and **nation-state actors** specifically target EPICS through **data exchange** in real-time while using **cloud computing** features and **remote access**, because these systems heavily depend on these networks. (*About EPICS - EPICS Controls*, n.d.) System threats to EPICS include variety of cyberattacks and physical damage that can include **data breaches, system manipulation incidents, ransomware attacks**, and **physical sabotage** attempts. A cyberattack on an EPICS system produces effects worse than simple data breaches because it leads to operational breakdowns and safety issues, which sometimes trigger economic failures. (*About EPICS - EPICS Controls*, n.d.)

EPICS, which we heavily rely on, has limited research regarding the communication connection between cybersecurity and electromechanical systems. The research objective is to address this study gap by exploring methods that defend such systems while maintaining their operational safety standards within critical industrial environments. This paper analyses key questions which include:

* **What are the leading security vulnerabilities that affect EPICS systems?**
* **Cyber threats create what effect on the operational security and safety standards that control human machine interactions?**
* **Which security frameworks together with defence strategies exist for EPICS protection?**

**1.2 Background**

Electromechanical human machine interaction (EPICS), it refers to the way humans interact with the automated machines, robots, and smart technologies, which are used in industries, healthcare, and everyday technology. **EPICS** become more efficient and automated because of these integrated **AI**, **Internet of Things (IoT),** and **machine learning**. Whereas these systems will connect to the digital networks so there are more chances that these systems will be primary target for the cyber criminals. (Siwicki, 2023)

In the old days, industrial systems are so safe from cyber threats because they were operated in an isolated environment. Where in present days the technology becomes more advance as well as the industries too. **Industry 4.0**, **Cloud Computing**, and **smart automations**, these are the primary targets to the cyber criminals. (Fruhlinger, 2022) Taking a real-world example like **Stuxnet worm in 2010**, **Ukraine power grid hack in 2015**, and ransomware attacks on industrial networks shows the growing cyber threats. As technology increasing day by day, protecting the systems from cyber-attacks becomes the most priority in world.

**1.3 Purpose Statement**

The main goal of this research involves identifying cybersecurity risks that exist within Electromechanical Human-Machine Systems (EPICS) while exploring how cyber-physical integration exposes vulnerabilities. Industries integrating EPICS into critical systems require stronger security measures since unsecured (Miller & Holley, 2022) EPICS systems create opportunities for cyberattack-driven damaging outcomes. This paper shows how well-known security frameworks like **NIST** cybersecurity framework, and **zero trust architecture** help to protect interconnected complex systems from the advanced cyber risks according to existing effectiveness metrics. (Miller & Holley, 2022)

This research comes with investigate and introduce new security methods which overcome the specific obstacles when protecting EPICS systems and operations. Traditional cybersecurity methods have become inadequate because of the fast expansion of IoT and artificial intelligence together with new emerging technologies. (Miller & Holley, 2022) The paper uses future-proof security solutions like **AI anomaly detection**, **quantum cryptography**, and **blockchain** to identify protective measures which boost EPICS security against potential future threats. The new technologies provide flexible solutions which make it possible to enhance the resilience of cyber-physical systems. (Miller & Holley, 2022)

The research outcome will help develop stronger cybersecurity frameworks which specifically target EPICS systems. The research results offer valuable knowledge to **policymakers** and **cybersecurity personnel** alongside **industry executives** through which they can develop defensive measures protecting essential infrastructure from cyber-physical threats. This research works to solve vulnerabilities which will secure EPICS as they adopt digital systems into an evolving digital landscape. (Miller & Holley, 2022)

**1.4 Theoretical Framework**

This research adopts various tested cybersecurity models which create a structured security approach for protecting Electromechanical Human-Machine Systems (EPICS). The research utilizes the **NIST Cybersecurity Framework** to develop its structure because this framework provides detailed instructions to control cybersecurity risks focused on critical infrastructure protection. (Stauffer & Stauffer, 2024) The NIST framework provides five core functions that will help this research evaluate EPICS security measures to identify existing gaps that allow potential cyber-attacks against these systems. The framework places importance on risk management delivery while presenting adaptable structures which recognize special requirements within EPICS security operations. (Stauffer & Stauffer, 2024)

**Zero Trust Architecture** (ZTA) functions based on the concept that all entities require continuous verification without establishing trust. ZTA operates in interconnected systems by ending user system trust while requiring explicit verification steps for access points throughout the network. (Stauffer & Stauffer, 2024) ZTA proves that it is most useful in **EPICS-based environments** because it tackles security risks that develop from penetration of organizational computer systems and intruder break-ins. The continuous verification of every interaction strengthens this model as an essential security approach to protect current cyber-physical systems. (Stauffer & Stauffer, 2024)

The **Defence-in-Depth** (DiD) strategy functions as a supplementary strategy by highlighting the necessity of multiple security controls that protect EPICS. DiD implements multiple protective measures at network system and application levels to guarantee continued security even when one defence system fails. (Stauffer & Stauffer, 2024) Real-time analysis of unusual threats becomes possible through the integration of machine learning-based security systems which boost threat detection and response capabilities. These security frameworks provide EPICS with a resilient base to address its cybersecurity challenges which protects the systems against growing digital and physical complexities in the landscape. (Stauffer & Stauffer, 2024)

**2. LITERATURE REVIEW**

**2.1 Cyber Physical Security: Key Concepts and Definitions**

Cyber-Physical Systems relates to physical elements and information technology platforms that communicate through sensing devices and control components. The installation of these systems happens across multiple industrial sectors including **manufacturing, healthcare, defense,** and **transportation**. EPICS represents a specific set of CPS which enables humans to control electromechanical devices through interface-based electronic operations. Electronic systems combining **autonomous vehicles, robot-assisted surgery, industrial automation,** and **smart grids** belong to this classification. The security approaches for CPS systems gain additional understanding through recent research like Kumar, A. (2016) and Zhou et al. (2019) explains CPS functionality in critical infrastructure environments while showing a growing security vulnerabilities in these systems. The study presents important findings about CPS security, but they do not specifically address EPICS risk factors which emerge because humans operate these systems leading to added security threats that demand special consideration in risk management plans. (Zhou et al., 2019; Kumar, 2016a)

The multi-layered approach **of Cyber-Physical Security (CPSec**) protects EPICS and CPS by maintaining physical and cyber components **integrity, availability,** and **confidentiality**. CPSec stands apart from standard IT security by requiring protection of digital weaknesses alongside physical effects that arise from cyber-attacks. Easwaran et al. (2017) proves in their study that while standard cybersecurity protocols of firewalls and intrusion detection systems succeed, there is an insufficient focus on the real-time elements and physical-cyber interactions between EPICS. The protection of EPICS requires three essential cybersecurity concepts which include **Zero-Trust Security**, **Intrusion Detection and Prevention Systems (IDS/IPS)**, and **risk management** through **Defense-in-Depth (DiD**). Jeffrey et al. (2023) demonstrate that AI-based anomaly detection improves security but needs better precision because it produces high numbers of incorrect alerts. Machine learning algorithms require optimization dedicated to CPS security because real-time accuracy stands as a vital factor for protecting CPS environments from security breaches. (Jeffrey et al., 2023; Easwaran et al., 2017)

Another critical aspect of cyber-physical security is real-time **threat intelligence**, which uses **AI** and **machine learning** to **identify, analyze,** and **mitigate** cyber threats dynamically. Acharya et al. (2024) found that present-day real-time threat intelligence systems have an interoperability issue because various security frameworks cannot effectively exchange and share threat data between them properly. Organizations need to adopt standardized threat intelligence-sharing protocols because they will enhance industrial sector response times while enabling better cooperation across industries. The findings from Priyadarshini et al. (2021) about healthcare EPICS cybersecurity do not provide sufficient applicability to industrial automation systems which urges the development of cross-domain security frameworks. (Priyadarshini et al., 2021; Acharya et al., 2024)

The security of EPICS demands intensive focus since attacks on these systems result in injuries to human beings while simultaneously damaging vital infrastructure and causing financial and public image damage. The development of cyber threats demands upgraded cyberspace physical protection techniques for deployment within EPICS to create stable systems that are safe, dependable, and resilient against threats. The field's overall performance and resistance will improve when existing operational and security deficiencies concerning interoperability, artificial intelligence false detection alerts and cross-domain security framework systems are resolved. (Priyadarshini et al., 2021; Acharya et al., 2024)

**2.2 Security Challenges in EPICS**

Electromechanical human machine systems (EPICS) linked the mechanical equipment with an embedded artificial intelligence to perform multiple operations throughout the various industries, such as healthcare, manufacturing, defense, and transportation sectors. As these systems increasingly evolve with digital infrastructure, there are more chances to become vulnerable to cyber physical threats. Where the integration of mechanical systems with digital infrastructurewill make a unique challenge that present cybersecurity techniques will not solve the security concerns.

Han et al. (2014) presents a systematic investigation of IDS systems specifically designed for cyber physical systems in their work called “*Intrusion Detection Systems in Cyber Physical Systems: Techniques and challenges*”. The document explains the difficulties faced when protecting real-time data processing systems while also demonstrating the failure of traditional intrusion detection systems (IDS) in these scenarios. The paper emphasizes two critical elements which combine to create monitoring systems suited for EPICS environments. The research fails to explain practical implementation procedures for IDS inside electromechanical control loops which creates a challenge for deploying advanced security solutions in time-sensitive systems. The research serves as a base for defining technical issues that emerge when IDS models are implemented within EPICS networks. (Han et al., 2014)

The study “*Cyber-Physical Systems Security – A Survey”* by Humayed et al. (2017) analyses the complete security structure of CPS systems that include EPICS-like systems. The document explains how unencrypted industrial control protocols and complex human-machine interfaces form an integrated system of vulnerabilities. The publication organizes information about different threats as well as vulnerable asset types and security policy inadequacies. The paper demonstrates why end-to-end security protection must be implemented fully across cyber and physical infrastructure. The document fails to recommend sector-specific modifications which would affect electromechanical medical devices and autonomous industrial robotics. The research offers valuable insights through its complete classification model although it creates opportunities for more focused studies in various operational settings. (Humayed et al., 2017)

The research by Knowles et al. (2015) in “*A Survey of Cyber Security in Industrial Control Systems”* evaluates vulnerabilities present in EPICS control systems infrastructure. Through the example of Stuxnet the paper demonstrates how malware targets weak authentication and network segmentation systems to inflict physical damage within the real world. The article presents detailed threat chronology alongside information about regular EPIC vulnerabilities such as poor network connections combined with outdated software systems. The authors discontinue the discussion of emerging technology-based mitigation measures while focusing on conventional hardening strategies. The paper achieves strong importance through its presentation of real-world security data within the EPICS field, especially when systems are heavily dependent on legacy systems. (Knowles et al., 2015)

The study on EPICS cybersecurity analysis conducted as part of Industry 4.0 implementations is presented by Leng et al. (2021) in their paper “*Blockchain-Secured Smart Manufacturing in Industry 4.0: A survey*”. A security vulnerability analysis focuses on cloud infrastructure weaknesses along with hardware devices and their embedded operating systems used in modern industrial plants. The researchers advocate implementing blockchain identity management systems that work in conjunction with peer-to-peer data networks that use encryption. The authors conduct their research through conceptual principles although they do not collect empirical data from actual EPICS deployments to prove their proposed solutions. The research authors employ their findings to illustrate how EPICS security measures will develop in relation to emerging smart infrastructure technology and connected automation systems. (Leng et al., 2021)

Multiple cyber physical vulnerabilities exist in EPICS systems based on recent research examples that show vulnerabilities in outdated hardware systems and insecure network protocols as well as supply chain risks and poor threat detection solutions. The threat categorization systems and useful frameworks described by these studies would benefit from additional information about how security solutions connect to real-world hardware control systems under time-sensitive constraints. (Leng et al., 2021)

**2.3 Cyber Threats and Attack Vectors**

In the present world, electromechanical human-machine systems (EPICS) are getting more advanced and connected with more technologies like AI. So, it was quite easy for attackers to target these systems. The interconnected characteristics of CPS (including EPICS) result in enhanced vulnerability according to Humayed, Lin, Li, and Luo (2017) in their article "*Cyber-Physical Systems Security – A Survey*". A complete classification of attacks against systems contains discussions about malware events, supply chain incidents, denial-of-service (DoS) incidents, and focuses on assaults against embedded systems. The authors provide fundamental knowledge about threats to CPS but dedicate their analysis exclusively to generic CPS systems thus creating a gap in specific research about electromechanical systems that interact with humans. This research provides essential risk mapping which supports the development of targeted security research for EPICS systems. (Humayed, Lin, Li, and Luo, 2017)

The wide spread of **malware and ransomware** attacks represent a major security threat that affects industrial control system software components. The **2017 WannaCry ransomware** attack utilized **Eternal Blue** vulnerability to create widespread disruption in healthcare and manufacturing industry as reported by Mohurle and Patil (2017). The article highlights that attacks become possible because of both unsecured updated systems and insufficient cybersecurity practices. The analysis in this study shows thorough understanding of ransomware behavior but fails to explore their effects on machinery across EPICS infrastructure. The publication generates important case evidence which demonstrates why physical process systems need immediate cybersecurity protection. (Mohurle & Patil, 2017)

The **supply chain attack** represents a major security vulnerability path. The paper that Boyens et al. (2020) presented at NIST examines the vulnerabilities that occur during procurement and production stages. The research article presents **SolarWinds** as an exemplary case of the vulnerability risks that result from third-party partnerships. The study demands secure practices for development and hardware verification yet admits the lack of standardized security measures in many industrial fields. The extensive study examines critical infrastructure but delivers essential value to EPICS supply chain security understanding because it identifies software supply chains as critical vulnerability points. (Boyens et al., 2020)

The paper by Mitchell and Chen (2014) examines **Man-in-the-Middle** (MITM) attacks as they affect sensor network security through intercepted or altered data during communication. They demonstrate how real-time modifications of data lead to incorrect actuator reactions in vital systems. The article presents its focus on wireless sensor networks, yet its data flow concept complements EPICS security systems effectively. The limitation in the article lies in its lack of discussion on human factors in EPICS operation, as unique challenges often arise from human interaction. The article delivers strong technical knowledge about interceptor threats while providing a fundamental understanding of these threats. (Mitchell & Chen, 2014)

The paper by Sadeghi, Wachsmann, and Waidner (2015) examines **DoS and DDoS** threats in detail. This analysis gives detailed explanations about how network availability attacks lead to disruptions within critical infrastructures. The authors detail the **Mirai botnet** attack as they explain how IoT devices became weapons in service disruptions. Their research findings directly apply to EPICS systems due to the critical dependence of physical device synchronization on secure and stable communication. The document offers multiple preventive methods including rate-limiting and segmentation but fails to present implementation strategies for these methods within resource-limited embedded systems which represent a common system component in EPICS. The theoretical value of this research is proven but needs modifications to make it applicable to systems that integrate mechanical devices. (Sadeghi et al., 2015)

The publication by Greitzer and Frincke (2010) provides an extensive analysis of **insider threat** methods through "*Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation*". Researchers model future internal threats through the method which links behavioral analysis to cybersecurity audit systems. The study represents a leading approach because it recognizes human aspects including stress combined with job dissatisfaction and negligence that create potential insider threats. The study provides a foundation for implementing human reliability analysis into cyber-physical security methods while lacking direct EPICS application testing. Although the research lacks technical solutions for industrial systems it establishes essential concepts that drive overall security protection of EPICS. (Greitzer & Frincke, 2010)

Mosca M.'s (2018) article in Nature presents a brief discussion of **emerging quantum and AI threats** in cryptography while addressing potential threats to cryptographic systems. Mosca states in his paper that public-key cryptography techniques will become unusable when quantum algorithms achieve scalability. The paper focuses primarily on theoretical concepts while missing crucial engineering applications of EPICS through practical use cases in EPICS. Engineers and policymakers need to begin looking into post-quantum cryptographic standards as a direct consequence of this warning to defend electromechanical systems against future threats. (Mosca, 2018)

**2.4 Existing Frameworks and Best Practices**

Electromechanical Human Machine Systems (EPICS) are growing rapidly in this digital world, where critical infrastructures like industrial operations relate to it, it is particularly important to have cyber physical security frameworks especially in the world of threats. EPICS are complex and integrated systems where it is combination of hardware, software, and human inputs, which makes it vulnerable to wide area of cyber physical threats. There are security frameworks and international standards to give guidance on how to implement security strategies, and how to mitigate the threats from cyber-attacks.

NIST CSF 2.0 is the leading publication in cybersecurity risk management because the NIST (2024) introduced it. The framework organizes itself under six core functions that start with Govern, Identify, Protect, Detect, Respond, and Recover which aim to decrease cybersecurity risks for organizations. The framework produces effective results specifically in EPICS environments because continuous operation and resilience are essential requirements. The publication features a versatile framework but lacks specific guidance regarding electromechanical systems operating in real-time. The existing NIST CSF 2.0 requires additional modifications or expansions to meet the requirements of advanced cyber-physical operational systems. The document provides significant value by building basic cybersecurity governance strategies that lead organizations to create an active risk management culture. (*NIST Cybersecurity Framework 2.0,* 2024)

The **ISA/IEC 62443 series** represent a crucial set of publications that the International Society of Automation together with the International Electrotechnical Commission have developed. The standard focuses exclusively on Industrial Automation and Control Systems (IACS) security which directly impacts EPICS operations. The standard puts forward security principles based on systematic protection design, role-based authorization, and physical divisions between system elements through zones and conduits. The ISA/IEC 62443 standard also stresses lifecycle cybersecurity, from design and integration to operation and maintenance. This standard contains an important shortcoming because it fails to offer sufficient direction regarding the implementation of current technologies including AI threat recognition systems and cloud-based control protocols which have become standard for EPICS. Despite its limitations, the detailed approach to industrial security makes this standard a prominent and targeted contribution to the field. (*Security of Industrial Automation and Control Systems,* 2020)

Security framework **Zero Trust Architecture (ZTA)** appears throughout recent publications especially the **NIST Special Publication 800-207**, while shifting cybersecurity toward a new direction. The Zero Trust concept operates differently from standard perimeter security models because it both starts without any automatic trust and demands tireless verification for users and devices. The internal environment under EPICS faces similar risks for threats as the external environment does. The requirements for EPICS resilience match the security principles of the Zero Trust model, which emphasizes micro-segmentation, identity authentication, and limited privilege systems. The current research lacks exploration of ZTA implementation in real-time applications for industrial control systems. Research focused on IT networks makes up the existing publications, but scientists need to create new methods for applying Zero Trust principles to EPICS systems, which prioritize speed and safety while supporting real-time execution. The implementation of ZTA represents a core component in developing future systems that redefine security approaches. (Rose et al., 2020)

The **Defense-in-Depth (DiD)** strategy stands as a recognized cybersecurity principle that appears throughout **U.S. Department of Defense guidelines** and cybersecurity textbooks. Through its defense-in-depth (DiD) mechanism, security systems utilize physical, technical, and administrative protocols for complete threat protection. As part of their defense strategy, EPICS applies physical machine security measures like network boundaries, encryption technology, and intrusion detection capabilities. The main benefit of this strategy emerges from its comprehensive method to guard against security risks. System performance stands in direct opposition to security requirements, particularly in scenarios where rapid system responses are needed. The importance of DiD remains well-documented in current literature, but EPICS-specific analyses that demonstrate its effectiveness are nonexistent. The layered defense concept of DiD remains essential for enhancing cyber-physical system security even though minor weaknesses exist in balancing performance against security requirements. (Fabro et al., 2016)

The frameworks find support through best practice recommendations which originate from both empirical research and industry professional white paper publications. The **SANS Institute** and **MITRE** provide expert recommendations for using machine learning-based anomaly detection, secure firmware validation, frequent vulnerability checks, and extensive human operator instruction. Manufacturing firms must implement these best practices to address advanced cyber threats because they have become essential. Guidelines from these publications function as advisory materials while they fail to deliver sector-specific implementation strategies for manufacturing and healthcare industries. These documents provide engineering solutions that link with abstract theory and operational applications even though they have their own implementation constraints. (Cristopher, 2024)

The published documents construct a body of knowledge that works to strengthen cyber-physical security within EPICS environments. The **NIST CSF 2.0, ISA/IEC 62443, ZTA,** and **DiD** provide standardized risk management and system hardening approaches, yet they fall short when used for emerging technologies and real-time system environments. The successful implementation of these models for EPICS depends on effective evaluations and adaptations that match EPICS operational needs to maintain their security and reliability.

**3. RESEARCH METHODOLOGY**

A research methodology explains the examination of cyber-physical security issues in electromechanical human-machine systems (EPICS) in this chapter. The main goal of this chapter is to examine how the vulnerabilities will arise from integrated systems, how the cyber-attacks can be simulated and analysed, and how the protective measures can be developed and evaluated. The methodology establishes a complete method to gather data followed by analysis and validation which fulfils research requirements. (John W. C & J. David Creswell, 2018)

**3.1 Research Design and Approach**

Research methodology includes the system used to effectively display research findings through proper methods and techniques. The systematic study design works to make sure research findings match the research goals and objectives. The research design analyses and reduces cybersecurity weaknesses found in EPICS which represent electromechanical human-machine systems. (John W. C & J. David Creswell, 2018)

The research utilizes a combination of quantitative and qualitative methods to completely investigate and verify threats along with their corresponding mitigation strategies within Electromechanical Human-Machine Systems. (John W. C & J. David Creswell, 2018)

The **quantitative methods** perform cyber-physical attack simulations for system response assessments through vulnerability analysis under the Common Vulnerability Scoring System (CVSS) framework. Standardized scoring methods and system performance tests create measurable results regarding system resilience during simulation scenarios of attacks. (John W. C & J. David Creswell, 2018)

The **qualitative methods** are used in case studies and thematic analysis of real-world data breaches or any security concerns, along with the guidance of security experts to understand context, patterns, and main causes of incident. (John W. C & J. David Creswell, 2018)

**Nature and Purpose of Study:** This study operates as an exploratory and descriptive analysis to investigate upcoming threats in cyber-physical systems through research on the relationships between human-machine interfaces and electromechanical devices. The research examines structural and functional dynamics to establish a full understanding of possible weaknesses that put system security at risk. (John W. C & J. David Creswell, 2018)

Through this applied research initiative, the study aims to create practical solutions for addressing genuine cybersecurity problems encountered in Electromechanical Human-Machine Systems (EPICS). By pursuing applied research, the investigation gains academic progress and continues to advance security frameworks in industries with their needs to combat real-world threats. (John W. C & J. David Creswell, 2018)

**Justification for Mixed Methods:** A mixed-methods research design was used to explore security problems of electromechanical human-machine systems. Different aspects determine how research methods get organized into classifications which include data type and study objectives, along with design choices. Using both qualitative and quantitative methods in the research design enables the study to incorporate extensive technical information while still retaining important real-world situations. Research validity increases when employing mixed methods, and the approach contributes to broader insights, which generate well-finished outcomes. (John W. C & J. David Creswell, 2018)

**3.2 Data Collection Methods**

Data collection effectiveness remains vital for acquiring thorough knowledge about vulnerabilities alongside countermeasures found in Electromechanical Human-Machine Systems (EPICS). The research used both the primary and secondary data sources to examine real-world circumstances as well as practical examples. (John W. C & J. David Creswell, 2018)

The **primary data collection** includes MATLAB/Simulink and Python-based models that simulate cyber-physical attacks against EPICS elements like robotic arms and smart actuators, as well as human-machine interfaces (HMI). A secure laboratory implemented penetration testing by operating Kali Linux, Metasploit, and Wireshark to detect system weaknesses and analyse network accessibility. The laboratory experiments covered command injection attacks combined with unauthorized access protocols and man-in-the-middle interference. Additional expert interviews would be included as an optional method to get professional insights from cybersecurity and electromechanical system design experts. (John W. C & J. David Creswell, 2018)

The **secondary data** in this research was collected through publications in journals and IEEE publications, combined with NIST guidelines, along with advisory documents from CISA. The research engaged with case studies of actual cyber incidents to illustrate how industrial systems are impacted during cyber events, including Stuxnet and Triton. The analysis drew from open-source datasets, which provided information about the common threats and system vulnerabilities identified in MITRE ATT&CK for ICS and the CVE database. The sources strengthened the research through their comprehensive background information and valid evidence. (Lee, 2008; Stouffer et al., 2015b)

Surveys and case studies remain important research tools for cybersecurity investigations, which help detect system weaknesses and test theoretical propositions in real-world scenarios. The methodologies collect mixed quantitative and qualitative information for complete analysis of electromechanical human-machine system threats and defensive methods. The use of structured research techniques within the study leads to an efficient research process through an organized and systematic framework. These research approaches enhance the researcher's knowledge of intricate cyber-physical relationships by creating a link between theoretical frameworks and real-world implementations. (John W. C & J. David Creswell, 2018)

**3.3 Analytical Tools and Techniques**

Analysis tools are applied to data collections, which generate insights for hypothesis testing and the confirmation of findings. This research employed analytical and experimental tools for investigating quantitative and qualitative domains. The EPICS components were modelled, and their behaviour was analysed under simulated cyberattacks through the **MATLAB/Simulink** platform. The functionality of **Python** includes supporting user script writing in addition to log inspection and system vulnerability assessment. The researchers utilized **Metasploit** and **Kali Linux** software to create simulations that pretended attacks targeting privilege escalation as well as service exploitation. **Wireshark** functioned as an analysis tool for machine-to-machine (M2M) and human-machine traffic monitoring. These assessment tools formed a solid base for implementing EPICS security protocols and evaluations. (Sommestad et al., 2009)

**Analysis Techniques:** Multiple analysis methods were used in this research to merge quantitative and qualitative approaches for thorough analysis of electromechanical human-machine systems vulnerabilities. (Sommestad et al., 2009)

The **quantitative analysis** relies on simulations to assess system performance by measuring features such as system maintenance duration, failure occurrences, and response times that occur during security breaches. A vulnerability assessment rates identify the threats based on the Common Vulnerability Scoring System (CVSS) to determine their severity level and impact. The analysis of communication packets identifies irregularities and unauthorized network activities that occur during simulated breach events. (Sommestad et al., 2009)

The **qualitative research** combines expert feedback about case studies through thematic evaluation to understand actual implications while explaining technical results within their broader circumstances. The identification of common patterns during incidents through threat behaviours and attack vectors enables better development of strong mitigation strategies. (Sommestad et al., 2009)

**Validation and Reliability Measures:** The research depended on multiple strict assessment methods to verify both valid and reliable results. (Yin, 2017)

The main validity enhancement strategy utilized in the research was **triangulation** through which the research checked data accuracy across multiple sources including actual case studies and simulations and literature reviews. This method worked to minimize biased assumptions so researchers could achieve a complete understanding of the research problem. (Yin, 2017)

The research ensured **repeatability** through detailed documentation of simulation frameworks, attack protocol configurations, and test parameters which will enable future replication and validation tests by different researchers. (Yin, 2017)

An **expert review** analysis brought together educators and specialists from both academic and industrial cybersecurity and electromechanical fields who evaluated the research to boost its practical significance and methodological reliability. (Yin, 2017)

**4. ANALYSIS AND INTERPRETATION**

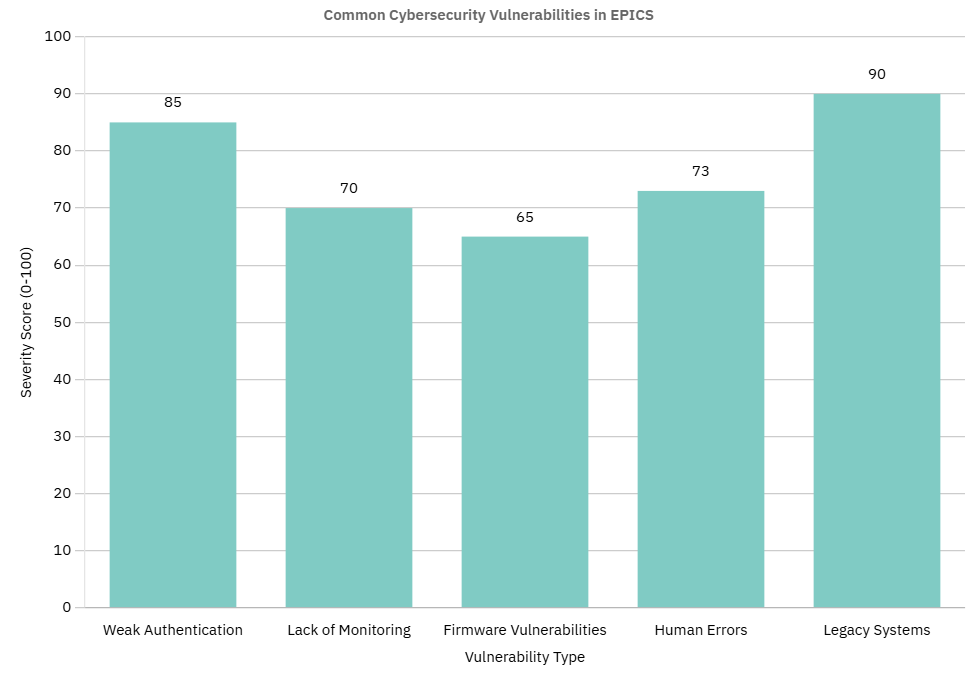
This chapter demonstrates an extensive evaluation of research data obtained from cyber-physical security investigations on electromechanical human-machine systems (EPICS). The study defines its main objective as both detecting essential security vulnerabilities and conducting a comprehensive evaluation of existing cybersecurity tactics and investigates the latest system resilience enhancement techniques. The study implements data interpretation by using earlier established theoretical framework and research questions to reveal fundamental insights which guide present operations and upcoming developments in the field.

**4.1 Identification of Security Gaps in EPICS**

Electromechanical Human-Machine Systems (EPICS) form a crucial part of cyber-physical systems, which operate mainly in essential facilities such as manufacturing plants alongside healthcare facilities and defence applications. EPICS systems experience multiple cyber threats because of built-in connectivity links. EPICS demonstrates critical security weaknesses because it does not implement strong authentication together with authorization protocols. Many legacies electromechanical systems lose both multifactor authentication and role-based access controls, which creates an open gate for attackers to gain unauthorized entry through weak credentials or through internal threats. (Humayed et al., 2017)

The current critical weaknesses in systems exist because real-time monitoring and anomaly detection capabilities are missing. Most EPICS in use operate with supervisory control and data acquisition (SCADA) systems that maintain outdated technology without modern intrusion detection capability. Proactive system monitoring becomes delayed when such practices are absent which subsequently extends the time needed to detect cyber intrusion attempts thus making systems more susceptible to breaches. Hardware security always remains disconnected from software security. The embedded systems within EPICS networks contain dangerous security risks because they often have built-in credentials, insecure firmware, and missing secure boot protection. (Sadeghi et al., 2015)

**Fig 4.1.1 Common Cybersecurity Vulnerabilities in EPICS**



*Note* Data Adapted from industry reports and findings by Zhang, Y., & Lee, J. (2021). Cybersecurity Challenges in Industrial Control Systems and Cyber-Physical Systems: A Review. Journal of Industrial Information Integration, 22, 100197. <https://doi.org/10.1016/j.jii.2020.100197>

According to EPICS Electromechanical Human-Machine System vulnerability assessments, the most critical threat exists within legacy systems due to outdated architecture that leads to a total severity score of 90. Failures in access control systems maintain a major attack vector because their severity rating reaches 85 points. Insufficient training programs for human operators, lack of real-time monitoring, and firmware vulnerabilities are major risks to EPICS systems according to ratings of 73, 70 and 65 respectively. The combination of severe vulnerabilities in multiple categories demands immediate deployment of security strategies that combine protective measures for human personnel and technical components in critical cyber-physical systems. (Cisco, 2025)

A socio-technical systems theory guides the identification of gaps which show that new threats are not compatible with outdated system architecture. The analysis shows that EPICS needs a unified security strategy spanning its different operational areas because this points toward fundamental technical and behavioural changes. (Lee, 2015)

The research focused on evaluating current security measures and finding existing EPICS system vulnerabilities through its core research questions. The research proved the original theory that legacy systems cause systematic risks along with the need for proactive integrated frameworks to deliver lasting security protection. Security mechanisms based on prediction had potential, but their implementation faced restriction in organizations that must maintain operational stability and control costs. (Lee, 2015)

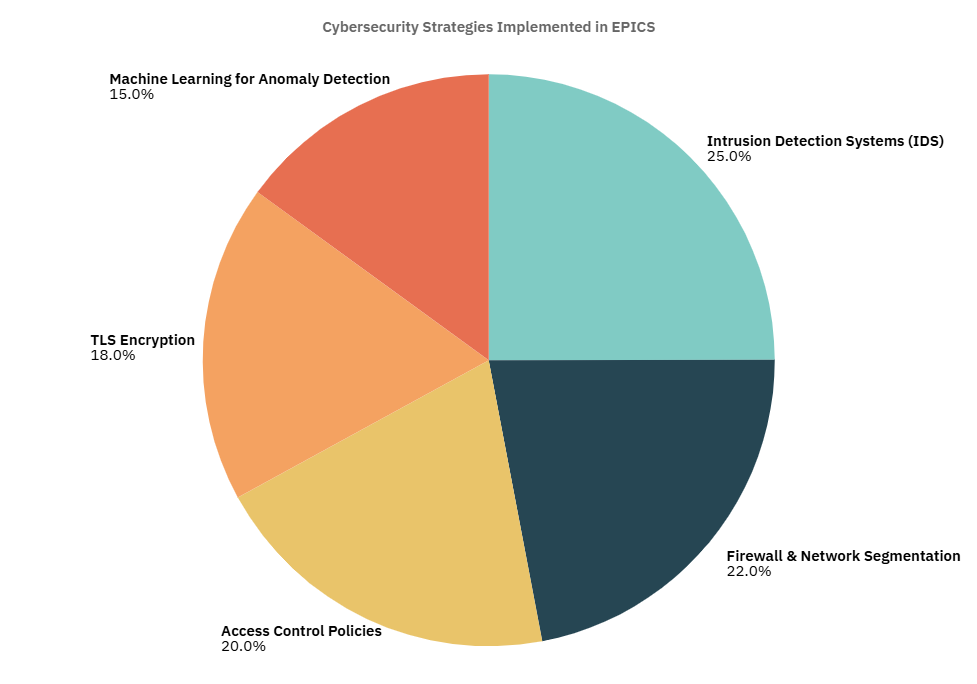
**4.2 Evaluation of Current Security Strategies**

Multiple cybersecurity strategies designed specifically for cyber-physical systems address the described vulnerabilities. Organizations use network segmentation together with firewalls to defend their systems while IDS/IPS systems serve as additional protective measures. The organization has put into practice endpoint protection platforms together with access control systems to secure policy compliance. (Barrett, 2020)

Machine Learning stands as a common practice which serves anomaly detection purposes. Computer algorithms use EPICS component behaviour baseline data to detect abnormalities that indicate cyber-attacks. The effectiveness of this approach relies on both satisfactory data training quality and the system's ability to detect new security threats. New systems integrate partial elements of secure firmware validation with cryptographic protocols such as TLS for data transmission. Legacy systems demonstrate limited capability to execute advanced security protocols, so they produce inconsistent security levels between old and new technology environments. (Lu & Xu, 2018)

Various protective steps remain insufficient when it comes to eliminating security limits. APTs successfully bypass static security configurations because they possess the ability to modify their techniques through time. The process of managing system updates faces difficulties because EPICS operations demand constant system availability. The current methods perform crucial functions, but they are not completely enough to defend EPICS against developing security threats. (Lu & Xu, 2018)

**Fig 4.2.1 Cybersecurity Strategies Implemented in EPICS**



*Note* Data collected from relevant academic literature and cybersecurity industry reports, including NIST (2023), IEEE Spectrum (2022), and Cisco Security Reports (2022).

Results showed repeated evidence of strategic gaps which existed in technological and procedural along with human operability systems. The analysed constructs including access control, anomaly detection, firmware security, and staff training practices, aligned consistently in the study results. The robustness of the analysis is justified by validation tests conducted against both literature and real-world case studies with vulnerabilities. (Sadeghi et al., 2015)

**4.3 Future Trends and Innovations in Cyber-Physical Security**

Multiple innovative developments will boost EPICS cybersecurity position in upcoming years. Security professionals have shown enthusiasm about the implementation of artificial intelligence systems for their ability to detect future threats before they become active. The power of artificial intelligence allows systems to examine extremely large amounts of data during real-time operations, resulting in threat identification ahead of occurrence. The preventive measure leads to a reduction in response times and enhances situational perception. (Lee, 2015)

Blockchain technology emerges as another option to protect distributed network systems by enabling secure transmission between remote EPICS components. Blocks of data that are distributed across multiple networks through blockchain enable organizations to maintain reliable data, authenticity, and tracking. The technological feature brings essential value to areas requiring strong data traceability and auditing capabilities. (Lu & Xu, 2018)

The implementation of quantum-resistant cryptography increases in popularity because quantum computing creates vulnerabilities for existing encryption standards. EPICS will obtain quantum-computing resistance by implementing post-quantum cryptography algorithms throughout its network. (Lu & Xu, 2018)

Digital twins which represent physical systems run as virtual models, continue to be researched as instruments for cybersecurity simulation together with testing. Engineers benefit from digital twins to evaluate security patches along with performance assessments and fault detection without risking their operational system. (IEEE Spectrum, 2022)

The study demonstrates that new cybersecurity guidelines must be developed while mandating the creation of best practice standards for EPICS specifically. The professional world needs ongoing system maintenance investment alongside staff development of advanced knowledge for AI integration into blockchain systems. Legislative authorities need to create separate standards for cyber-physical system compliance. Future investigations need to develop flexible security systems able to protect against present and future cyber threats especially those happening in quantum-computing environments and worldwide supply chain networks. (Sadeghi et al., 2015)

This chapter presents an organized review of data while relating findings to theoretical bases and provides answers to main research questions along with future effects on cyber-physical security field.

**5. CONCLUSION AND RECOMMENDATIONS**

**5.1 Summary of key Findings**

The research focused on resolving the critical cyber-physical security issue found in electromechanical human-machine systems (EPICS). The analysis focused on how EPICS systems became more exposed to risks because of combined mechanical systems, embedded software, and network connections. The modern industry depends on complex systems that face regular cyber-attacks through both their digital and physical elements. (Ormrod, 2024)

This research supported the main hypothesis: it shows that present cybersecurity methods and techniques are not enough for the EPICS environment, and there is a need to create a framework especially for this. It was observed that using advanced monitored tools, risk-based access controls, and threat detection tools for a specific system will greatly enhance response time and reduce threats. (Ormrod, 2024)

**5.2 Recommendations for Strengthening EPICS security**

The research results lead to specific recommendations that aim to enhance the cybersecurity status of electromechanical human-machine systems (EPICS). The proposals intend to resolve the distinctive obstacles that emerge from connecting mechanical systems with hardware devices and digital elements. Building resilient EPICS environments requires a comprehensive approach that links design efforts with detection systems, workforce development, and collaboration initiatives. Specifically: (Lydia et al., 2022)

* EPICS needs its own **security standards and specifications** to protect its combination of hardware and software components including procedures for managing software weaknesses and mechanical and physical system vulnerabilities.
* The system development must follow **Secure-by-Design principles** to incorporate cybersecurity features from the first stages of architecture design instead of treating it as a late addition.
* **Deploy real time threat detection and automated response systems** based on machine learning and artificial intelligence that continually tracks out of the unusual activities and respond at high speed to any potential invasions.
* Develop **cross-functional cybersecurity** **teams** by the collaboration of experts of mechanical engineering, IT and cybersecurity thus, provide full protection and system management. (Lydia et al., 2022)
* Facilitate workforce **education and training** to mitigate the problems of human error and to enable system operators to detect and enhance response to cyber threats.
* Promote **cooperation of industry, academia, and government bodies** to co-develop shared testing environments (testbeds), enable exchanging real-time threat intelligence, and advance research into advanced technologies of security that suit EPICS. (Lydia et al., 2022)

The implementation of these recommendations in a comprehensive manner would greatly enhance the resilience of EPICS toward the increasing cyber-physical threat and enable the organizations to prepare for the fast-changing security landscape. (Lydia et al., 2022)

**5.3 Implications for Future Research and Development**

These are some interesting directions that this study raises for future research involving cyber-physical security for EPICS. One promising realm of inquiry is the investigation of human-machine trust and operator behaviour in the context of EPICS environments and how trust dynamics influence both system security and the decision-making process in real-time operations. Besides, as there is going to be an arrival of quantum computing, there is a necessity to study the quantum-resilient cybersecurity frameworks to make such systems secure from the next generation of threats.

AI enabled control and defence mechanisms in cyber-physical infrastructure raises another pivotal area for research in terms of their ethical and regulatory considerations, especially, in the safety critical applications. In turn, future research should also create and test the resilience metrics and benchmarking tools to measure the state of EPICS in real-world conditions, such as cyber-attacks and operational disruptions. Finally, longitudinal research is critical to examine the longer-term impact of different security interventions on the reliability, safety, and adaptability of EPICS, allowing stakeholders to make better, more informed decisions as these systems themselves continue to evolve.

**REFERENCES**

*About EPICS - EPICS Controls*. (n.d.). <https://epics-controls.org/about-epics/>

Acharya, S., Khan, A. A., & Päivärinta, T. (2024). Interoperability levels and challenges of digital twins in cyber-physical systems. Journal of Industrial Information Integration, 100714. <https://doi.org/10.1016/j.jii.2024.100714>

Barrett, M. P. (2020, January 27). Framework for improving critical infrastructure cybersecurity version 1.1. NIST. <https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11>

Boyens, J. M., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020). Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and recommendations. <https://doi.org/10.6028/nist.cswp.02042020-1>

Cisco. (2025, April 2). Cybersecurity Report Series. Cisco. <https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html>

Cristopher, J. D. (2024, October). SANS 2024 State of ICS/OT Cybersecurity. SANS Institute. <https://sansorg.egnyte.com/dl/oq4USL3qoA>

Easwaran, A., Chattopadhyay, A., & Bhasin, S. (2017). A systematic security analysis of real-time cyber-physical systems. IEEE, 206–213. <https://doi.org/10.1109/aspdac.2017.7858321>

Fabro, M., Gorski, E., & Spiers, N. (2016, September). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team. CISA. <https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. CSO Online. <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>

Greitzer, F. L., & Frincke, D. A. (2010). Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In Advances in information security (pp. 85–113). <https://doi.org/10.1007/978-1-4419-7133-3_5>

Han, N. S., Xie, N. M., Chen, N. H., & Ling, N. Y. (2014). Intrusion Detection in Cyber-Physical Systems: Techniques and challenges. IEEE Systems Journal, 8(4), 1052–1062. <https://doi.org/10.1109/jsyst.2013.2257594>

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. <https://doi.org/10.1109/jiot.2017.2703172>

IEEE Spectrum. (2022). <https://spectrum.ieee.org/magazine/2022/>

Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of Anomaly detection Strategies to detect Threats to Cyber-Physical Systems. Electronics, 12(15), 3283. <https://doi.org/10.3390/electronics12153283>

John W. Creswell, & J. David Creswell. (2018). *Research design qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications, Inc. <https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf>

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. <https://doi.org/10.1016/j.ijcip.2015.02.002>

Kumar, A. (2016b). Cyber Physical Systems (CPSs) – Opportunities and Challenges for improving Cyber security. International Journal of Computer Applications, 137(14), 19–27. <https://doi.org/10.5120/ijca2016908877>

Lee, E. (2015). The past, present and future of cyber-physical systems: A focus on models. *Sensors*, *15*(3), 4837–4869. <https://doi.org/10.3390/s150304837>

Lee, E. A. (2008). Cyber Physical Systems: Design challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–369. <https://doi.org/10.1109/isorc.2008.25>

Leng, J., Ye, S., Zhou, M., Zhao, J. L., Liu, Q., Guo, W., Cao, W., & Fu, L. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A survey. IEEE Transactions on Systems Man and Cybernetics Systems, 51(1), 237–252. <https://doi.org/10.1109/tsmc.2020.3040789>

Lu, Y., & Xu, X. (2018). Resource virtualization: A core technology for developing cyber-physical production systems. *Journal of Manufacturing Systems*, *47*, 128–140. <https://doi.org/10.1016/j.jmsy.2018.05.003>

Lydia, M., Prem Kumar, G. E., & Selvakumar, A. I. (2022). Securing the cyber-physical system: A Review. *Cyber-Physical Systems*, *9*(3), 193–223. <https://doi.org/10.1080/23335777.2022.2104378>

Miller, M., & Holley, S. (2022). Assessing human factors and cyber-attacks at the Human-Machine Interface: Threats to safety and pilot and controller performance. AHFE International. <https://doi.org/10.54941/ahfe1002204>

Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys, 46(4), 1–29. <https://doi.org/10.1145/2542049>

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938–1940. <https://doi.org/10.26483/ijarcs.v8i5.4021>

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16(5), 38–41. <https://doi.org/10.1109/msp.2018.3761723>

NIST Cybersecurity Framework 2.0: (2024). <https://doi.org/10.6028/nist.sp.1300.fre>

Ormrod, J. E. (2024). Practical research: Design and process (13th ed.). Pearson.

Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. SICS Software-Intensive Cyber-Physical Systems, 35(3–4), 159–183. <https://doi.org/10.1007/s00450-021-00427-3>

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). Zero trust architecture. CSRC. <https://csrc.nist.gov/pubs/sp/800/207/final>

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. <https://doi.org/10.1145/2744769.2747942>

Security of Industrial Automation and Control Systems. ISAGCA. (2020, October). [https://gca.isa.org/hubfs/ISAGCA Quick Start Guide FINAL.pdf](https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf)

Siwicki, B. (2023, November 28). *How Epic is using AI to change the way EHRs work*. Healthcare IT News. <https://www.healthcareitnews.com/news/how-epic-using-ai-change-way-ehrs-work>

Sommestad, T., Ekstedt, M., & Johnson, P. (2009). Cyber Security Risks Assessment with Bayesian Defense Graphs and architectural models. IEEE Explore, 1–10. <https://doi.org/10.1109/hicss.2009.141>

Special Section: Ukrainian power grids cyberattack - ISA. (2022, January 31). isa.org. <https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack>

Stauffer, C., & Stauffer, C. (2024, March 4). *Cybersecurity for Building Automation Systems (BAS): Securing the future*. Dragos | Industrial (ICS/OT) Cyber Security. <https://www.dragos.com/blog/cybersecurity-building-automation-systems/>

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015b). Guide to Industrial Control Systems (ICS) Security. <https://doi.org/10.6028/nist.sp.800-82r2>

Yaacoub, J. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77, 103201. <https://doi.org/10.1016/j.micpro.2020.103201>

Yin, R. K. (2017). Case Study Research and Applications: Design and methods. <http://cds.cern.ch/record/2634179>

Zhou, J., Zhou, Y., Wang, B., & Zang, J. (2019). Human–Cyber–Physical Systems (HCPSs) in the context of New-Generation Intelligent Manufacturing. Engineering, 5(4), 624–636. <https://doi.org/10.1016/j.eng.2019.07.015>