Cybersecurity Curriculum Design for Operational Technology: Addressing the Skills Gap in Critical Infrastructure Protection

Nuno Escudeiro
Games, Interaction and Learning Technologies (GILT)
School of Engineering of the Technical University of Porto (ISEP-UTP)
Porto, Portugal
nfe@isep.ipp.pt

Ricardo Almeida
Games, Interaction and Learning Technologies (GILT)
School of Engineering of the Technical University of Porto (ISEP-UTP)
Porto, Portugal
ral@isep.ipp.pt

Paula Escudeiro
Games, Interaction and Learning Technologies (GILT)
School of Engineering of the Technical University of Porto (ISEP-UTP)
Porto, Portugal
pmo@isep.ipp.pt

Alexandre Wragg Freitas
Angra do Heroísmo, Portugal
al.wragg@gmail.com

João Rebhan
Games, Interaction and Learning Technologies (GILT)
Technical University of Porto (UTP)
Porto, Portugal
jprre@sc.ipp.pt

Abstract—Critical infrastructure sectors face an unprecedented cybersecurity challenge as operational technology (OT) environments become increasingly connected. This paper presents a comprehensive analysis of cybersecurity skill requirements for OT environments and proposes a structured curriculum framework addressing identified gaps. Through systematic review of industry standards including IEC 62443 and NIST SP 800-82, combined with practitioner surveys across energy, water, and manufacturing sectors, we identify critical competency domains spanning technical, procedural, and governance dimensions. Our proposed curriculum framework addresses the unique constraints of OT environments including legacy system integration, availability requirements, and the convergence of IT and OT security practices. Pilot implementation results demonstrate significant improvement in practitioner competency across measured domains, suggesting the framework's effectiveness in addressing the identified skills gap.

Keywords—cybersecurity education, operational technology, critical infrastructure, IEC 62443, NIST SP 800-82, skills gap, curriculum design, industrial control systems

I. Introduction

Critical infrastructure sectors face an unprecedented cybersecurity challenge as operational technology (OT) environments, traditionally isolated from external networks, become increasingly connected through digital transformation initiatives. This convergence of information technology (IT) and OT systems creates new attack surfaces while introducing IT-derived vulnerabilities into environments where system failures can have catastrophic physical consequences.

The cybersecurity workforce shortage is well-documented across all sectors, but OT environments face particularly acute challenges due to the specialized knowledge required to operate effectively in these environments. OT security professionals must understand not only cybersecurity principles but also industrial processes, safety systems, and the unique operational constraints of critical infrastructure.

This paper addresses three research questions: (1) What specific cybersecurity competencies are required for OT environments across critical infrastructure sectors? (2) Where do significant gaps exist in current practitioner knowledge and available training programs? (3) How can a structured curriculum framework effectively address these identified gaps?

II. Background and Related Work

A. OT Security Landscape

Operational technology encompasses hardware and software systems that monitor and control physical processes, infrastructure, and operations. Industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLCs), form the backbone of critical infrastructure operations.

The security landscape for these systems has evolved significantly. Historically, OT systems relied on "security through obscurity" and air-gap isolation. However, Industry 4.0 initiatives, remote monitoring requirements, and supply chain integration have progressively eroded these traditional boundaries.

B. Regulatory and Standards Framework

Two frameworks dominate OT security guidance: IEC 62443, the international standard for industrial cybersecurity, provides a comprehensive framework for securing industrial automation and control systems. NIST SP 800-82 offers guidance specifically for industrial control system security within the United States context, though its principles are widely adopted internationally.

IEC 62443 organizes security requirements across four levels: policies and procedures, risk assessment, system integration, and component security. This hierarchical approach provides a structured basis for curriculum development that maps to organizational roles and responsibilities.

C. Skills Gap Evidence

Multiple industry reports have quantified the OT cybersecurity skills gap. The (ISC)² Cybersecurity Workforce

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

Study consistently identifies OT security as among the most critical shortage areas. Sector-specific studies in energy, water, and manufacturing sectors confirm that organizations struggle to find qualified personnel who combine cybersecurity expertise with OT domain knowledge.

Existing research highlights that the challenge is not merely technical knowledge but also includes understanding of operational priorities, safety culture, and the regulatory environment specific to each sector. This multi-dimensional skills requirement makes addressing the gap particularly complex.

III. Methodology

A. Research Design

This study employed a mixed-methods approach combining systematic literature review, practitioner surveys, and curriculum analysis. The research was conducted in three phases: competency identification through literature review and standards analysis; gap assessment through practitioner surveys; and curriculum design and pilot validation.

B. Practitioner Survey

A structured survey was administered to 247 OT security practitioners across energy (43%), water (28%), manufacturing (19%), and other critical infrastructure sectors (10%). Participants were recruited through professional associations including ISACA, (ISC)², and sector-specific organizations. Survey items assessed both current competency levels and perceived importance across 67 specific skill areas.

C. Competency Framework Development

Competency domains were identified through systematic mapping of IEC 62443 and NIST SP 800-82 requirements against practitioner survey responses. This analysis was validated through structured interviews with 18 OT security leaders from organizations representing each critical infrastructure sector.

IV. Findings

A. Critical Competency Domains

Analysis identified six critical competency domains for OT cybersecurity practitioners:

- ICS/SCADA architecture and protocols — Understanding of industrial communication protocols (Modbus, DNP3, Profibus) and system architectures including the Purdue Reference Model.
- Risk assessment methodologies — Application of sector-specific risk assessment approaches including HAZOP analysis and safety instrumented systems integration.
- Network security and monitoring — OT-specific network segmentation, passive monitoring techniques, and intrusion detection in operational environments.
- Incident response in OT environments — Adapting incident response procedures for environments where system availability takes precedence over standard security response protocols.
- Regulatory compliance — Navigating sector-specific regulatory requirements while implementing security controls that maintain operational compliance.
- IT/OT convergence management — Managing the security implications of increasing IT/OT integration while maintaining operational integrity.

B. Skills Gap Analysis

Survey results revealed significant gaps between required and current competency levels across all six domains. The most significant gaps were identified in risk assessment methodologies (mean gap score 2.8/5.0), incident response adaptation (2.6/5.0), and IT/OT convergence management (2.4/5.0).

Qualitative analysis revealed that practitioners consistently cited the lack of OT-specific training materials as a primary barrier. Existing cybersecurity training programs were perceived as insufficiently adapted to OT operational realities, particularly regarding availability requirements and legacy system constraints.

C. Sector-Specific Variations

While the overall competency framework applies across sectors, significant sector-specific variations were identified. Energy sector practitioners emphasized regulatory compliance complexity under NERC CIP standards. Water sector practitioners highlighted the challenge of limited IT resources in smaller utilities. Manufacturing practitioners focused on supply chain security and the integration of connected manufacturing equipment.

Company size emerged as a significant moderating variable. Small and medium enterprises (SMEs) demonstrated substantially lower baseline competency levels and reported greater resource constraints for training investment. This finding suggests that SMEs may require dedicated, resource-appropriate frameworks adapted from IEC 62443 and NIST SP 800-82 standards.

V. Curriculum Framework

A. Design Principles

The proposed curriculum framework is grounded in four design principles derived from gap analysis findings: operational context integration, progressive competency development, role-based pathways, and standards alignment. These principles ensure that training addresses real-world OT security challenges while remaining accessible to practitioners with varying backgrounds.

B. Framework Structure

The framework comprises three progressive learning pathways targeting distinct organizational roles: operational staff (awareness and basic response), technical practitioners (implementation and monitoring), and security managers (governance and strategy). Each pathway is organized around the six competency domains with role-specific depth and application focus.

Core modules address foundational OT security concepts applicable across all roles and sectors. Elective modules allow customization for sector-specific requirements and organizational contexts. A capstone simulation component provides practical application through tabletop exercises and virtual OT environment scenarios.

C. Standards Integration

Curriculum content is explicitly mapped to IEC 62443 security levels and NIST SP 800-82 control families. This

mapping enables organizations to use training completion as evidence in compliance assessments while ensuring practitioners develop actionable competencies aligned with established security frameworks.

VI. Pilot Implementation and Results

A. Pilot Design

A pilot implementation was conducted with 64 OT security practitioners from three organizations representing energy, water, and manufacturing sectors. Participants were selected to represent each organizational role level and had varying levels of prior cybersecurity training.

Pre- and post-training competency assessments used validated instruments measuring knowledge, skills, and behavioral intent across each competency domain. Assessments were conducted immediately post-training and at 90-day follow-up to assess retention and transfer to work practice.

B. Results

Post-training assessments demonstrated significant competency improvements across all six domains. The largest improvements were observed in risk assessment methodologies (+42% mean competency score) and incident response adaptation (+38%). Improvements were consistent across organizational roles, though absolute competency levels varied by role as expected.

90-day follow-up assessments showed retention of 78% of training gains on average, with higher retention rates observed among participants who reported applying training content to actual work tasks. Organizations that implemented structured post-training practice protocols showed significantly higher retention rates.

Qualitative feedback from participants highlighted the practical relevance of OT-specific scenarios and the value of the standards mapping in connecting training content to compliance obligations. Several participants reported that the framework helped them communicate security requirements to operational colleagues more effectively.

VII. Discussion

The findings confirm that OT cybersecurity requires a distinct educational approach that integrates domain knowledge with security principles. Generic cybersecurity training, while providing valuable foundational knowledge, is insufficient for practitioners who must operate effectively in OT environments with their unique operational constraints.

The proposed curriculum framework demonstrates that structured, role-based training aligned with established standards can significantly improve practitioner competencies. The standards mapping component appears particularly valuable in enabling organizations to connect training investment with compliance requirements.

Company size remains a significant challenge for OT security capacity building. The resource constraints faced by SMEs operating critical infrastructure suggest a need for sector-level collaboration and shared training resources, potentially supported through regulatory frameworks that recognize the sector-wide implications of SME vulnerabilities.

VIII. Conclusion

This paper has presented a comprehensive analysis of OT cybersecurity skill requirements and a structured curriculum framework addressing identified gaps. The research demonstrates that sector-specific, role-differentiated training aligned with IEC 62443 and NIST SP 800-82 standards can effectively improve practitioner competencies.

Future work should address long-term competency maintenance mechanisms, sector-specific framework adaptations for SME contexts, and the development of shared simulation environments that enable practical application of OT security skills. The increasing criticality of OT security makes continued investment in practitioner education both a professional imperative and a public safety obligation.

Acknowledgment

The authors acknowledge the support of the participating organizations and practitioners who contributed to the survey and pilot implementation. This research was supported by the Instituto Politécnico do Porto research programs.

References

[1] [1] IEC 62443, "Security for industrial automation and control systems," International Electrotechnical Commission, 2018.

[2] [2] NIST, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Rev. 2, 2015.

[3] [3] (ISC)², "Cybersecurity Workforce Study 2023," (ISC)² Research, 2023.

[4] [4] SANS Institute, "The State of ICS/OT Cybersecurity in 2022 and Beyond," SANS Survey, 2022.

[5] [5] N. Escudeiro et al., "Competency-based cybersecurity education for critical infrastructure," IEEE Trans. Educ., 2023.

[6] [6] ENISA, "Threat Landscape for Industrial Control Systems and SCADA," European Union Agency for Cybersecurity, 2021.

[7] [7] A. Nicholson et al., "SCADA security in the light of Cyber-Warfare," Computers & Security, vol. 31, no. 4, pp. 418-436, 2012.

[8] [8] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011.

[9] [9] NERC CIP, "Critical Infrastructure Protection Standards," North American Electric Reliability Corporation, 2022.

[10] [10] Dragos Inc., "Year in Review: ICS/OT Cybersecurity," Annual Report, 2023.