Chemeca2026
Innovate. Integrate. Impact.
28 – 30 September 2026
Melbourne, Australia

Hazards
Australasia 2026

Chemeca 2026 and Hazards Australasia
28 – 30 September, Melbourne, Australia

From Accidental Exposure to Deliberate Attack: The Emerging Cyber Threat to Process Safety

Shyamal Sharma & Paresh Keari

MWS Risk Pty Ltd

Shyamal.Sharma@mwsrisk.com | Paresh.Kerai@mwsrisk.com

ABSTRACT

Industrial control systems are becoming increasingly connected to networks beyond the traditional plant boundary. Once largely isolated, control environments are now integrated with corporate networks, remote operations platforms, cloud services, and systems that exchange operational data in real time. While this connectivity provides significant benefits in operational visibility, efficiency, and asset optimisation, it also introduces new risks to systems responsible for controlling hazardous industrial processes.

In the early years of industrial cyber incidents, attacks affecting control systems were often inadvertent, with industrial environments becoming collateral damage from malware targeting common operating systems and enterprise networks. Over time, however, cyber activity has evolved from opportunistic disruption to deliberate attempts by malicious actors to influence or compromise industrial systems and operational technology environments.

Incidents such as Stuxnet and the TRITON malware demonstrated that cyber capabilities can directly target industrial control and safety systems, highlighting the potential for cyber activity to influence physical industrial processes. More recent cyber attacks against critical infrastructure, often occurring alongside geopolitical tensions, further illustrate how these capabilities can disrupt communications, degrade operational capability, and interfere with essential services. These events demonstrate techniques that may also be adopted by malicious actors targeting industrial environments.

The rapid advancement of Artificial Intelligence is beginning to influence both offensive and defensive aspects of cybersecurity. AI technologies are enabling automated vulnerability discovery, accelerated attack development, and more sophisticated social engineering, while also supporting advanced detection and anomaly monitoring within industrial networks. This acceleration is likely to increase both the pace and sophistication of cyber threats targeting operational technology environments.

As cyber threat generation capabilities become more accessible and increasingly sophisticated, the implications for industrial operations and process safety are becoming more significant. For process safety practitioners, cyber threats represent another potential initiating cause of hazardous scenarios within complex industrial systems. Understanding how digital vulnerabilities translate into operational and safety risks highlights the importance of integrating cyber considerations into established process safety and risk management practices.

KEY WORDS

Process Safety; Industrial Control Systems (ICS); Operational Technology (OT) Cybersecurity; Safety Instrumented Systems (SIS); Cyber-Physical Risk; Critical Infrastructure; Critical Assets; Industrial Cybersecurity; Process Hazard Analysis

BIOGRAPHY

Shyamal Sharma – Director, MWS Risk

Shyamal Sharma is a Director at MWS Risk and a Chartered Professional Engineer specialising in control systems engineering, functional safety, and technical risk management. With more than 20 years of experience in the design, engineering, and commissioning of process control and safety systems, he has supported major projects across the energy, resources, mining, infrastructure, and industrial sectors.

Shyamal is a TÜV Certified Functional Safety Engineer and an approved Hazard Specialist with extensive experience in safety instrumented systems, hazardous area engineering, and process safety studies. His work focuses on helping organisations manage operational and safety risks associated with complex industrial systems, including the interaction between control systems, safety systems, and emerging cyber threats to industrial operations.

Paresh Kerai – OT Cyber Security Lead, MWS Risk

Paresh Kerai is an Operational Technology (OT) cyber security specialist with experience supporting critical infrastructure and industrial organisations to strengthen the security of control systems and digital operations. His work focuses on cyber risk assessments, governance frameworks, and the implementation of security standards such as IEC 62443 and the NIST Cybersecurity Framework.

Paresh has worked across the energy, resources, utilities, and broader industrial sectors, helping organisations improve the security and resilience of control systems and safety-critical environments. He works closely with engineering and operational teams to identify cyber risks, develop practical mitigation strategies, and strengthen the resilience of industrial systems while aligning cyber security with broader operational and safety objectives.

CONFERENCE PROGRAM

Please indicate which conference program your abstract relates to:

☒ Hazards Australasia

☐ Chemeca