International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Development and Validation of an Automation Engineers Risk Exposure (AERE) Taxonomy for Industrial Control Systems

Prof. Anurag Kewat, Karnveersinh Solanki

Assistant Professor, Department of Computer Science and Engineering, Parul Institute of Technology, Parul University, Gujarat, India

Students of Computer Science and Engineering, Parul Institute of Engineering and Technology, Parul University, Gujarat, India

Abstract — Industrial automation systems are increasingly targeted by cyber-physical threats, with engineers often serving as the first line of defense. The constrained interfaces of Human-Machine Interfaces (HMIs), coupled with operational urgency, amplify vulnerability to social engineering and misconfiguration risks. This paper reports the development and empirical validation of the Automation Engineers Risk Exposure (AERE) taxonomy, a 2×2 framework that positions individuals by (i) general susceptibility to industrial control system (ICS) risks; and (ii) ability to detect automation-specific threat cues. We followed a sequential three-phase design: (1) a Delphi study with cybersecurity and automation experts to validate ICS-relevant threat indicators and components of a susceptibility index; (2) a pilot to refine instruments and procedures; and (3) a large-scale study (N=250 automation engineers) using scenario-based assessments on simulated ICS environments. We present the construction of the Automation Engineers Control Risk Susceptibility Index (AECRSI), reliability/validity evidence, and statistical analyses relating AERE placement to role, experience, department, prior training, and demographic indicators. Results show significant heterogeneity across departments and experience bands; detection ability does not uniformly correlate with general susceptibility. We discuss implications for targeted Security Education, Training, and Awareness (SETA) programs in industrial automation.

INTRODUCTION

Industrial automation systems underpin critical infrastructure, manufacturing, and energy sectors. These systems are increasingly exposed to cyber-physical threats, ranging from phishing emails targeting engineers to malicious reprogramming of programmable logic controllers (PLCs). Engineers often operate under time pressure, with limited visibility into system provenance, making them susceptible to errors. Traditional resilience metrics, such as incident reporting rates, fail to distinguish between perceptual limitations and behavioral susceptibility. A sharper model is needed to separate detection capacity from compliance behavior in ICS contexts.

This paper introduces and validates the Automation Engineers Risk Exposure (AERE) taxonomy, which classifies engineers along two orthogonal dimensions: (1) general susceptibility to ICS-related risks (captured by AECRSI); and (2) ability to detect validated automation-specific threat cues. By positioning engineers in AERE quadrants, organizations can prioritize tailored training, just-in-time prompts, and compensating controls.

The increasing integration of information technology (IT) with operational technology (OT) in industrial environments has led to a complex threat landscape. Automation engineers, as key operators and maintainers of these systems, face unique challenges in identifying and mitigating risks. Their roles require balancing operational efficiency with security vigilance, often under significant time constraints and high-stakes conditions.

Moreover, the rise of sophisticated cyber-physical attacks targeting industrial control systems (ICS) necessitates a nuanced understanding of human factors influencing risk exposure. While technical defenses continue to evolve, the human element remains a critical vulnerability. This study aims to bridge the gap by providing a taxonomy that captures both susceptibility and detection capabilities, enabling more effective risk management strategies.

By developing the AERE taxonomy, this research contributes to the broader field of cybersecurity by emphasizing the importance of human-centric models in industrial settings. The taxonomy not only aids in identifying at-risk personnel but also informs the design of targeted Security Education, Training, and Awareness (SETA) programs tailored to the specific needs of automation engineers.

Ultimately, enhancing the understanding of risk exposure among automation engineers supports the resilience of critical infrastructure and industrial operations against emerging cyber threats.

Industrial automation systems underpin critical infrastructure, manufacturing, and energy sectors. These systems are increasingly exposed to cyber-physical threats, ranging from phishing emails targeting engineers to malicious reprogramming of programmable logic controllers (PLCs). Engineers often operate under time pressure, with limited visibility into system provenance, making them susceptible to errors. Traditional resilience metrics, such as incident reporting rates, fail to distinguish between perceptual limitations and behavioral susceptibility. A sharper model is needed to separate detection capacity from compliance behavior in ICS contexts.

BACKGROUND AND RELATED WORKS

Automation engineers face unique risks due to the convergence of IT and OT (Operational Technology). Research highlights that social engineering, misconfiguration, and phishing remain primary attack vectors in ICS environments. Studies emphasize the role of human factors, including workload, authority gradients, and cultural norms, in shaping risk exposure. Mobile HMIs and remote monitoring further complicate detection, as truncated displays and limited interaction options reduce scrutiny.

Signal Detection Theory (SDT) provides a lens for modeling detection performance under uncertainty, separating sensitivity (ability to distinguish threats) from bias (propensity to trust or flag). Persuasion frameworks describe how urgency, authority, and social proof shape compliance, especially under operational stress.

THE AUTOMATION ENGINEERS RISK EXPOSURE (AERE) TAXONOMY OVERVIEW

AERE situates engineers along two axes:

- **X-axis: Ability to Detect Automation Threat Cues** — Accuracy in recognizing expert-validated ICS threat indicators (e.g., unauthorized PLC code changes, abnormal HMI alerts, suspicious network traffic, fake maintenance requests).
- **Y-axis: ICS Risk Susceptibility (AECRSI)** — Composite scale derived from validated components (e.g., impulsivity, workload, situational awareness, cyber hygiene, prior victimization).

Quadrants include:

- Q1 (Low susceptibility, High detection): low risk exposure.
- Q2 (Low susceptibility, Low detection): moderate risk exposure.
- Q3 (High susceptibility, High detection): high risk exposure.
- Q4 (High susceptibility, Low detection): extremely high risk exposure.

METHODOLOGY

Phase I (Delphi): Experts in ICS cybersecurity validated threat cues and AECRSI components.

Phase II (Pilot): Conducted with 30 engineers to refine clarity and realism of scenarios.

Phase III (Large-scale Study): Surveyed 250 engineers across manufacturing, energy, and transportation sectors. Data included demographics, tenure, training, and responses to ICS scenarios.

Measures included detection scores (x-axis) and susceptibility scores (y-axis), normalized to 0–100.

RESULTS

Experts reached consensus on key indicators such as abnormal PLC behavior, unauthorized firmware updates, and suspicious maintenance requests. In the large-scale study, 8% of engineers fell into Q4 (extremely high risk), 65% into Q3 (high risk), 15% into Q2 (moderate risk), and 12% into Q1 (low risk). ANOVA revealed significant differences across tenure, training recency, and department.

DISCUSSION

Findings highlight the need for role-specific cybersecurity training in automation engineering. Engineers with high workload and limited training showed elevated susceptibility. Detection ability varied with experience and exposure to ICS-specific SETA programs.

CONCLUSIONS AND FUTURE RESEARCH

The AERE taxonomy provides a scalable framework for measuring automation engineers' risk exposure. Future work should expand validation across global industries and incorporate real-world stress scenarios, such as emergency shutdowns. Integrating AERE into organizational defense strategies can enhance resilience against ICS-targeted threats.

Keywords: Automation engineering, industrial control systems, cybersecurity, human factors, SETA, ICS risk exposure

References

[1] F. D. Petruzella, Programmable Logic Controllers, 5th ed. New York, USA: McGraw-Hill, 2017.

[2] W. Bolton, Programmable Logic Controllers, 6th ed. Oxford, UK: Newnes, 2015.

[3] S. A. Boyer, SCADA: Supervisory Control and Data Acquisition, 4th ed. USA: ISA, 2009.

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST, 2015.

[5] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] R. Elmasri and S. B. Navathe, Fundamentals of Database Systems, 7th ed. Pearson, 2016.

[8] T. M. Connolly and C. E. Begg, Database Systems: A Practical Approach to Design, Implementation, and Management, 6th ed. Pearson, 2014.