Brown University

Systematization of Knowledge: Platforms, Pedagogies, and Practices for Effective ICS/OT Security Training

A systemization of Industrial Control Systems/Operational Technology Security Training.

by
José D. Sandoval

A thesis submitted in partial fulfillment for the degree of
Bachelor of Arts in Computer Science with Honors.

in the
Department of Computer Science

Advisor: Vasileios P. Kemerlis; Reader: Nikos Triandopoulos

April, 2025

Abstract

Industrial Control Systems (ICS), along with Operational Technology (OT) that control vital infrastructure, operate under increasing complex cyber threats (Ribeiro), while persistent training challenges, along with accessibility and realism issues, produce a substantial cybersecurity talent deficiency. This work aims to organize the existing knowledge about ICS/OT security education approaches as well as their training methods and platforms. This research investigates academic literature together with industry reports alongside threat intelligence information and pedagogical principles (Jagoda et al.; Ackermann), as well as presents training methods including physical labs (Sauer et al.), hybrid testbeds (Genge et al.), and virtual environments. A detailed design and architectural specification of "Colonial Outpost Security Lab," a new virtual gamified constructionist training platform, serves as the primary case study to demonstrate how best practices should be applied. The analysis systematization defines essential evaluation dimensions by comparing platform authenticity to accessibility constraints, as well as evaluating pedagogical approaches, threat simulation approaches, and training assessment methods. The analysis of various sources reveals that accessible virtualization technologies, especially containerization, are highly effective, along with active learning methods that include constructionism and GBL for motivational and cognitive benefits, and scenario-based training should model complete incident procedures and IT/OT integration complexities. High-fidelity simulation at scale remains an unresolved issue, together with practical team training and robust skill transfer evaluation. The systematization presents a structured overview of the field along with essential success factors and unaddressed problems while offering direction for future research and development of practical ICS/OT security training.

Section 1: Introduction (Systemization of Knowledge Framing)

1.1 The Critical Need for Effective ICS/OT Security Training

Modern society relies on Industrial Control Systems (ICS) and Operational Technology (OT) for managing essential infrastructure, including energy grids and water treatment facilities, as well as manufacturing plants and transportation networks. Security protection of these systems remains essential because cyberattacks result in catastrophic effects that surpass financial losses to cause environmental destruction and interrupt fundamental services, and potentially lead to fatalities. The threat environment against OT systems has transformed from basic malware threats into sophisticated state-sponsored operations that use customized tools for destructive and disruptive attacks. OT has faced multiple significant attacks, including Stuxnet, Industroyer, and Industroyer2 on the Ukrainian power grid and TRISIS against safety systems and versatile

frameworks like PIPEDREAM/INCONTROLLER(“Just Released! Dragos’s 2023 OT Cybersecurity Year in Review Is Now Available | Dragos”). OT facilities remain exposed to attack because even unsophisticated cybercriminals use elemental security weaknesses such as default PLC credentials on internet-visible US water facility equipment.

The rise of IT/OT network convergence has become a new security challenge in addition to the existing threats. The pursuit of operational efficiency through integration has eliminated historical "air gaps" while expanding vulnerabilities and producing intricate security issues because of different system priorities and technologies, as well as OT equipment longevity and cultural differences between IT and OT personnel. Specialized skills combining IT security expertise with a deep understanding of OT processes and safety constraints, and unique protocols are needed to defend these converged environments effectively.

The creation of this specialized workforce encounters substantial barriers during development. A worldwide shortage of cybersecurity professionals remains a significant problem that affects the specialized ICS/OT sector most profoundly. Traditional teaching methods fail to deliver satisfactory results. Theoretical education lacks practical depth; High-fidelity physical hardware labs are too expensive, unreachable, and complicated to scale or update, while many virtual environments lack proper realism, teaching foundations, and modern threat relevance. The combination of rising threats, system complexity, skills shortages, and training limitations produces an immediate need for advanced ICS/OT security education methods.

1.2 Scope and Methodology of this Systematization

This thesis implements a Systematization of Knowledge (Systemization of Knowledge) to explore Platforms, Pedagogies, and Practices for ICS/OT Security Training because of its vital need and changing solution environment. The analysis focuses on organizing current state-of-the-art information to identify key dimensions, trends, trade-offs, challenges, practical strategies, and open problems within this domain.

Our methodology includes a combination of knowledge acquisition and synthesis techniques:

- **Literature Review:** Analysis of academic papers that explore ICS/OT security alongside cybersecurity education and serious games alongside learning sciences, pedagogical theories, and human-computer interaction.
- **Platform Analysis:** Examination of existing ICS/OT training platforms along with physical labs (Sauer et al.), hybrid cyber-physical testbeds (Genge et al.), and various virtual approaches (Formby and Rad; Ekisa et al.; Dehlaghi-Ghadim et al.). The research examines the platforms' technical systems along with their functions, restrictions, expense levels, availability, and teaching elements.
- **Industry & Threat Intelligence Review:** The study incorporates results from industry surveys together with threat intelligence reports (Kesselring; *APT Cyber Tools Targeting ICS/SCADA Devices | CISA*) and real-world incident analyses to determine present threats and vulnerabilities as well as operational challenges and training needs.

- **Analysis of Frameworks and Standards:** NIST CSF 2.0, together with NIST SP 800-82 Rev 3 ISA/IEC 62443 and MITRE ATT&CK for ICS, receive analysis in this research.
- **Case Study Design:** A thorough architectural outline, together with pedagogical structures, scenario ideas, and implementation blueprint, was developed for the Colonial Outpost Security Lab platform. This provides an in-depth example of synthesizing best practices into a proposed solution, even though the platform itself is in early development and not yet evaluated.
- **Synthesis:** Thematically organized synthesis of data acquired from multiple sources.

1.3 Contributions of this Systematization

This Systematization of Knowledge provides the following contributions to the field of ICS/OT security training and education:

- **Structured Overview:** This paper delivers a complete examination of the training environment by grouping ICS/OT platforms into physical, hybrid, and virtual categories and dividing pedagogical methods into SBL, GBL, Constructionism, and other approaches.
- **Analysis of Inherent Trade-offs:** A systematic evaluation of training environment design trade-offs focuses on fidelity and realism, together with cost, scalability, accessibility, and maintainability.
- **Analysis of Pedagogical Effectiveness:** Theoretical foundations and practical evidence collected from literature and the Colonial Outpost Security Lab case study demonstrate which pedagogical methods work best in developing practical skills and critical thinking in this complex technical domain.
- **Synthesis of Best Practices and Lessons Learned:** The research provides an overview of key challenges (e.g., safe simulation of complex threats, IT/OT bridge, skill assessment) and practical training strategies identified across various approaches.
- **Identification of Gaps and Future Directions:** This work presents existing knowledge deficits and practical shortcomings while providing exact directions for upcoming studies that will advance ICS/OT security training development.

This research provides researchers, educators, practitioners, and policymakers with an integrated perspective of ICS/OT security education challenges and opportunities, which offers directions for better training solutions development.

1.4 Roadmap

This paper follows this structure, starting from Section 2, which describes the Systematization of Knowledge methodology. The third section evaluates ICS/OT training platforms and their environments by studying various platform types with their corresponding advantages and disadvantages. This section organizes pedagogical methods that apply to ICS/OT security training as well as those implemented in the field. Section 5 explores content realism methods by focusing on threat modeling alongside process simulation. This paper explores

multiple methods for measuring training effectiveness. Section 6 presents approaches for assessing training effectiveness. The analysis results in Section 7 combine key insights with learned lessons along with identified ongoing challenges and unresolved problems. The final section presents a summary of the main findings from this systematization.

Section 2: Methodology

The Systemization of Knowledge method uses an organized system to discover and evaluate existing knowledge about platforms, teaching approaches, and practices for Industrial Control System (ICS) and Operational Technology (OT) security training. The research aims to establish a complete understanding of the field, together with its significant developments and difficulties, and propose directions for future research and development.

2.1 Scope Definition

This systematization examines training methods designed to instruct IT professionals, OT engineers, security analysts, and students about ICS and OT security needs. This includes:

- **Training Platforms:** Physical testbeds, hybrid cyber-physical testbeds (CPTs), and various virtual environments (VM-based, container-based).
- **Pedagogical Strategies:** ICS/OT security training utilizes and is suitable for the following educational theories and techniques: scenario-based learning (SBL), problem-based learning (PBL), gamification, game-based learning (GBL), constructionism, and collaborative learning.
- **Content and Realism:** Methods for simulating ICS/OT processes, protocols, network architectures, contemporary cyber threats, and alignment with industry standards.
- **Evaluation Techniques:** Approaches used to assess the effectiveness of training platforms and pedagogical methods, including quantitative metrics, qualitative feedback, and behavioral analysis.

The timeframe primarily considers developments from the early 2010s to the present (early 2025), reflecting the period of increased awareness and research following major incidents like Stuxnet, while acknowledging foundational concepts from earlier work where relevant.

2.2 Knowledge Source Identification

This Systemization of Knowledge provides thorough coverage by drawing its knowledge from a broad array of sources.

- **Academic Literature:** Peer-reviewed publications from relevant conferences (e.g., ACM CCS, USENIX Security, NDSS, RAID, ESORICS, ACSAC, CCSC, SIGCSE, ITiCSE) and journals (e.g., IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, Computers & Security, ACM Transactions on Privacy and Security, Computers & Education, British Journal of

Educational Technology, Simulation & Gaming). This includes research presenting specific testbeds, analyzing pedagogical approaches, and discussing ICS/OT security challenges.

- **Industry Reports and Threat Intelligence:** Publications from cybersecurity vendors, security research organizations, government agencies, and analyses of specific incidents. These provide crucial context on real-world threats, vulnerabilities, industry trends, and operational challenges.
- **Technical Documentation and Platform Analysis:** Publicly available information, technical papers, and user documentation related to various ICS training platforms, virtualization technologies, emulation tools, and security tools used within these environments.
- **Pedagogical Theories:** Foundational literature on learning theories relevant to simulation and technical training, including Constructivism (Ackermann), Constructionism (Ackermann), Situated Learning, Experiential Learning, Game-Based Learning, and Cognitive Load Theory (Mukherjee et al.).
- **Case Study Design:** The detailed architectural design, pedagogical framework, scenario concepts, and implementation strategy were developed for the 'Colonial Outpost Security Lab' platform. This provides an in-depth example of synthesizing best practices into a proposed solution.
- **Security Frameworks and Standards:** Key documents defining best practices and requirements, such as the NIST Cybersecurity Framework (CSF) 2.0, NIST SP 800-82 Revision 3, and the ISA/IEC 62443 series, which frame the security goals training should address.

2.3 Data Extraction and Synthesis Process

The systematization process involved several stages:

- Source Collection: Gathering relevant documents based on keyword searches in academic databases, citation chaining, review of major security/education conference proceedings, and known industry resources.
- Information Extraction: Reviewing collected sources to extract key information related to the defined scope: platform architectures, technical features, pedagogical approaches employed, types of scenarios used, evaluation methods, reported outcomes, identified challenges, and proposed solutions or best practices.
- Categorization and Taxonomy Development: Iteratively developing classification schemes (taxonomies) for key dimensions based on recurring themes and distinct characteristics observed in the sources. This included categorizing platform types (physical/hybrid/virtual, VM/container), pedagogical strategies, threat simulation approaches, and evaluation metrics.

- Comparative Analysis: Analyzing and comparing different approaches within each category based on identified criteria. The trade-offs associated with varying choices of design were explicitly considered.
- Thematic Synthesis: Identifying overarching themes, persistent challenges, successful strategies, lessons learned, and significant gaps across the synthesized body of knowledge.
- Case Study Integration: Using the specific design decisions and features from the Colonial Outpost Security Lab platform development as a proposed solution to illustrate broader points, support synthesized insights, or highlight particular approaches within the developed taxonomies.

2.4 Limitations of the Systemization of Knowledge Methodology

This systematization, similar to any systematization of knowledge, is not without certain inherent limitations. Though attempting to be as inclusive as possible, some literature may have been overlooked, particularly grey literature or proprietary platform details. As with all analysis and synthesis, this involves interpretation, which means the potential for researcher bias is present, although attempts were made to make sure the conclusions were well supported by the sources. Additionally, ICS/OT security and the associated training technologies are dynamic; this systemization of knowledge presents information up to early 2025 and requires periodic updates to stay current.

Section 3: Systematization of ICS/OT Training Platforms and Environments

3.1 Introduction

Industrial Control System (ICS) and Operational Technology (OT) security training needs effective environments that let learners apply defensive techniques against realistic threats in simulated or real industrial environments. Training platform selection directly affects the realism, price, expandability, ease of access, and type of learning that can be delivered. Over the last decades, different methods have appeared, including physically identical replicas and completely virtualized software environments. This paper categorizes these diverse platforms and analyses their inherent advantages, disadvantages, and trade-offs, specifically regarding their suitability for broad-based education and professional training. This analysis draws from existing literature and the Colonial Outpost Security Lab case study development.

3.2 Taxonomy of Platform Types

Based on the reviewed literature and existing implementations, ICS/OT training platforms can be broadly categorized into three main types:

- Physical Testbeds: Utilize fundamental, industrial-grade hardware components.

- Hybrid Cyber-Physical Testbeds (CPTs): Combining physical hardware elements with software emulation or simulation.
- Virtual Testbeds: Reconstruct ICS/OT components and networks by software. These can be further subdivided based on virtualization technology.

3.3 Physical Testbeds

Physical testbeds consist of actual industrial hardware that replicates a specific process. Examples range from large university labs to more focused, lower-cost setups like LICSTER. LICSTER, for instance, uses Raspberry Pis for PLC/HMI functions, communicating via Modbus TCP with simple physical I/O (like sensors and a conveyor belt model) and remote IO modules, all mounted portably and designed for affordability in teaching interactions at Levels 0-2. The primary advantage of physical testbeds is their high physical fidelity, making them essential for specific hardware vulnerability testing or training involving physical interaction. However, they suffer from significant disadvantages, including high costs for acquisition, maintenance, and space; low scalability; inflexibility, making reconfiguration difficult; poor accessibility; high maintenance overhead; and potential safety concerns if not managed adequately during attack simulations.

3.4 Hybrid Cyber-Physical Testbeds (CPTs)

Hybrid CPTs blend real hardware with software simulation or emulation. A notable example is Genge et al.'s framework, which utilized an Emulab-based testbed for cyber components like workstations and network devices that interacted with a physical process simulated in real-time using Simulink. This setup enabled safe experimentation with real malware targeting the cyber infrastructure while observing the simulated physical outcomes. Other CPTs involve real PLCs controlling simulated processes or the reverse scenario. The main benefit of CPTs is the balance they strike between the fidelity offered by included hardware and improved cost/flexibility compared to purely physical labs, allowing for testing specific hardware-software interactions. Genge et al. noted their cost efficiency over ad-hoc physical labs for conducting numerous experiments. Nevertheless, CPTs retain hardware costs and maintenance requirements, face complexity in integrating physical and virtual elements, and present challenges in scalability, reproducibility, and accessibility when compared to fully virtual solutions. Genge et al. acknowledged that lower physical layer fidelity was a trade-off made for safety and cost reasons.

3.5 Virtual Testbeds

Virtual testbeds replicate the entire ICS/OT environment using software through virtualization, emulation, and simulation.

3.5.1 VM-Based

These testbeds use hypervisors like VirtualBox, VMware, or KVM to run full OS instances for each component. GRFICS serves as an example, using five VirtualBox VMs to

emulate a PLC (OpenPLC), HMI (ScadaBR), firewall (pfSense), engineering workstation, and includes a 3D visualization of the Tennessee Eastman chemical process via Unity. This open-source platform aimed to lower barriers to accessing a complete virtual ICS network. Analysis showed strong component isolation but significant resource overhead (around 5GB RAM and 39GB disk per instance), which limits scalability on standard hardware and increases setup complexity. Some studies noted limitations in network segmentation for specific research, and the visualization was tied to a particular process.

3.5.2 Container-Based

This approach uses lightweight OS-level virtualization like Docker or LXC, where containers share the host OS kernel. VICSORT, built upon GRFICS to address resource limits, used LXC/LXD containers, significantly reducing RAM (~1.2GB) and disk (~23GB) needs, offering faster startups (<10s), using newer OS versions, and emphasizing easy deployment. It kept core components like the PLC, HMI, workstation, firewall, and process simulation within its containerized structure. ICSSIM is another Docker-based framework providing Python-based classes for simulating DCS components and communications. It focuses on versatility for diverse scenarios, comprehensiveness across components, flexible network architecture, reproducibility via Docker, high fidelity through realistic control loops and protocols, and extensibility using isolated containers. It includes an 'Attack Generator' container with Kali Linux tools based on MITRE ATT&CK/ENISA and supports various process simulation methods. The proposed 'Colonial Outpost Security Lab' design also adopts the container-based (Docker) approach, aiming for low resource use, scalability, reproducibility, and accessibility by leveraging tools like OpenPLC and SCADA-LTS with Python for simulation. (Alves and Morris; Rodrigues Alves et al.; Miranda; Formby et al.)

3.5.3 Advantages of Virtual Testbeds

Low cost, high scalability and flexibility, excellent accessibility and reproducibility, and inherent safety, making them ideal for attack simulation without real-world risk. They directly tackle the limitations of physical labs for broad training deployment and align well with modern software practices like DevOps/DevSecOps. However, potential fidelity limitations exist compared to physical hardware, especially concerning precise real-time behavior, hardware quirks, or complex physical layer interactions. They also lack the tactile experience of working with physical equipment and require careful design to ensure sufficient functional realism for learning objectives.

3.6 Key Trade-offs and Trends

Training platform selection requires making decisions about Fidelity, Cost, Scalability, and Accessibility.

- Physical testbeds score very well on physical fidelity but are very poor on cost, scalability, and accessibility.

- Hybrid testbeds may offer some advantages in terms of flexibility over purely physical labs, but they still have the cost and complexity associated with hardware components.
- Virtual testbeds excel in cost, scalability, accessibility, flexibility, and safety, making them ideal for broad educational deployment. While fidelity, particularly for real-time and hardware-specific aspects, remains a consideration requiring careful design, the advantages are compelling for training purposes.

The trend in the field is toward container-based virtual testbeds, which is evident from the platforms presented in the VICSORT, ICSSIM, and the Colonial Outpost Security Lab case study. It seems that this approach provides the most promising solution, which offers sufficient functional realism for the security training scenarios and also provides the necessary accessibility and scalability to address the tremendous skills gap in the ICS/OT field. The focus moves from the exact replication of every physical detail to developing pedagogically practical, realistic simulations that can provide accessible, hands-on learning of key security concepts and practices. Section four investigates the pedagogical approaches for ICS/OT security training systematization.

Section 4: Systematization of Pedagogical Approaches for ICS/OT Security Training

4.1 Introduction: The Importance of How We Teach

The technical fidelity and accessibility of training platforms, which are discussed in Section 3, represent only one of the essential aspects of effective Industrial Control System (ICS) / Operational Technology (OT) security education. The pedagogical approach—the underlying theory and methods guiding how learning activities are structured and facilitated—is equally, if not more, critical in developing the deep understanding, critical thinking, practical skills, and adaptability required to defend complex industrial environments. Simply providing access to a realistic simulation is insufficient; how learners interact with that simulation, construct knowledge, and develop competencies is paramount. This section systematizes prominent pedagogical theories and strategies relevant to and employed within ICS/OT security training, analyzing their principles and applicability, often using the designed Colonial Outpost Security Lab environment as a case study illustrating their proposed integration.

4.2 A Spectrum of Pedagogical Approaches

Technical and cybersecurity education methods range from traditional instructionist models to more modern active and social learning paradigms. Key approaches relevant here start with Behaviorism/Instructionism, the conventional models focused on knowledge transmission. Next is Constructivism/Constructionism, which emphasizes active knowledge building by the learner. Experiential/Situated Learning grounds learning in authentic contexts and direct experience. Problem-Based Learning (PBL) and Scenario-Based Learning (SBL) structure learning around solving realistic problems or navigating specific situations. Finally, Game-Based

Learning (GBL) and Gamification utilize game elements or full games to enhance motivation and learning.

4.3 Behaviorism/Instructionism (Baseline)

4.3.1 Description

This traditional approach views learning as the transmission of information from instructor to learner. Methods often involve lectures, readings, demonstrations, and assessments focused on recall of facts and procedures (e.g., rote memorization of protocol details or compliance checklists). The learner is often seen as a passive recipient.

4.3.2 Application & Analysis (ICS/OT Context)

While helpful in imparting foundational knowledge (e.g., definitions of terms, overview of standards), purely instructionist methods are widely recognized as insufficient for developing the higher-order skills needed in ICS/OT security. They fail to cultivate practical application, critical thinking under pressure, adaptability to novel situations, or effective problem-solving in complex, dynamic environments. Most modern technical training incorporates elements beyond pure instructionism.

4.4 Constructivism and Constructionism: Learning by Building

4.4.1 Description

Constructivism, heavily influenced by Piaget, posits that learners actively construct understanding by interpreting new experiences through the lens of their existing knowledge and adapting their mental models. Learning is not passive reception but an active building process. Constructionism, developed by Papert, extends this by arguing that knowledge construction is particularly effective when learners are "consciously engaged in constructing a public entity," whether physical or digital. This "learning by making" or "learning by doing" emphasizes learner agency, exploration, and the creation of shareable artifacts. It aligns with the "maker culture," valuing experimentation, collaboration, and learning from failure.

4.4.2 Application & Analysis (ICS/OT Context)

These theories are highly relevant and increasingly influential in designing practical technical training. Within an ICS/OT context, instead of just being told about firewall rules, learners actively construct firewall configurations within the simulation environment. Rather than simply reading about incident response, they build a response strategy by executing commands, isolating affected systems, and analyzing logs generated within the simulation. The Colonial Outpost Security Lab environment is explicitly designed based on constructionist principles; learners are tasked with building the outpost's defenses, their actions directly shape the state of the environment, and their success represents a constructed solution to the security challenges presented. This active engagement promotes more profound understanding and a

sense of ownership compared to merely following prescribed instructions. Platforms that allow learners to create or modify scenarios themselves further embody the principles of constructionism.

4.5 Experiential and Situated Learning: Learning in Context

4.5.1 Description

Experiential Learning (Kolb, Dewey) emphasizes learning through direct experience and reflection on that experience. Situated Learning (Lave & Wenger) argues that learning is inseparable from the context and social interactions in which it occurs; knowledge is best acquired within "communities of practice" working on authentic tasks. Both value concrete, contextualized, and often social learning over abstract decontextualized knowledge.

4.5.2 Application & Analysis (ICS/OT Context)

Experiential learning benefits greatly from the utilization of simulation environments. Students directly observe the simulated outcome of cyberattacks together with the outcomes of their defensive measures, such as process disruption and data loss. The Colonial Outpost Security Lab delivers an immersive situated environment. The hatch puts learners in the position of defenders who must respond to particular operational limitations and security threats. Team-based scenarios create a situated community of practice by encouraging learners to collaborate while they share knowledge and negotiate solutions that replicate real-world SOC or IR team dynamics. Through this specific context, students experience more relevant learning that supports the transfer of information.

4.5.3 Lab Design

The Colonial Outpost Security Lab presents the context for the narrative to provide a situated environment. The outpost's operational limitations make learning more tangible because learners must respond to ransomware attacks that use "Pirate" tactics and techniques. The implementation of team-based modes will create an environment that builds a situated community of practice. The After-Action Review (AAR) function will analyze mission logs and outcomes through structured reflection procedures.

4.6 Problem-Based Learning (PBL) and Scenario-Based Learning (SBL)

4.6.1 Description

PBL structures learning around authentic, complex problems that learners must investigate and resolve, often requiring self-directed learning. Learning activities in SBL rely on specific scenarios, which serve as narratives. A well-implemented PBL/SBL system enables meaningful task connections to significant learning goals and promotes ownership while utilizing genuine problems and facilitating reflection along with practical experimentation of ideas.

4.6.2 Application & Analysis (ICS/OT Context)

The ICS/OT field benefits most from Scenario-Based Learning (SBL), which stands as the primary paradigm for delivering practical cybersecurity training. The authentic problems required for Problem-Based Learning (PBL)/Scenario-Based Learning (SBL) originate from actual ICS incidents, including ransomware attacks and APT campaigns such as Industroyer2 and SIS attacks like TRISIS and insider threats.

4.6.3 Lab Design

The Colonial Outpost Security Lab Design Example structures its missions as interconnected SBL activities that challenge participants to diagnose security threats while implementing defensive measures. Scenarios derive from actual incident types, while the security controls and frameworks, including MITRE ATT&CK for ICS, provide their foundation.

4.7 Game-Based Learning (GBL) and Gamification

4.7.1 Description

Gamification uses particular elements such as points, badges, leaderboards, progress bars, and challenges in non-game environments to boost engagement and motivation levels. GBL makes use of the entire games, including digital and physical versions, which were developed to achieve specific educational goals. A well-developed GBL framework allows students to develop critical thinking skills as well as strategic planning abilities and decision-making skills while operating under pressure and collaborating with others in a protected environment of trial and error. The incorporation of narrative and "worlding" components in GBL enables learners to discover identities while studying complex systems through possibility spaces. Modern cybersecurity training programs use GBL and Gamification to fight training monotony and boost participant engagement.

4.7.2 Lab Design

The Colonial Outpost Security Lab design proposes implementing GBL through its overarching narrative, defined threat actor roles, a progressive mission structure, and an integrated feedback and reward system. The aim is to leverage both intrinsic motivation, driven by the story, challenge, and sense of mastery, and extrinsic motivation, through points and badges tied to meaningful security outcomes like effective threat containment or safe system recovery. Key challenges include balancing educational objectives with entertainment value, sustaining learner motivation over the long term, and avoiding potential pitfalls such as overemphasizing competition or relying on superficial rewards. Providing diverse pathways and challenges within the game world aligns with Papert's concept of "wide walls," catering to different learner interests and learning styles.

4.8 Synthesis: Towards Integrated Active Learning

4.8.1 Core Principles

Core principles emerge for effective pedagogy in this domain. First, active construction is essential; learners must actively do and build, not just passively receive information, aligning with Constructionism. Second, learning needs authentic context, occurring within realistic, scenario-based problems relevant to real-world ICS/OT challenges, reflecting SBL/PBL and Situated Learning principles. Third, experiential learning is crucial, involving direct experience with simulated attacks and defenses coupled with reflection. Fourth, engaging design through the thoughtful application of Gamification and GBL can significantly enhance motivation and persistence. Fifth, environments must allow for safe failure, enabling learners to experiment, make mistakes, and learn from them without real-world consequences. Finally, collaboration is necessary; training should incorporate opportunities for teamwork to develop essential communication and coordination skills needed in IT/OT environments. Designing high-quality, pedagogically sound scenarios is demanding. Balancing game elements with learning objectives requires careful consideration. Assessing the higher-order thinking skills fostered by these active approaches needs robust methods beyond simple performance metrics. Facilitating adequate reflection and collaborative learning within these environments also requires skilled instruction or well-designed system support mechanisms.

4.8.2 Lab Design

The platform design serves as an example of such integration, which uses GBL to deliver SBL/PBL problems to learners while they build defenses (Constructionism) through hands-on interaction with a realistic simulation (Experiential Learning) supported by feedback loops promoting reflection.

4.8.3 Remaining Challenges

Creating high-quality scenarios that adhere to pedagogical standards proves to be quite challenging. The process of balancing game components with learning targets requires careful attention. These approaches require advanced methods to assess the higher-order thinking skills they develop because traditional performance metrics are insufficient. Adequate reflection and collaborative learning in these environments require either skilled instruction or well-designed system support to succeed.

The development of adaptable, skilled professionals needed for ICS/OT infrastructure security requires a transition from traditional instructionism to integrated active learning approaches that combine realistic SBL with engaging GBL and constructionist principles within accessible virtual platforms.

Section 5: Systematization of Content and Realism in Training

5.1 Introduction: The Importance of Relevant and Realistic Content

The effectiveness of Industrial Control System (ICS) / Operational Technology (OT) security training depends heavily on the content presented and its realism beyond the selection of training platforms (Section 3) and pedagogical approaches (Section 4). The training needs to include accurate representations of real-world industrial environments through scenarios, threats, system behaviors, and operational contexts that learners will encounter. This section systematizes approaches to achieving realism in training content, focusing on threat modeling and simulation, process and protocol fidelity, and alignment with industry standards. This section analyzes the methods employed by multiple platforms. It examines the Colonial Outpost Security Lab case study to determine the natural trade-offs that occur between realistic simulation, safety, accessibility, and educational effectiveness.

5.2 Threat Modeling and Simulation

Realistic simulation of cyber threats stands as the essential component for hands-on ICS/OT security education. The learning experience aims to provide students with controlled exposure to the operational methods (TTPs) of relevant adversaries.

5.2.1 Approaches to Threat Simulation:

5.2.1.1 Scripted Attacks

The standard training method uses automated adversary actions through predefined scripts operating within the simulation environment. The scripts replicate particular TTPs that derive from recorded incidents and malware attacks. The ICSSIM framework uses an 'Attack Generator' container with Kali Linux tools to perform scripted attacks that reproduce MITRE ATT&CK for ICS or ENISA reports-based DoS, MITM, or replay attacks. The Colonial Outpost Security Lab design utilizes similar attack mechanisms to recreate the TTPs of its defined threat actor archetypes, which include Pirates, Invading Force, and Saboteurs.

5.2.1.2 Malware Emulation/Simulation

Some platforms use malware emulation to replicate particular malware behavior by reproducing file encryption like ransomware and control logic manipulation from Stuxnet and PIPEDREAM, as well as communication disruption from Industroyer2 without deploying actual malicious code. The system uses programming code to replicate how malware influences system states and network traffic patterns.

5.2.1.3 Live Malware

The introduction of actual malware samples for analysis or response practice becomes possible in advanced research testbeds that use hybrid or well-isolated virtual environments,

according to Genge et al. The highest threat fidelity comes from this method, but it poses significant risks to safety and containment procedures.

5.2.1.4 APT Simulation

APT Simulation requires the creation of advanced persistent threat simulations that include stealth operations and reconnaissance alongside IT/OT boundary crossing, privilege escalation, and long-term foothold maintenance during multi-stage campaigns that extend past typical exercise periods. Such implementation proves difficult to execute efficiently during limited training periods. The simulation of PIPEDREAM attacks through native platform tools presents a particularly complex challenge because it demands extensive system understanding from the simulation.

5.2.2 Realism vs. Safety Trade-off

The simulation of threats needs to maintain proper safety measures when delivering realistic scenarios to students. Training with live malware poses safety issues for broad educational programs. The use of scripted attacks that replicate TTPs and their effects provides learners with a secure environment to practice defensive measures against authentic techniques without exposing them to unsafe code. Containerization enhances safety during malicious action simulations through its strong isolation features.

5.2.3 Keeping Threats Current

The threat landscape evolves constantly. Training effectiveness demands that simulated threats maintain current status by reflecting new malware (such as FrostyGoop employing Modbus against exposed devices), evolving ransomware approaches, new security weaknesses in incidents (such as unsecured default credentials in water facility attacks), and new threat group tactics used by entities like CHERNOVITE and BENTONITE. The modular structure of ICSSIM and Colonial Outpost Security Lab allows simpler updates of attack scripts than hardware-based or monolithic systems do.

5.3 Process and Protocol Simulation Fidelity

The need for authentic training demands both authentic threats and an authentic simulation of the ICS/OT environment with its controlled physical processes and its communication protocols.

5.3.1 Physical Process Modeling:

Various methods are used for modeling the physical process being controlled. These range from simple mathematical models or Python scripts generating sensor/actuator data, as planned for Colonial Outpost Security Lab and feasible in ICSSIM, to integration with high-fidelity engineering simulation software like MATLAB/Simulink, used by Genge et al. and supported by ICSSIM, or even Hardware-in-the-Loop (HIL) setups. Some platforms, like GRFICS, have used 3D game engines for visualization purposes. Accurately modeling complex

physics, chemical reactions, or precise real-time dynamics solely in software presents fidelity challenges. Virtual simulations offer lower physical fidelity compared to CPTs or physical labs. However, for many security training goals, high functional fidelity, meaning the system responds plausibly to commands and attacks, can be more critical than perfect physical accuracy. The simulation must be realistic enough for learners to grasp the potential physical consequences of cyber events.

5.3.2 Protocol Realism:

5.3.2.1 Importance:

Security problems frequently emerge because standard ICS communication protocols, including Modbus, DNP3, IEC 61850, OPC UA, and S7, have authentication and encryption weaknesses alongside particular implementation weaknesses. Threat actors develop tools specifically targeting these protocols (Jones; *CHERNOVITE's PIPEDREAM Targeting Industrial Control Systems (ICS)*).

5.3.2.2 Implementation:

OpenPLC supports Modbus protocol integration, and ICSSIM provides protocol implementations together with extension capabilities for multiple communication standards. The training environment enables students to view and analyze traffic while interacting with native protocol communications to learn about protocol vulnerabilities and IDS/NSM protocol monitoring capabilities.

5.3.3 Network Architecture Realism:

Realistic network segmentation according to Purdue Model levels or IEC 62443 Zones and Conduits must be simulated because it allows students to learn about defense-in-depth, firewall configuration, and IT to OT lateral movement paths, which attackers commonly exploit. Virtual networking capabilities within Docker and hypervisors enable users to generate these segmented architecture models.

5.4 Alignment with Standards and Frameworks

Realistic content also means aligning training scenarios and objectives with recognized industry standards and security frameworks. Learners receive education and practice training that fulfills compliance requirements, together with established best practices. The training exercises need to link their obstacles to solutions that correspond with vital framework elements in NIST CSF 2.0 and NIST SP 800-82 Rev 3 and ISA/IEC 62443 Zones/Conduits and Security Levels and foundational requirements. The scenarios can include sector-specific compliance elements for specific audience members (e.g., NERC CIP for energy).

The simulated environment allows learners to practice applying framework principles through risk assessment (Identify), security control implementation (Protect), monitoring tool usage (Detect), incident response execution (Respond), system restoration (Recover), and

policy/risk strategy understanding (Govern). The Colonial Outpost Security Lab scenarios were explicitly developed for exercising controls throughout these domains.

5.5 Synthesis: Balancing Realism, Scope, and Learning Objectives

Perfect realism in all training environment dimensions (threats, processes, protocols, hardware specifics) proves difficult to achieve because of budget constraints and cost implications. The primary hurdle exists in determining the appropriate level of realism that must be completed to accomplish both learning objectives and operational efficiency. The focus on TTPs and their effects, together with the simulation of real adversary methods and operational attack outcomes, proves to be more beneficial for learning than using live malware or achieving physical replication. Training with protocols and architectures that are widely used in networks provides learners with widely applicable skills. Scenario-based training that follows industry standards makes content more relevant and helps learners meet real-world security requirements for compliance and security program standards. Easy content updates of threats, vulnerabilities, and protocols remain essential for maintaining long-term relevance because threats and technologies continuously evolve. Virtual, modular platforms excel here. A well-balanced approach to training content development should focus on practical skill-building through realistic methods, but must remain accessible and safe with clearly defined learning objectives.

Section 6: Systematization of Evaluation Methods for Training Effectiveness

6.1 Introduction: Measuring What Matters

The development of innovative platforms, pedagogies, and content for Industrial Control System (ICS) / Operational Technology (OT) security training is crucial, yet the actual impact of these training methods can only be determined through rigorous evaluation. The evaluation of training effectiveness when focusing on complex cognitive and practical skills, such as cybersecurity in high-stakes environments, is a significant challenge. Evaluation approaches need to move past basic completion metrics and self-assessment to properly measure the acquisition of knowledge and practical competencies, together with decision-making capabilities, as well as real-world application of skills. This section outlines the standard evaluation methods used to assess ICS/OT security training programs while reviewing their effectiveness and limitations through both literature examples and the Colonial Outpost Security Lab case study.

6.2 Taxonomy of Evaluation Methods

Evaluation approaches for technical and simulation-based training include several categories. Knowledge assessment measures the recall and understanding of concepts. Performance metrics quantify task execution efficiency and effectiveness within the training environment itself. Behavioral analysis involves observing and analyzing how learners approach tasks and make decisions during the simulation. Qualitative feedback and usability assessment

gather subjective user perceptions and identify any issues with the platform's usability. Finally, skill transfer assessment attempts to measure the application of learned skills in different contexts or real-world situations, which is often the most challenging aspect to evaluate.

6.3 Knowledge Assessment

6.3.1 Methods

This is usually done using traditional assessment tools given before or after the training. The assessment includes multiple-choice quizzes, short answer questions, or concept mapping exercises, which assess declarative knowledge about ICS terminology and protocol functions, standard requirements, and basic procedural knowledge about incident response plan steps.

6.3.2 Analysis

The main advantage of knowledge assessment is its simplicity and quantifiability, which makes it easier to measure theoretical understanding. The assessments help verify that learners have acquired the essential knowledge required to perform skills. The main drawback of these assessments is their inability to evaluate practical skills, critical thinking abilities, or performance under pressure. Knowledge test scores that reach a high level do not guarantee that learners will succeed in authentic situations.

6.4 Performance Metrics (In-Simulation)

6.4.1 Methods

Simulation platforms can automatically log and quantify learner actions and outcomes during scenarios, providing objective data on practical skill execution. Examples planned for the Colonial Outpost Security Lab evaluation include time-based metrics like Detection-to-Response Time (DTR), time-to-patch, or time-to-recover. Outcome-based metrics might track success/failure rates in achieving objectives, incident containment effectiveness, configuration accuracy, or the number and severity of simulated operational disruptions caused by learner actions or inaction. Efficiency metrics could analyze resource utilization, command efficiency, or adherence to procedural steps. Automated scoring based on predefined benchmarks, similar to ICSTASY's capabilities, is often employed.

6.4.2 Analysis

Performance metrics provide measurable proof of specific skills being used in the particular simulation environment. They are ideal for observing student growth over time and for evaluating both group and individual progress while pinpointing specific areas of deficiency (e.g., constant detection time delays). The performance metrics lack information about the decision-making process because rapid reactions may be random luck, and extended reactions might include deliberate thought processes. Establishing relevant non-gameable metrics demands precise scenario development.

6.5 Behavioral Analysis

6.5.1 Methods

Behavioral analysis focuses on the process of learner engagement rather than just the outcome. Techniques include detailed action/command logging, recording user interactions, commands used, and navigation patterns to reveal strategies or deviations. In team scenarios, communication analysis of chat logs or transcripts helps understand coordination, information sharing, and team dynamics. Think-aloud protocols, where learners verbalize their thoughts during a scenario, provide direct insight into their real-time reasoning and decision-making. Observational analysis involves trained observers noting specific behaviors, strategies, or difficulties encountered by learners.

6.5.2 Analysis

The behavioral analysis generates detailed qualitative information that reveals the causes behind performance results. The assessment methodology shows incorrect problem-solving approaches and successful methods, as well as group collaboration performance and mental pressure effects on decision-making. This additional assessment method enhances the understanding of cognitive functions beyond simple quantitative measures. The time required for analysis tends to be lengthy, particularly when working with think-aloud or communication data, while interpretation might involve personal biases.

6.6 Qualitative Feedback and Usability Assessment

6.6.1 Methods

Gathering learners' subjective experiences is done through various tools. Surveys and questionnaires use Likert scales and open-ended questions to assess perceived learning, engagement, realism, difficulty, confidence, and satisfaction; careful design regarding question sequence and type is essential. Interviews and focus groups allow for deeper exploration of user experiences and opinions through semi-structured discussions. Usability testing involves observing users interacting with the platform to identify interface issues, confusion points, or design flaws that might impede learning.

6.6.2 Analysis

The assessment of qualitative feedback provides essential information regarding learner experiences and detects learning barriers and interface complexity problems found in Colonial Outpost Security Lab pilots while evaluating perceived value and collecting improvement recommendations. Although subjective, it delivers essential user feedback that helps assess training effectiveness.

6.7 Skill Transfer Assessment

6.7.1 Methods

Measuring skill transfer—the ability to apply learned skills effectively in new contexts, especially the real world—is the ultimate goal, but is notoriously difficult. Direct assessment in operational settings is often impractical or unsafe. Researchers frequently rely on proxies, such as assessing performance on novel, unseen scenarios within the simulation that require adapting learned skills. Delayed post-tests measure knowledge or performance retention over time. Expert evaluation involves experienced practitioners rating learner performance in complex simulation scenarios. Self-report measures, like asking learners about their confidence in applying skills on the job, are also used but are considered relatively weak indicators.

6.7.2 Analysis

Training research faces a significant difficulty in assessing transfer alongside a well-documented gap that affects most studies about cybersecurity simulations. The majority of research focuses its assessment on student performance within training simulations. Demonstrating robust transfer requires carefully designed studies, often longitudinal, which are complex and resource-intensive.

6.8 Synthesis: Towards Holistic Evaluation

A robust, mixed-methods approach is most effective for evaluation. This involves combining objective performance metrics to quantify skill execution within the simulation, behavioral analysis to understand underlying decision-making processes, qualitative feedback to capture user experience, engagement, and usability insights, and knowledge assessments to measure foundational understanding.

Multiple data sources provide a more accurate and dependable assessment of learning outcomes and the impact of the training environment on student acquisition. Standardization of metrics between platforms and separation of pedagogical from platform elements and simulation validity and skill transfer measurement present ongoing challenges. The advancement of ICS/OT security training science demands resolution of these evaluation challenges.

Section 7: Discussion: Insights, Lessons Learned, and Open Problems

7.1 Introduction

A thorough evaluation of Industrial Control System (ICS) / Operational Technology (OT) security training platforms occurs in the preceding sections by analyzing training platforms and teaching methods, content realism, and evaluation methods (Section 6). This part combines essential findings from the research analysis to reveal major trends along with ongoing difficulties and vital learning points that help develop effective training programs. The analysis

combines data from research literature, industry reports, platform assessments, and the Colonial Outpost Security Lab case study to determine essential gaps and identify crucial research and development needs for this vital area.

7.2 Key Insights and Trends

Our systematization reveals several significant trends and insights shaping the field of ICS/OT security training:

7.2.1 Shift Towards Accessible Virtualization

The world is rapidly moving away from expensive, inflexible physical testbeds toward virtualized environments that especially use lightweight containerization (Docker, LXC). VICSORT, together with ICSSIM and Colonial Outpost Security Lab, shows how container-based solutions meet multiple essential requirements by providing cost-effective access to scalable and reproducible training, which expands learning possibilities for an enlarged student population. Virtualization has become the standard educational approach for delivering scalable instruction because high-fidelity physical or hybrid labs remain essential for particular research needs.

7.2.2 Embracing Active Learning Pedagogies

Traditional instruction methods no longer work for teaching practical cybersecurity competencies because they lack sufficient effectiveness. Modern training methods use active learning principles as their core teaching approach. Modern training approaches now use active learning principles to deliver effective instruction. Three fundamental learning methods derived from literature and implemented in Colonial Outpost Security Lab include Constructionism through defense creation, realistic threat-based Scenario-Based and Problem-Based Learning, and strategic Game-Based Learning/Gamification, which employs meaningful mechanics and narrative elements.

7.2.3 Focus on Functional Realism and Contemporary Threats

Virtual labs face ongoing challenges to reach perfect physical fidelity, but current efforts focus on delivering high functional realism. Training platforms must replicate standard ICS communication protocols, including insecure ones like Modbus, along with accurate depictions of network segmentation and operational constraints regarding uptime requirements and patching timeframes, as well as TTPs that match contemporary adversary tactics. Training materials need to include contemporary threats such as sophisticated APT frameworks (PIPEDREAM) and targeted ransomware instead of outdated attack models. Threat model maintenance stands as an accepted fundamental requirement.

7.2.4 Maturing Evaluation, but Transfer Remains Elusive

The field of evaluation continues to mature while the challenge of demonstrating real-world application of learned skills remains the most significant hurdle. Modern evaluation

techniques now employ automated metrics such as DTR and containment rates and behavioral analysis while advancing beyond basic knowledge assessments. A mixed-methods evaluation approach, which combines numerical metrics with feedback assessments (used for Colonial Outpost Security Lab evaluation), provides a more complete understanding of effectiveness. The most critical evaluation hurdle continues to be measuring the successful application of simulation-based skills in real-world work environments.

7.2.5 IT/OT Convergence Demands Integrated Training:

Training programs must integrate instruction for IT/OT environments because of the merging of these domains. Training programs need to address security issues of merged networks while teaching OT and IT personnel to communicate and develop combined security expertise. Training scenarios must present attacks that span between IT and OT domains and need synchronized responses from both teams.

7.3 Persistent Challenges and Gaps

Achieving high fidelity becomes difficult at scale because it remains costly and complex to access, especially when dealing with real-time constraints and diverse proprietary hardware emulation and complex physical process interactions, even with virtualization. The need to find equilibrium among these competing demands requires developers to make specific design decisions that suit particular learning objectives. Training alone cannot close the IT/OT skills and cultural gap because substantial organizational transformation, along with sustained leadership backing and continuous inter-departmental activities beyond training, is necessary to achieve integrated IT/OT security teams. The existing skills shortage exacerbates this problem. Training content remains relevant only when updates occur frequently because threats and vulnerabilities, along with technologies, change quickly. Training value decreases when institutions use static libraries as their only resource or when updates happen rarely. Open-source and community models serve as potential solutions, but their effectiveness depends on active maintenance efforts.

The assessment of intricate cognitive abilities like critical thinking, alongside ethical decision-making, adaptability, and teamwork, proves challenging when depending solely on automated evaluation systems. The implementation of observation together with AARs and think-aloud protocols proves beneficial yet expensive and difficult to scale. Implementation of complex teaching methods, including constructionism or simulation-based training, demands instructors who have expertise in ICS/OT security and education methodology. Training programs face challenges when seeking facilitators who have both technical and educational competencies. The transfer of skills from training to real operational environments remains the most significant research and evaluation gap, as Section 6.7 demonstrates.

7.4 Lessons Learned for Effective Training Design

Key lessons for design emerge: prioritize accessibility and scalability using virtualization and open-source tools. Mandate active, hands-on learning grounded in constructionist principles

and realistic scenarios (SBL/PBL). Engage learners through relevant context, narrative, and thoughtful motivation mechanics like GBL/Gamification, ensuring rewards align with security behaviors. Simulate the full incident response lifecycle, including often-neglected recovery stages: model IT/OT integration and collaboration in scenarios. Focus on functional realism, prioritizing plausible TTPs, common protocols, standard architectures, and realistic consequences, keeping threat models current. Integrate structured reflection and feedback opportunities like AARs. Adopt an iterative, data-driven design process using mixed evaluation methods to refine the training based on evidence.

Virtualization with containerization techniques, along with open-source tools, should be chosen because they reduce costs while reaching more learners. The design needs to accommodate deployment on standard hardware, together with cloud platforms. Active learning requires hands-on experiences from students instead of passive observation or reading. Training programs should use constructionist principles to have students construct security defenses while addressing problems in practical simulation-based learning (SBL/PBL). The combination of context and motivation techniques, along with game mechanics in GBL/Gamification systems, should be used to create intrinsic and extrinsic motivation among learners. The reward system needs to match the security behaviors that are expected from learners.

The training should simulate the complete IR lifecycle by including activities that span from detection through analysis to containment and eradication, and finally recovery, with a special emphasis on the often-ignored latter stages. The training should model how IT and OT systems integrate and how different roles need to work together through simulated NPCs or split-task scenarios. The training should focus on using realistic Tactics, Techniques, and Procedures (TTPs) as well as standard protocols and typical architectures, and realistic consequences rather than physical precision if trade-offs must be made. Keep threat models current. The system requires built-in opportunities for learners to review their actions together with their results through AARs and debriefs. The feedback needs to be immediate, along with being specific and practical. The evaluation should combine multiple methods to obtain data that helps reveal weaknesses that enable ongoing improvement of both the platform and its content and teaching methods.

7.5 Open Problems and Future Research Directions

Future research should address the gaps that emerge from identified weaknesses and educational findings. The study focuses on creating accurate yet efficient models for complex physical processes and real-time network interactions in virtual environments. Real system configurations need automated translation into virtual models as part of research efforts. The development of AI tutors should focus on creating two systems: AI opponents who adapt their actions through player input and AI tutors who offer customized scaffolding along with feedback based on student performance and behavioral patterns. The research aims to explore the best methods of combining virtual simulations with physical components (Hardware-in-the-Loop) for particular training goals while managing their complexity and cost implications. The development of assessment techniques using behavioral data and performance in complex novel

scenarios needs to be researched for validating improved transfer of higher-order skills to real-world applications.

The research should develop and analyze platform features and pedagogical structures that enhance distributed IT/OT security team learning, coordination, and communication. The research should perform rigorous comparative analyses to discover which specific teaching methods (game mechanics, narrative structures, reflection prompts) work best for various learning objectives and student groups in the ICS/OT domain. The research needs to develop sustainable models for content creation through open-source approaches or community-based initiatives to validate and disseminate high-quality training scenarios and platform modules. Continued research and development of open problems represents the essential pathway for better ICS/OT security training expansion across the world.

Section 8: Conclusion

The security of Industrial Control Systems (ICS) and Operational Technology (OT) that operate our critical infrastructure is of paramount global importance. But with the rising level of cyber threats targeting these environments alongside operational constraints and a persistent shortage of specialized skills, this is a significant challenge. To address this, it is necessary to have technological defenses as well as highly effective training methods to prepare a competent workforce. Given the fragmented nature of current training approaches and the need for clearer insights, this paper provided a systematization of knowledge on platforms, pedagogies, and practices for ICS/OT security education.

This systemization of knowledge has been developed by analysing academic literature, industry reports, existing training platforms (physical, hybrid, virtual), pedagogical theories, and the detailed design of a practical case study (the Colonial Outpost Security Lab environment). This systemization of knowledge has made several contributions to the analysis by presenting a categorization of training platforms, examining the critical trade-offs between fidelity, cost, scalability, and accessibility, and highlighting the significant advantages of modern containerized virtual labs (e.g., VICSORT, ICSSIM, the Colonial Outpost Security Lab architecture) for broad deployment. This systemization of knowledge has also systematized relevant pedagogical approaches, stressing the effectiveness of integrating active learning principles such as constructionism, scenario-based learning, and game-based learning over traditional instructionist methods. Furthermore, it analysed the crucial role of content realism and reviewed methods for evaluating training effectiveness, noting the persistent challenge of measuring real-world skill transfer.

Key insights derived include the clear trend towards accessible virtualization, the synergistic power of combining engaging pedagogy with realistic simulation, the necessity of focusing training on the whole incident response lifecycle within converged IT/OT contexts, and the critical importance of continuously updating content. Challenges persist, particularly in achieving high fidelity affordably, effectively bridging the IT/OT cultural gap, robustly assessing complex skills, and ensuring training content stays current.

In conclusion, this systematization suggests that the most promising path forward for practical ICS/OT security training is an integrated approach. These approaches should combine technically sound, accessible simulation platforms (using virtualization and open-source tools) with thoughtfully designed, active learning pedagogies (such as constructionism and game-based learning) that deliver realistic, scenario-based content that is aligned with contemporary threats and industry standards. The proposed Colonial Outpost Security Lab design is presented as a blueprint for such an integration. For the field to advance and critical infrastructure to become more secure, it is important to continue researching the open problems and to evaluate integrated designs like the Colonial Outpost Security Lab empirically.

Section 9: References

Ackermann, E. *Piaget's Constructivism, Papert's Constructionism: What's the Difference?* 2001. *Semantic Scholar*, https://www.semanticscholar.org/paper/Piaget-%E2%80%99-s-Constructivism-,-Papert-%E2%80%99-s-:-What-%E2%80%99-s-Ackermann/89cbcc1e740a4591443ff4765a6ae8df0fdf5554.

Aljundi, Ibrahem, et al. "Protecting Critical National Infrastructures: An Overview of Cyberattacks and Countermeasures." *Intelligent Sustainable Systems*, edited by Atulya K. Nagar et al., Springer Nature, 2024, pp. 295–317. *Springer Link*, https://doi.org/10.1007/978-981-99-7569-3_25.

Alves, Thiago, and Thomas Morris. "OpenPLC: An IEC 61,131–3 Compliant Open Source Industrial Controller for Cyber Security Research." *Computers & Security*, vol. 78, Sept. 2018, pp. 364–79. *ScienceDirect*, https://doi.org/10.1016/j.cose.2018.07.007.

Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Institute Electricity Information Sharing and Analysis Center, 18 Mar. 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf. National Security Archive.

APT Cyber Tools Targeting ICS/SCADA Devices | CISA. 25 May 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a.

Arnab, Sylvester, et al. *Pedagogy-Driven Design of Serious Games: An Overall View on Learning and Game Mechanics Mapping, and Cognition-Based Models*.

Assante, Mike. *The ICS Cybersecurity Leadership Cycle*.

Bicer, Ali, et al. "Moving from STEM to STEAM: The Effects of Informal STEM Learning on Students' Creativity and Problem Solving Skills with 3D Printing." *2017 IEEE Frontiers*

in Education Conference (FIE), 2017, pp. 1–6. *IEEE Xplore*, https://doi.org/10.1109/FIE.2017.8190545.

Bonvoisin, Jérémy, et al. "Standardisation of Practices in Open Source Hardware." *Journal of Open Hardware*, vol. 4, no. 1, 1, Aug. 2020. *ojs.lib.uwo.ca*, https://doi.org/10.5334/joh.22.

Byres, Eric, and Justin Lowe. *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*.

Carlson, Josh. "Unifying the IT/OT SOC with Intelligence-Driven Cybersecurity | Dragos." *Dragos*, 3 Sept. 2024, https://www.dragos.com/blog/unified-it-ot-soc-with-intelligence-driven-cybersecurity/.

Cherdantseva, Yulia, et al. "A Review of Cyber Security Risk Assessment Methods for SCADA Systems." *Computers & Security*, vol. 56, Feb. 2016, pp. 1–27. *ScienceDirect*, https://doi.org/10.1016/j.cose.2015.09.009.

CHERNOVITE's PIPEDREAM Targeting Industrial Control Systems (ICS). 13 Apr. 2022, https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/.

"CIS Adapts Critical Security Controls to Industrial Control Systems." *Tenable®*, 29 June 2018, https://www.tenable.com/blog/cis-adapts-critical-security-controls-to-industrial-control-systems.

"Constructionism (Learning Theory)." *Wikipedia*, 5 Feb. 2024. *Wikipedia*, https://en.wikipedia.org/w/index.php?title=Constructionism_(learning_theory)&oldid=1203563760.

Control Systems Are a Target | SANS Poster.

https://www.sans.org/posters/control-systems-are-a-target/. Accessed 30 Apr. 2025.

Cybersecurity Best Practices for Industrial Control Systems | CISA. 17 Dec. 2020, https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-industrial-control-systems.

Dehlaghi-Ghadim, Alireza, et al. "ICSSIM — A Framework for Building Industrial Control Systems Security Testbeds." *Computers in Industry*, vol. 148, June 2023, p. 103906. *ScienceDirect*, https://doi.org/10.1016/j.compind.2023.103906.

Dragos_Year-In-Review-Exec-Summary-2022.Pdf. https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf?hsLang=en. Accessed 30 Apr. 2025.

Ekisa, Conrad, et al. "VICSORT - A Virtualised ICS Open-Source Research Testbed." *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, 2022, pp. 1–8. *IEEE Xplore*, https://doi.org/10.1109/Cyber-RCI55324.2022.10032670.

ESET Research. "Industroyer2: Industroyer Reloaded." *We Live Security*, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/. Accessed 30 Apr. 2025.

European Network and Information Security Agency. *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing.* Publications Office, 2018. *DOI.org (CSL JSON)*, https://data.europa.eu/doi/10.2824/851384.

Ford, Simon, and Tim Minshall. *3D Printing in Education: A Literature Review*. *Zotero*, https://www.researchgate.net/publication/308204531_3D_printing_in_education_a_literature_review.

Formby, David, and Milad Rad. *Lowering the Barriers to Industrial Control System Security*

with GRFICS.

Gardiner, Joseph, et al. “Oops I Did It Again: Further Adventures in the Land of ICS Security Testbeds.” *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy - CPS-SPC’19*, ACM Press, 2019, pp. 75–86. *Crossref*, https://doi.org/10.1145/3338499.3357355.

Genge, Béla, et al. “A Cyber-Physical Experimentation Environment for the Security Analysis of Networked Industrial Control Systems.” *Computers & Electrical Engineering*, vol. 38, no. 5, Sept. 2012, pp. 1146–61. *ScienceDirect*, https://doi.org/10.1016/j.compeleceng.2012.06.015.

Gore, Karoline. *Cybersecurity for Industrial Control Systems: Best…* 28 June 2025, https://levelblue.com/blogs/security-essentials/cybersecurity-for-industrial-control-systems-best-practices.

Graffer, Ingrid, et al. *Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations*.

Green, Benjamin, et al. *{ICS} Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource*. 2020. *www.usenix.org*, https://www.usenix.org/conference/cset20/presentation/green.

Hanyu, Xiao, et al. “Exploring the Gamification of Cybersecurity Education in Higher Education Institutions: An Analytical Study.” *SHS Web of Conferences*, 2023.

Herold, Benjamin. “The Maker Movement in K-12 Education: A Guide to Emerging Research.” *Education Week*, 11 Apr. 2016. *www.edweek.org*, https://www.edweek.org/teaching-learning/the-maker-movement-in-k-12-education-a-guide-to-emerging-research/2016/04.

Hosseinzadeh, Salaheddin, et al. “Design and Development Considerations of a Cyber Physical Testbed for Operational Technology Research and Education.” *Sensors (Basel, Switzerland)*, vol. 24, no. 12, June 2024, p. 3923. *PubMed Central*, https://doi.org/10.3390/s24123923.

Hulsebos, Rob. *The Maroochy Incident, 18 Years Later | LinkedIn*. https://www.linkedin.com/pulse/maroochy-incident-18-years-later-rob-hulsebos/. Accessed 30 Apr. 2025.

Humayed, Abdulmalik, et al. *Cyber-Physical Systems Security -- A Survey*. arXiv:1701.04525, arXiv, 17 Jan. 2017. *arXiv.org*, https://doi.org/10.48550/arXiv.1701.04525.

Hurst, William, et al. “A Survey of Critical Infrastructure Security.” *Critical Infrastructure Protection VIII*, edited by Jonathan Butts and Sujeet Shenoi, Springer, 2014, pp. 127–38. *Springer Link*, https://doi.org/10.1007/978-3-662-45355-1_9.

ICS/OT Cybersecurity Year In Review 2022 Executive Summary. Dragos, 2023, https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Exec-Summary-2022.pdf?hsLang=en.

Jack, Hugh, and Scott C. Rowe. *Teaching Industrial Control with Open-Source Software*. 2023. *peer.asee.org*, https://peer.asee.org/teaching-industrial-control-with-open-source-software.

Jagoda, Patrick, et al. “Worlding through Play: Alternate Reality Games, Large-Scale Learning, and ‘The Source.’” *American Journal of Play*, vol. 8, no. 1, 2015, pp. 74–100.

Jones, David. “Dragos Warns of Novel Malware Targeting Industrial Control Systems | Cybersecurity Dive.” *Cybersecurity Dive*, 23 July 2024, https://www.cybersecuritydive.com/news/dragos-malware-industrial-control-systems/722

125/.

"Just Released! Dragos's 2023 OT Cybersecurity Year in Review Is Now Available | Dragos." *The Dragos Blog*, 20 Feb. 2024, https://www.dragos.com/blog/2023-ot-cybersecurity-year-in-review-now-available/.

Kesselring, Leslie. "Dragos OT Cybersecurity 'Year in Review' Reports Rise in Geopolitically Driven Attacks, Ransomware, and Threat Groups." *Business Wire*, https://www.businesswire.com/news/home/20240220296605/en/Dragos-OT-Cybersecurity-Year-in-Review-Reports-Rise-in-Geopolitically-Driven-Attacks-Ransomware-and-Threat-Groups. Accessed 30 Apr. 2025.

Knowles, William, et al. "A Survey of Cyber Security Management in Industrial Control Systems." *International Journal of Critical Infrastructure Protection*, vol. 9, June 2015, pp. 52–80. *ScienceDirect*, https://doi.org/10.1016/j.ijcip.2015.02.002.

Kovacs, Eduard. "ICS at Multiple US Water Facilities Targeted by Hackers Affiliated With Iranian Government." *SecurityWeek*, 4 Dec. 2023, https://www.securityweek.com/ics-at-multiple-us-water-facilities-targeted-by-hackers-affiliated-with-iranian-government/.

Krotofil, Marina, and Dieter Gollmann. "Industrial Control Systems Security: What Is Happening?" *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 2013, pp. 664–69. *IEEE Xplore*, https://doi.org/10.1109/INDIN.2013.6622963.

Labs, Keepnet. "The Power of Gamification in Security Awareness Training - Keepnet." *Keepnet Labs*, 12 Nov. 2024, https://keepnetlabs.com/blog/the-power-of-gamification-in-security-awareness-training.

Lee, Donghwan, et al. "ICSTASY: An Integrated Cybersecurity Training System for Military

Personnel." *IEEE Access*, vol. 10, 2022, pp. 62232–46. *IEEE Xplore*, https://doi.org/10.1109/ACCESS.2022.3182383.

Lee, Robert M., and Tim Conway. *The Five ICS Cybersecurity Critical Controls*.

Leinonen, Teemu, et al. "3D Printing in the Wild: Adopting Digital Fabrication in Elementary School Education." *International Journal of Art & Design Education*, vol. 39, no. 3, Aug. 2020, pp. 600–15. *Crossref*, https://doi.org/10.1111/jade.12310.

Matovu, Richard, et al. "Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges." *2022 IEEE Frontiers in Education Conference (FIE)*, 2022, pp. 1–9. *IEEE Xplore*, https://doi.org/10.1109/FIE56618.2022.9962519.

Miranda, Thiago da Cunha Rocha Devesa de. *Uso do SCADABR para desenvolvimento de sistemas supervisórios de processos químicos simulados*. Feb. 2022. *app.uff.br*, https://app.uff.br/riuff/handle/1/24591.

Miri, Mina. *ISAIEC-62443-Compliance-in-Industrial-Control-Systems*. Security Compass, https://www.securitycompass.com/whitepapers/isa-iec-62443-compliance-in-industrial-control-systems/. Accessed 30 Apr. 2025.

Mirkovic, Jelena, and Terry Benzel. *Teaching Cybersecurity with DeterLab*.

Morelli, Umberto. *An Open and Flexible CyberSecurity Training Laboratory in IT/OT Infrastructures*.

Muehlbauer, Melissa. "NIST SP 800-82 Revision 3 Highlights and Key Differences." *Secolve*, 5 Oct. 2023, https://secolve.com/nist-sp-800-82-revision-3-highlights-and-key-differences/.

Mukherjee, Madhav, et al. *Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes*.

Nadeem, Sarim. "How Gamification Closes The Cybersecurity Skills Gap." *Forbes*,

https://www.forbes.com/councils/forbestechcouncil/2025/02/26/the-growing-cybersecurity-skills-gap-a-breach-waiting-to-happen/. Accessed 30 Apr. 2025.

Nazir, Sajid, et al. “Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques.” *Computers & Security*, vol. 70, Sept. 2017, pp. 436–54. *ScienceDirect*, https://doi.org/10.1016/j.cose.2017.06.010.

Nicholson, A., et al. “SCADA Security in the Light of Cyber-Warfare.” *Computers & Security*, vol. 31, no. 4, June 2012, pp. 418–36. *ScienceDirect*, https://doi.org/10.1016/j.cose.2012.02.009.

NIST CSF 2.0: A Comprehensive Guide. 5 June 2024, https://sectrio.com/blog/comprehensive-guide-to-nist-csf-v2/.

Parsons, Dean. *The State of ICS/OT Cybersecurity in 2022 and Beyond*. no. October 2022, 2022. *Zotero*, https://hub.dragos.com/hubfs/Survey_ICSOT-Cybersecurity_Dragos.pdf?hsLang=en.

Pickard, John, et al. “IPv6 Security Course with Remote Labs - Design and Development.” *2013 ASEE Annual Conference & Exposition Proceedings*, ASEE Conferences, p. 23.834.1-23.834.11. *Crossref*, https://doi.org/10.18260/1-2--19848. Accessed 30 Apr. 2025.

Pillitteri, Victoria Y., et al. “Tailoring Security Controls for Industrial Control Systems.” *NIST*, Nov. 2015. *www.nist.gov*, https://www.nist.gov/publications/tailoring-security-controls-industrial-control-systems.

Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions. https://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx. Accessed 30 Apr. 2025.

Resnick, Mitchel. “Designing for Wide Walls. This Essay Was Originally Published In… | by Mitchel Resnick | Medium.” *Medium*, https://mres.medium.com/designing-for-wide-walls-323bdb4e7277. Accessed 30 Apr. 2025.

Ribeiro, Anna, Manjunath GH, et al. “Addressing ICS Cybersecurity Training amid Rising Adversarial Threats and Evolving Tactics.” *Industrial Cyber*, 19 Nov. 2023, https://industrialcyber.co/features/addressing-ics-cybersecurity-training-amid-rising-adversarial-threats-and-evolving-tactics/.

Ribeiro, Anna. “Dragos Detects Escalation in Adversarial Capabilities, as Pipedream Threat Group Widens Attack Competence.” *Industrial Cyber*, 14 Feb. 2023, https://industrialcyber.co/news/dragos-detects-escalation-in-adversarial-capabilities-as-pipedream-threat-group-widens-attack-competence/.

Ribeiro, Anna, Jonathon Gordon, et al. “Mounting Need for ICS Cybersecurity Professionals to Broaden Training, Break Barriers, While Closing Skills Gap.” *Industrial Cyber*, 22 Jan. 2023, https://industrialcyber.co/features/mounting-need-for-ics-cybersecurity-professionals-to-broaden-training-break-barriers-while-closing-skills-gap/.

Ribeiro, Anna. “New OPSWAT-SANS Survey Detects Growing Gap in ICS/OT Cybersecurity Budgets amid Rising Threats.” *Industrial Cyber*, 5 Mar. 2025, https://industrialcyber.co/reports/new-opswat-sans-survey-detects-growing-gap-in-ics-ot-cybersecurity-budgets-amid-rising-threats/.

Rodrigues Alves, Thiago, et al. “OpenPLC: An Open Source Alternative to Automation.” *IEEE Global Humanitarian Technology Conference (GHTC 2014)*, IEEE, 2014. *Crossref*,

https://doi.org/10.1109/ghtc.2014.6970342.

Salazar, M., et al. “Enhancing Cybersecurity Learning through an Augmented Reality-Based Serious Game.” *2013 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, 2013, pp. 602–07. *Crossref*, https://doi.org/10.1109/educon.2013.6530167.

SANS ICS Security - Control Systems Are a Target.

“Sans Icsps Ics418 0923 Web | PDF | Computer Security | Security.” *Scribd*, https://www.scribd.com/document/717025548/Sans-Icsps-Ics418-0923-Web. Accessed 30 Apr. 2025.

“SANS_5-Critical-Controls.Pdf on Egnyte.” *Egnyte*, https://sansorg.egnyte.com/dl/R0r9qGEhEe. Accessed 30 Apr. 2025.

Sauer, Felix, et al. *LICSTER -- A Low-Cost ICS Security Testbed for Education and Research*. 2019. *arXiv.org*, https://doi.org/10.14236/ewic/icscsr19.1.

Scarfone, Karen A., and Peter M. Mell. “Guide to Intrusion Detection and Prevention Systems (IDPS).” *NIST*, Feb. 2007. *www.nist.gov*, https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps .

Stouffer, Keith, et al. *Guide to Operational Technology (OT) Security*. NIST Special Publication (SP) 800-82 Rev. 3, National Institute of Standards and Technology, 28 Sept. 2023. *csrc.nist.gov*, https://doi.org/10.6028/NIST.SP.800-82r3.

Tao, Yaodong, et al. “Experience and Lessons in Building an ICS Security Testbed.” *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, 2019, pp. 1–6. *IEEE Xplore*, https://doi.org/10.1109/ICIAI.2019.8850804.

Tharot, Kanthanet, Quoc Duong, et al. “A Cybersecurity Training Concept for Cyber-Physical

Manufacturing Systems." *Procedia CIRP*, vol. Volume 120, no. 2023, pp. 1375–80. *Zotero*, https://doi.org/10.1016/j.procir.2023.09.179.

Tharot, Kanthanet, Quoc Bao Duong, et al. "A Low-Cost Environment for Teaching Fundamental Cybersecurity Concepts in CPS." *Systems, Software and Services Process Improvement*, edited by Murat Yilmaz et al., Springer Nature Switzerland, 2023, pp. 356–65. *Springer Link*, https://doi.org/10.1007/978-3-031-42307-9_25.

The Five ICS Cybersecurity Critical Controls Webcast. Directed by SANS ICS Security, 2023. *YouTube*, https://www.youtube.com/watch?v=tzDbaJiwt30.

Thompson, Lily A., et al. *Gamification in Cybersecurity Education; the RAD-SIM Framework for Effective Learning*.

Toll, William. "IEC 62443 in 2025: Network Segmentation Requirements and Changes." *Elisity Blog*, 7 Jan. 2025, https://www.elisity.com/blog/iec-62443-in-2025-network-segmentation-requirements-and-changes.

Un Concept de Formation à La Cybersécurité Pour Les Systèmes de Fabrication Cyber-Physiques Dans l'environnement Des Usines d'enseignement En France - Fondation Grenoble INP. https://fondation-grenoble-inp.fr/en/projet/a-cybersecurity-training-concept-for-cyber-physical-manufacturing-systems-within-teaching-factory-environment-in-france/. Accessed 30 Apr. 2025.

Zambrano, Xiomara, et al. "Sistema de bombeo de agua para riego mediante la aplicación de tecnologías de la Industria 4.0." *Maestro y Sociedad*, May 2024, pp. 125–37.