Chemeca 2025 and Hazards Australasia
28 – 30 September, Adelaide, South Australia

The Importance of Cyber Risk in Industrial Systems: Integrating Process Hazards Analysis and Cyber Risk for Resilient Operations

Author(s) Name

Paresh Lalji Kerai

Affiliation(s)

exida

E-mail

pkerai@exida.com

ABSTRACT

The convergence of operational technology (OT) and information technology (IT) has heightened the vulnerability of industrial control systems (ICS) to cyber threats, making cyber risk a critical concern for process safety and operational resilience. Traditional risk management frameworks often neglect the dynamic nature of cyber threats, which can jeopardise functional safety and result in hazardous process conditions.

The presentation delves into integrating functional safety and cyber process hazard analysis (CyberPHA) methodologies to strengthen industrial cybersecurity risk assessments. It emphasises how cyber-induced failures can affect safety instrumented systems and other protective layers, elevating the risk of cascading failures in critical infrastructure. The discussion covers best practices for evaluating cyber risks in safety-critical environments, utilising CyberPHA methodologies to systematically identify and mitigate vulnerabilities in industrial automation and control systems (IACS).

Organisations can bridge the divide between traditional process safety and contemporary cyber risk management by aligning cybersecurity measures with IEC 61508, IEC 62443, and ISA/IEC 61511 standards. This strategy ensures that cyber-physical threats are incorporated into hazard and operability studies (HAZOPs), layer of protection analysis (LOPA), and safety lifecycle management, ultimately enhancing the resilience of industrial operations.

KEY WORDS

Include any key words

BIOGRAPHY

Mr Kerai is a strategic technology and Senior OT cybersecurity engineer who has worked with leading-edge cyber security and threat intelligence solutions for both Industrial Control Systems and Enterprise networks. He has extensive experience, including an academic and practical deep understanding of computer and network security, with skills aligned with enterprise and industrial cyber security solutions focusing on SCADA/ICS security.

Within excess of 10 years of computer, network security and industrial control system experience, Mr Kerai continues to research emerging technologies being developed globally within the cyber security domain and actively attends and speaks at cyber security conferences. Mr Kerai has provided expert consultation for both private and government sectors in various security standards, including IEC 62443 standards, NIST CSF, SOCI Act, AESCF, and ISO 27001 standards.