SecureOps: Toward Resilience for Security and Privacy in Industrial Applications

1st RECS 2024 - 26-29 November 2024, Recife, Brazil

Hebert Silva
SENAI - GSTI
Sao Paulo, Sao Paulo, Brazil
hebert@sp.senai.br

Rodrigo Santos
SENAI - Anchieta
Sao Paulo, Sao Paulo, Brazil
rodrigo.vsantos@sp.senai.br

Oliver Guerino
SENAI - Informatica
S. C. do Sul, Sao Paulo, Brazil
oliver.silva@sp.senai.br

ABSTRACT

The SecureOps Lab was established to tackle cybersecurity challenges in Cyber-Physical Systems (CPS), Operational Technology (OT), and the Internet of Things (IoT). Despite the opportunities these technologies offer, their complexity makes them vulnerable to cyber attacks. The lab combines physical and virtual environments to develop, validate, and verify resilient security solutions, simulating real-world scenarios to ensure practical and robust outcomes using the Technology Readiness Level (TRL) framework. As a controlled environment, the lab explores vulnerabilities, tests defense mechanisms, and enhances resilience in security solutions. This work presents initial results and discusses a case study involving a Proof of Concept (PoC) of the Purdue Model using Fortinet's IoT Solution.

KEYWORDS

Resilience, Cybersecurity, Cyber-Physical Systems, Operational Technology, Internet of Things, Technology Readiness Level

1 INTRODUCTION

The integration of Cyber-Physical Systems (CPS), Operational Technology (OT), Internet of Things (IoT), and Industrial Internet of Things (IIoT) has transformed industrial processes, enhancing automation and efficiency. However, this connectivity also increases cybersecurity risks, potentially leading to severe disruptions, financial losses, and safety concerns. Addressing these vulnerabilities is essential for modern industrial operations, requiring resilient security solutions against evolving cyber threats.

To meet these challenges, SENAI São Paulo's Competence Development Center (CDC) in Advanced Manufacturing and Cybersecurity established the SecureOps Lab, a network of advanced labs that develop and validate security solutions for industrial applications. This initiative enhances resilience in CPS, OT, and IoT by conducting Proof of Concepts (PoCs) and testing models in controlled environments, contributing scalable solutions for both large and small enterprises.

The SecureOps Lab focuses on three main goals: i)Advancing Resilience Technologies through Technology Readiness Levels (TRL), progressing from theory to practical application with measurable outcomes. ii)Emphasizing Human Factors by integrating user training and awareness to reduce errors and strengthen security practices. iii) Incorporating Privacy Measures like homomorphic encryption, ensuring data protection within an interconnected industrial context. Through its structured approach, the SecureOps Lab bridges industry and academia, fostering skilled cybersecurity professionals and contributing viable security frameworks for industrial adoption. This paper presents a PoC case study of the Purdue Model using Fortinet's IoT Solution, illustrating practical applications and challenges in securing industrial infrastructures. The paper is organized as follows: Section 2 covers key concepts; Section 3 examines related work; Section 4 details our methodology; Section 5 describes the lab setup and case studies; Section **??** discusses findings; and Section 7 outlines conclusions and future directions.

2 BACKGROUND

CPS are interconnected devices that interact with each other and the physical world, integrating computation, communication, control, and monitoring techniques. These systems have gained attention due to their potential benefits to society, the economy, environment, and citizens [6] [7]. Advances in Information Communication Technology (ICT) have driven research in fields like IoT, CPS, and Social Computing, reshaping information science and human activities [8].

Operational Technology (OT) refers to hardware and software systems designed to monitor and control devices, processes, and physical events in industrial environments. Unlike IT, which is data-centric, OT focuses on the direct control and manipulation of physical operations. It includes industrial control systems such as SCADA, distributed control systems, and PLCs, critical for industrial operations' reliability and security [9]. Key components include PLCs, RTUs, HMIs, and safety systems like SIS, which ensure compliance and risk management, and protocols like Modbus, PROFINET, and Ethernet/IP, fundamental for network architecture [9].

The IIoT integrates the internet, advanced computing, and OT, using interconnected devices that collect, analyze, and exchange data to optimize operations. This digital ecosystem, built on CPS and advanced technologies, differs from traditional IoT by focusing on industrial applications requiring robustness and security [10]. The IIoT blends IT and OT, presenting unique security challenges due to interconnectivity and critical infrastructure. Its growth reflects increased productivity and reduced costs, with the market expected to nearly double from 2021 to 2023 [10].

The Purdue Model provides a structured framework for organizing industrial network components, spanning from physical devices to enterprise-level operations across six levels [19] [20]: i) Level 0: physical processes (sensors and actuators); ii) Level 1: basic control (PLCs); iii) Level 2: area supervisory control (HMIs and SCADA); iv) Level 3: site operations; v) Level 4: production data integration with business logistics; vi) Level 5: enterprise network (data analytics, corporate management).

The interconnected nature of IoT devices makes them vulnerable to security threats, compromising the integrity of systems. Attackers may target these systems to steal data or control operations [10]. The integration of IT and OT, alongside the scale and complexity of IIoT, introduces an expanded attack surface, with vulnerabilities in industrial control systems, sensors, and communication protocols. These convergences facilitate industrial innovation but also expose systems to cybersecurity risks [10], potentially leading to data loss, operational disruptions, financial losses, and safety risks. Addressing these challenges requires robust cybersecurity measures tailored to the IIoT, securing communication channels and ensuring ecosystem resilience against advanced threats [10] [11].

3 RELATED WORKS

Previous studies highlight gaps in IoT threat detection using machine learning, such as detecting zero-day threats and adapting to changing network traffic patterns [11][10]. There's a need to improve machine learning effectiveness in unsupervised environments and manage the complexity and volume of IoT data. Deep learning models, while promising, require substantial resources, which may not be feasible for IoT devices. The SecureOps lab aims to address these gaps, for example, by using federated learning to identify context-aware threats like describe by [13].

The proposed approach aims to reduce false positives and negatives in IoT threat detection. The complexity of IoT attacks and the need for privacy-friendly data integration from multiple devices pose challenges [11]. These gaps offer opportunities for research on robust, adaptable, and efficient threat detection methods, crucial for IoT security. These issues are being addressed in the SecureOps Laboratory. CPS and cybersecurity research is growing worldwide. The CPS Security Laboratory Network Project [1] focuses on cybersecurity in critical infrastructures. The SecureOps Lab at SENAI São Paulo [1] has a broader focus, including advanced manufacturing. In DeCPS [2] aims to enhance CPS and IoT security using advanced technologies. The Gachon University CPS Security Research Center [3] focuses on cybersecurity in critical infrastructures. The CyPSi Lab at the University of Delhi [4] has a broad scope, while the CPS Lab at the University of Jeddah [5] explores a wide range of technologies.

These research laboratories, each with its unique focus, collectively advance CPS security, resilience, and technological innovation, addressing complex industrial and societal challenges. The SecureOps Lab plays a critical role by integrating advanced technologies to enhance industrial security, efficiency, and resilience. Its key contributions include a broad technological scope, support for practical applications, workforce innovation, and a strong emphasis on operational security, rapid response, and strengthening the resilience of industrial environments.

4 METHODOLOGY

The methodology addresses five research objectives within the context of the CDC of SENAI São Paulo for enhancing security in industrial systems. Each objective corresponds to different levels of Technology Readiness Level (TRL) [12]. The following Figure 1 presents the research methodology of SENAI's CDC, which utilizes the Technology Readiness Levels (TRL). This approach provides a structured framework for the development and implementation of technologies, progressing from theoretical conception to practical application in operational environments.

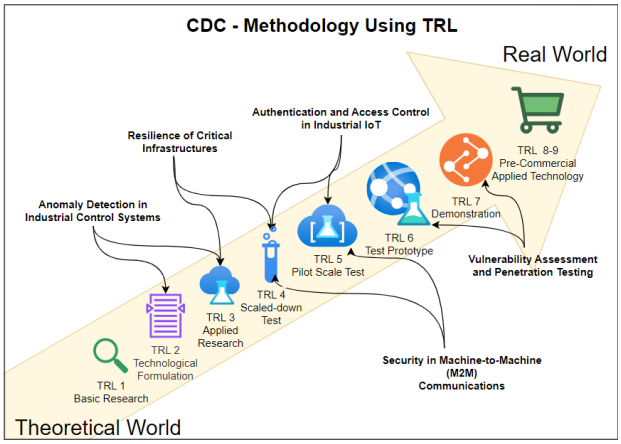

Figure 1: Methodology using TRL

Below, we detail the proposed methodologies for each of the research lines:

(1) **Anomaly Detection in Industrial Control Systems (TRL 2-3):** Develop and implement AI algorithms to identify anomalous behaviors in industrial control systems using simulated and real datasets. Train and validate machine learning models, including deep learning techniques, to predict and identify suspicious activities, enhancing control systems' ability to mitigate cyber attacks.

(2) **Resilience of Critical Infrastructures (TRL 3-4):** Develop methods incorporating system redundancies, isolation techniques, and rapid service recovery post-attack. Simulate attack scenarios to test and refine solutions, maximizing resilience without compromising operational efficiency.

(3) **Authentication and Access Control in Industrial IoT (TRL 4-5):** Explore innovative authentication mechanisms using blockchain and biometrics. Conduct prototyping and practical testing to ensure security and usability in industrial environments.

(4) **Security in Machine-to-Machine (M2M) Communications (TRL 4-5):** Develop secure communication protocols for M2M communications in industrial settings. Analyze and enhance existing protocols, focusing on data integrity and confidentiality. Validate protocols through field tests under various network conditions.

(5) **Vulnerability Assessment and Penetration Testing (TRL 6-7):** Develop methodologies and tools for continuous vulnerability assessment and penetration testing on industrial systems. Create an adaptable testing framework to identify and mitigate vulnerabilities proactively.

TRL estimate the maturity of a technology from basic principles (TRL1) to proven systems (TRL9). We use TRL to guide development, ensuring technologies are appropriately tested before progressing.

This systematic approach manages deployment risks and ensures technologies meet necessary requirements before integration. Each methodology addresses specific security challenges in industrial systems, advancing the TRL and ensuring solutions are practical and effective. Collaboration with industry experts and continuous feedback will align solutions with the sector's needs [12][14]. Each research line methodology is designed to address specific challenges in the security of industrial systems, progressively advancing the TRL and ensuring that developed solutions are practical, effective, and implementable in real industrial environments. Throughout the development, collaborations with industry experts and continuous feedback will be essential to align the solutions with the real and dynamic needs of the sector.

5 IMPLEMENTATION

To enhance the understanding of how the CDC tackles challenges related to CPS, OT, and IIoT, Figure 2 illustrates the high-level relationship between the CDC's topic approaches, research interests, and the abstraction layers of the CPS field. This visualization aids in clarifying how security strategies are applied in an integrated manner across the different layers that make up cyber-physical systems. Ahead, you will find a detailed description of how these subgroups function within CPS.

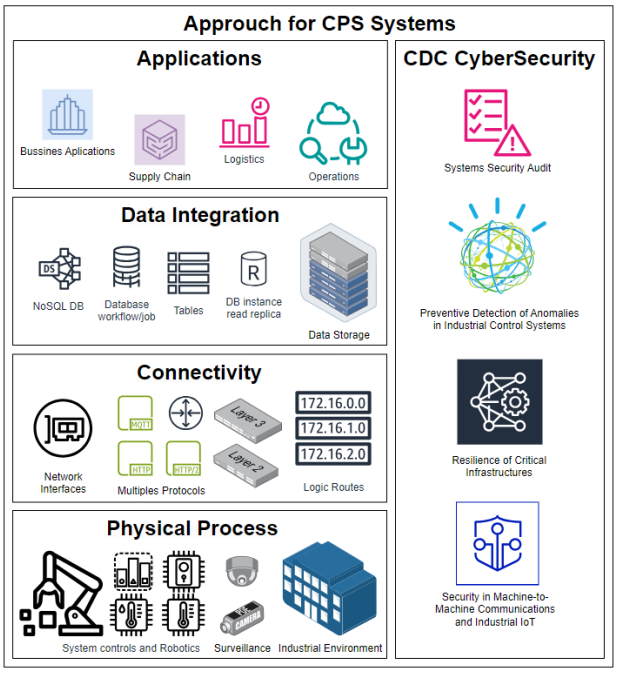

Figure 2: CDC Approach for CPS Cybersecurity

The Application Layer focuses on user interfaces and applications that directly interact with the CPS, OT, and IIoT. It encompasses monitoring tools, control software, and other components that operate machinery or process data. Security in this layer is vital as it often presents visible and accessible attack surfaces for cyber threats. The Data integration layer involves aggregating and processing data from multiple sources within the CPS, OT, and IIoT. This includes sensor data, operational data, and external data inputs that are crucial for the system's decision-making processes. Ensuring the integrity and security of this data is essential, as any manipulation can result in incorrect decisions, potentially leading to operational disruptions or safety hazards.The Connectivity layer is composed fir CPS, OT, and IIoT components and the external world. It involves network interfaces, communication protocols, and other mechanisms for data exchange. Security measures in this layer are crucial to prevent unauthorized access and protect data during transit from interception or alteration. It is also where network resilience and redundancy are addressed to maintain system operations in the face of potential cyber attacks.The Physical Processes layer refers to the physical components and actions controlled by the CPS, OT, and IIoT, such as motors, valves, and other mechanical parts. It is where the "physical" aspect of cyber-physical systems comes into play. Security in this layer involves ensuring the safety, authorization, and intended execution of commands by these components. It also includes protecting the physical components from direct sabotage or manipulation.

5.1 SecureOps Laboratories

The SecureOps Lab is physically located in two SENAI units situated in the Vila Mariana neighborhood of São Paulo city and in the downtown area of São Caetano do Sul. Both units have facilities that enable the simulation of an industrial environment (SENAI Vila Mariana[1]) and handle cybersecurity challenges (SENAI Sao Caetano do Sul[2]). This combination allows researchers to interact within the proposed methodology, developing theoretical concepts from the state of the art to real-world implementation with industrial use cases.

5.1.1 ***Industry 2.0.*** The Industry 2.0 brought transformations and challenges that require innovative monitoring and control solutions with sensor-based technologies. Developed devices from SENAI, can be installed on industrial equipment to modernize the production process. However, the integration of these devices raises cybersecurity concerns. The SecureOps Lab studies the security of these devices and their communications, serving as a test environment to evaluate the effectiveness of security protocols and strategies, which is included in the physical approach as depicted in Figure 2 of the methodology.

5.1.2 ***Industry 3.0.*** The transition into Industry 3.0 brought about the integration of digital technology and automation into manufacturing processes, setting the stage for significant advancements but also introducing new challenges such as system interoperability, data management, and the need for skilled workforce adaptation [16]. In this context, Figure 3 illustrates the FMS 200 SMC plant [17], a component of the SecureOps Lab. This setup is crucial for bridging the gap between theoretical solutions and their practical application within the industry. By employing the FMS 200 SMC plant, the SecureOps Lab enables the testing of proposed solutions in real-world scenarios, facilitating the validation and verification of their applicability and effectiveness in actual industrial settings. This approach not only enhances the reliability of new technologies

[1]SENAI Manufacture - https://eletronica.sp.senai.br
[2]SENAI Informatics https://sp.senai.br/unidade/informatica/

but also ensures that they can be seamlessly integrated into existing industrial ecosystems.

Figure 3: Didactic Industry 3.0 Implantation

5.1.3 ***Industry 4.0.*** Smart 4.0 is a modular educational platform designed to facilitate the teaching and understanding of Industry 4.0 technologies [15]. It integrates IoT and OT components to simulate real industrial processes. This platform includes modules like Storage, Manipulator, Manufacturing and Separation, which work together to represent the full cycle of an automated production line. Key IoT features include environment for virtual process simulations, cloud-based platforms for data handling, and IoT devices for connecting sensors and actuaries to the internet. The Figure 4 displays a comprehensive plant setup featuring all integrated modules and the Figure 5 display details about specific module. This visual representation provides a clear overview of how different components function together within a unified system, highlighting the interactions and connectivity between modules. This integrated approach is essential for demonstrating the cohesive operation of the entire plant, which is crucial for understanding the full capabilities and efficiencies that can be achieved through such a configuration.

On the operational side, Smart 4.0 employs robust OT technologies such as SCADA systems for real-time data acquisition and control, PLCs for managing physical operations, and MES to monitor and document production processes. These components are essential for teaching how modern factories operate and are managed, providing students with hands-on experience using cutting-edge technologies that drive today's smart factories. This combination of IoT and OT allows Smart 4.0 to offer a comprehensive and realistic educational tool in the field of industrial automation and data management.

5.1.4 ***SecureOps Main Lab.*** In the main laboratory of SecureOps, an advanced integration of technologies optimizes the operation and monitoring of machinery. Yashkawa's articulated robotic arms are connected to Siemens Programmable Logic Controllers (PLCs), facilitating a constant and accurate exchange of data regarding the

Figure 4: SMART Didactic Industry 4.0 Implantation

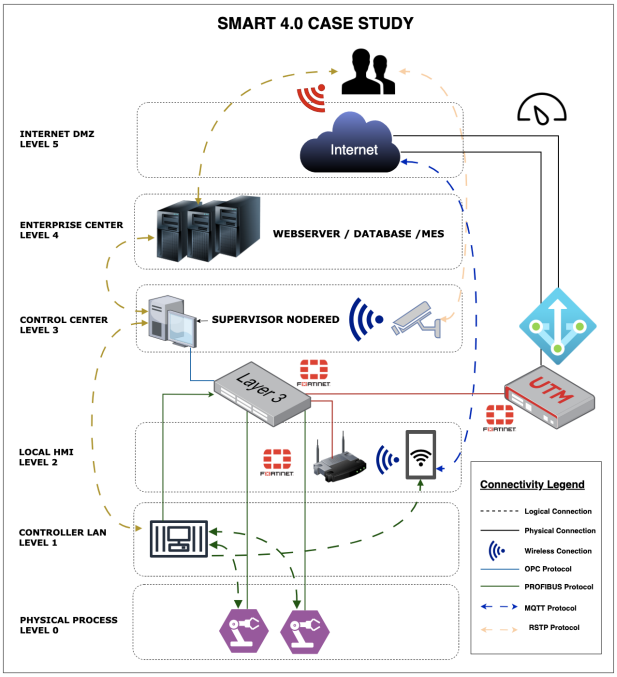

Figure 5: PoC using Fortinet Solution for IoT cybersecurity

robots' positioning and functionality. This information is sent to a Gateway (IBBX), which acts as a central point for data collection. Simultaneously, EMCO CNC machines are monitored by a variety of sensors measuring vibration, temperature, electrical data, and pressure. All collected data, from both the PLCs and the CNC sensors, are directed to the same Gateway, which then forwards them to cloud storage using AWS services. This setup not only ensures efficient and secure operations but also facilitates remote data analysis and management. The logical topology is clearly demonstrated in Figure 6, and Figure 7 is an actual photograph of the lab.

In the Main SecureOps Lab network scenario, a complex interplay of communication protocols ensures robust data handling

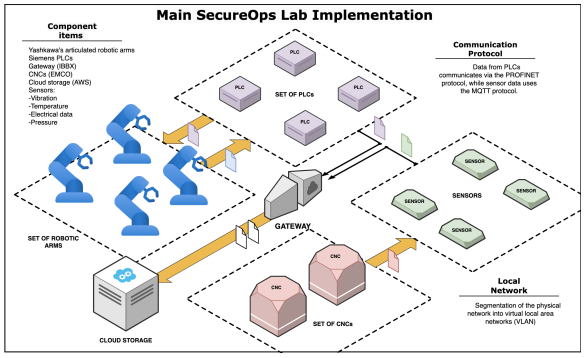

Figure 6: Main SecureOps Lab Implementation

Figure 7: Photograph of Main SecureOps Lab

and operational control. Programmable Logic Controllers (PLCs) communicate using the PROFINET protocol, a standard that supports real-time automation requirements and integrates seamlessly with industrial network equipment. Meanwhile, various sensors distributed across the facility transmit data using the MQTT protocol, a choice favored for its lightweight nature and effectiveness in IoT environments with bandwidth constraints. The network is segmented into multiple virtual local area networks (VLANs). This segmentation is crucial for managing the different types of traffic and securing sensitive areas of the network. By isolating different parts of the network into VLANs, SecureOps can control which devices communicate with each other, thereby reducing the risk of overloading the network and improving overall performance.

6 DISCUSSION

The Purdue model PoC using Fortinet highlighted challenges in integrating legacy systems not designed for cybersecurity. Upgrading these systems can be costly and disruptive. To mitigate this, a detailed assessment and phased migration plan are essential. Encapsulation solutions can protect legacy systems during gradual replacement, and virtualization can isolate old systems to minimize operational impact. Implementing the Purdue model introduces operational complexity due to detailed network segmentation, potentially causing configuration errors and coordination issues. Continuous team training and collaboration between IT and OT are crucial. Network automation tools and detailed procedures can manage complexity and reduce errors. Despite challenges, using Fortinet's IoT solution provided valuable insights into the environment, aided by event visualization in the FortiAnalyzer tool.

The costs of implementing the Purdue model can be high, including hardware, software, and training expenses. This highlights the need for affordable solutions for small industries. Organizations should adopt a holistic approach with clear policies, collaboration incentives, and interdisciplinary teams. Workshops can help align IT and OT cultures. The long lifecycles of many industrial devices make vulnerability management and system updates challenging. Patch management solutions and a strict vulnerability policy are crucial. Security-by-design practices can mitigate long-term challenges. With the Fortinet Solution, Purdue model-based measures were implemented without major disruptions. The PoC was key for testing new implementations, allowing benefits to be assessed in a lab before production deployment.

The Purdue model, ISO 27001:2022, NIST CSF 2.0, IEC 62443 standard, and TISAX work together to enhance synergies between IT and OT, establishing a comprehensive security framework across different infrastructure layers. At levels 0 and 1, these standards focus on protecting devices (ISO 27001:2022: A.13.1.1) and ensuring data security (NIST CSF 2.0: PR.DS-2, PR.DS-4), aligning with IEC 62443's emphasis on securing industrial components [21][23][22]. For level 1 (Basic Control), they address user access to control systems (ISO 27001:2022: A.9.1.2) and monitoring activities (ISO 27001:2022: A.12.4.1), reinforcing TISAX requirements for traceability and access management. At level 2 (Process Control), the focus shifts to protection against malicious code (ISO 27001:2022: A.12.3.1) and implementing robust defenses for vulnerable systems, closely aligning with IEC 62443's guidelines for safeguarding control system components and TISAX's focus on maintaining secure industrial operations [21][23][22][24].

At level 3 (Supervision and Operation), the emphasis is on maintaining well-documented procedures (ISO 27001:2022: A.12.1.1) and ensuring network information integrity (ISO 27001:2022: A.12.4.3), supported by security event analysis (NIST CSF 2.0: DE.AE-3) and aligned with IEC 62443's requirements for continuous monitoring of operational processes [21][23][22][24]. At level 4 (Production Management), priorities include incident management (ISO 27001:2022: A.16.1.1), business continuity planning (ISO 27001:2022: A.17.1.2), and enhanced incident response (NIST CSF 2.0: RS.RP-1, RC.CO-3), aligning with TISAX's emphasis on incident handling and operational resilience. Finally, at level 5 (Corporate Management), the focus shifts to establishing security policies (ISO 27001:2022: A.6.1.1), protecting records (ISO 27001:2022: A.18.1.3), and managing external dependencies and partners (NIST CSF 2.0: ID.BE-5). This approach is reinforced by strong governance (NIST CSF 2.0: ID.GV-1), IEC 62443's standards for secure interconnections, and TISAX's requirements for secure collaborations within the supply chain.

7 CONCLUSION

The SecureOps lab, equipped with advanced industrial equipment, serves as a crucial platform for cybersecurity research and development. It conducts comprehensive testing and simulations of cyber-attack scenarios on ICS, facilitating PoC trials to validate cybersecurity measures. The lab also refines communication protocols like MQTT and PROFINET, enhancing their resilience against security threats. By adopting the Purdue model, ISO 27001:2022, NIST CSF 2.0, IEC 62443 and TISAX guidelines, the lab has built a robust security infrastructure that strengthens the synergy between IT and OT, boosting organizational resilience. Additionally, the lab fosters research collaborations with industry and academia, promoting innovation in industrial cybersecurity and safeguarding operations against evolving threats.

Future research could explore privacy-preserving cryptographic methods like homomorphic encryption and integrate blockchain technology to enhance data security and trust. Developing platforms for secure threat intelligence sharing and using machine learning to synthesize data could enhance the collective cybersecurity landscape. Additionally, creating low-cost security solutions for small industries and establishing testing frameworks for securing IoT devices in realistic environments can further strengthen resilience against current and future threats.

ACKNOWLEDGMENTS

SENAI São Paulo, our team members and advisors for their invaluable support and contributions to this research.

REFERENCES

[1] Luleå University of Technology, Cyber-Physical Systems Lab, Luleå tekniska universitet, January 25, 2024. [Online]. Available: https://www.ltu.se/en/research/research-subjects/dependable-communication-and-computation-systems/research-projects/project-archive/2024-01-25-cyber-physical-systems-lab. [Accessed: April 25, 2024].

[2] University of Rhode Island, "Dependable Cyber-Physical Systems Laboratory," College of Engineering. [Online]. Available: https://web.uri.edu/decps/. [Accessed: Apr. 25, 2024].

[3] Gachon University, "CPS Security Research Center," Gachon University. [Online]. Available: https://ce.gachon.ac.kr/cps-security-research-center. [Accessed: Apr. 25, 2024].

[4] Institute of Informatics and Communication, University of Delhi, "CyPSi Lab – Cyber Physical Systems Interconnections Laboratory," Institute of Informatics and Communication, University of Delhi. [Online]. Available: http://cps.iic.ac.in/. [Accessed: Apr. 25, 2024].

[5] University of Jeddah. Cyber Physical System Laboratory, [Online]. Available: https://www.cps-uj.org/. [Accessed: April 25, 2024].

[6] K. Zhang, Y. Shi, S. Karnouskos, T. Sauter, H. Fang and A. W. Colombo, "Advancements in Industrial Cyber-Physical Systems: An Overview and Perspectives," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 716-729, Jan. 2023, doi: 10.1109/TII.2022.3199481.

[7] S. Kim, K. -J. Park and C. Lu, "A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design," in IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1534-1573, thirdquarter 2022, doi: 10.1109/COMST.2022.3187531.

[8] S. Rho, A. Vasilakos, W. Chen,Cyber physical systems technologies and applications, Future Generation Computer Systems, Volume 56,2016,Pages 436-437, ISSN 0167 -739X,https://doi.org/10.1016/j.future.2015.10.019.

[9] Eric D. Knapp, 4 - Introduction to Industrial Control Systems and Operations, Editor(s): Eric D. Knapp, Industrial Network Security (Third Edition), Syngress, 2024, Pages 65-90, ISBN 9780443137372, https://doi.org/10.1016/B978-0-443-13737-2.00011-7.

[10] S. H. Mekala, Z. Baig, A. Anwar, S. Zeadally, Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions, Computer Communications, Volume 208, 2023, Pages 294-320, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2023.06.020.

[11] R. Ahmad, I. Alsmadi, Machine learning approaches to IoT security: A systematic literature review, Internet of Things, Volume 14, 2021, 100365, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2021.100365.

[12] P. Raffaini, L. Manfredi, Chapter 15 - Project management, Editor(s): Luigi Manfredi, Endorobotics, Academic Press, 2022, Pages 337-358, ISBN 9780128217504, https://doi.org/10.1016/B978-0-12-821750-4.00015-3.

[13] H. Silva and R. Moraes. "Privacy-Preserving IoT Intrusion Detection: Challenges and Solutions in Implementing the CSAI-4-CPS Model."*CS & IT Conference Proceedings*. Vol. 14. No. 7. CS & IT Conference Proceedings, 2024.

[14] K. Armstrong, Chapter 13 - Emerging Industrial Applications, Editor(s): Peter Styring, Elsje Alessandra Quadrelli, Katy Armstrong, Carbon Dioxide Utilisation, Elsevier, 2015, Pages 237-251, ISBN 9780444627469, https://doi.org/10.1016/B978-0-444-62746-9.00013-X.

[15] Exxer, Launch Smart 4.0. [Online]. Available: https://registro.exxer.com/lancamento-smart-4-0. [Accessed: April 28, 2024].

[16] IEEE Innovative. IEEE is Fueling the Fourth Industrial Revolution. [Online]. Available: https://innovate.ieee.org/innovation-spotlight-ieee-fueling-fourth-industrial-revolution/ [Accessed: April 28, 2024].

[17] SMC Internation Training. FMS-200 - Flexible integrated assembling systems. [Online]. Available: https://www.smctraining.com/en/webpage/indexpage/431 [Accessed: April 28, 2024].

[18] L. Wainstein, D. Tarlow, C. McClister, S. Bhar and B. Gold "Microsoft Defender for IoT and your network architecture - Microsoft Defender for IoT," [online] Available: https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/understand-network-architecture [Accessed: April 29, 2024].

[19] T.J. Williams, The Purdue Enterprise Reference Architecture, IFAC Proceedings Volumes, Volume 26, Issue 2, Part 4, 1993, Pages 559-564, ISSN 1474-6670, https://doi.org/10.1016/S1474-6670(17)48532-6.

[20] D. Garton. Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation. US Department of Energy, v. 14, p. 2022-10, 2022.

[21] ISO/IEC 27001:2022, "Information technology — Security techniques — Information security management systems — Requirements", International Organization for Standardization, Geneva, Switzerland, 2022.

[22] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0", NIST, Gaithersburg, MD, USA, 2022.

[23] International Electrotechnical Commission, "IEC 62443 - Industrial communication networks - Network and system security," IEC Standard 62443, 2018.

[24] ENX Association, "TISAX (Trusted Information Security Assessment Exchange) - Information Security Requirements," TISAX Standard, Version 5.0, 2023.

[25] H. Silva, "CSAI-4-CPS: A Cyber Security characterization model based on Artificial Intelligence For Cyber Physical Systems," 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), Baltimore, MD, USA, 2022, pp. 47-48, doi: 10.1109/DSN-S54099.2022.00032.