KPMG

Securing Industrial Control Systems

Be in a defensible position.
Be cyber resilient.

Cyber attacks to Industrial Control Systems (ICS) are becoming common. Critical sectors like oil & gas, power & utilities, chemicals, transportation, mining, and pharma/food manufacturing must improve their cyber security to help ensure availability and safety of their operations and products.

Species such as the silk floss trees have adapted to ward off threats in the most challenging environments. Organizations also need to protect, detect and respond to ever-changing threats.

Why cyber attacks to Industrial Control Systems (ICS) matter

Typical attacks to Industrial Control Systems (ICS) can be divided into two categories:

- **Cyber-physical attacks** to Process Control Systems (PCS), Distributed Control Systems (DCS), and Supervisory Control and Data Acquisition (SCADA), with focus on components like programmable logic controllers (PLC), Human Machine Interface (HMI), and their infrastructure. These attacks aim at causing:
  - Unauthorized changes in product specification, generating business loss and threatening end-users
  - Unplanned disruption of production or destruction of equipment, interrupting business and resulting in financial and reputational loss
  - Unmanaged safety risks to employees and surrounding communities
- **Industrial espionage attacks** to components and systems like Data Historians and Distributed Control Systems (DCS), and their databases. These attacks aim at stealing:
  - Confidential information on product recipes, allowing competitors to obtain industrial secrets
  - Key process data impacting efficiency and productivity, eroding competitive advantage
  - Bulk production and inventory data, allowing market manipulation and weakening negotiation positions

Why should Boards and Management be concerned?

Typically, visibility over ICS cyber risks and security capabilities is limited at the Board and Management level, often with reports that 'all is well'. Some operations teams believe they are safe because they have safety systems in place, their ICS is air-gapped and not connected to other networks, their operation control rooms are staffed 24x7, or they still use old platforms and serial connections.

This is not enough. Recent cyber-attacks involving power plants, pipelines, steel mills, and other critical infrastructure have proven that these measures are not 100% effective to prevent disruption and destruction from cyber attacks.

How can KPMG help you build a defensible position?

Assessing Risks and Capabilities

Using established methodologies, international standards and experience, we assist Boards and Management to understand their business cyber risk and existing capabilities, and set an evolutionary path and roadmap to a defensible position.

Improving Governance

Often the management of operational and information technology (OT and IT) is undertaken by separate teams with different drivers and reporting lines. We help bridge the gap between teams and reduce uncertainty over responsibilities.

Building Assurance

From point-in-time ICS-specialized security testing to creating ICS-inclusive Internal Audit programs and Governance, Risk and Controls (GRC) integration, we help improve continuous monitoring and reporting to Boards and Management.

Delivering Transformation

Cyber threats evolve at a faster pace than ICS technology and there is a shortage of resources with both strong ICS and cyber security skills. We help bring specialized knowledge, sound program and project management practices.

How we have helped others

Oil & Gas Company

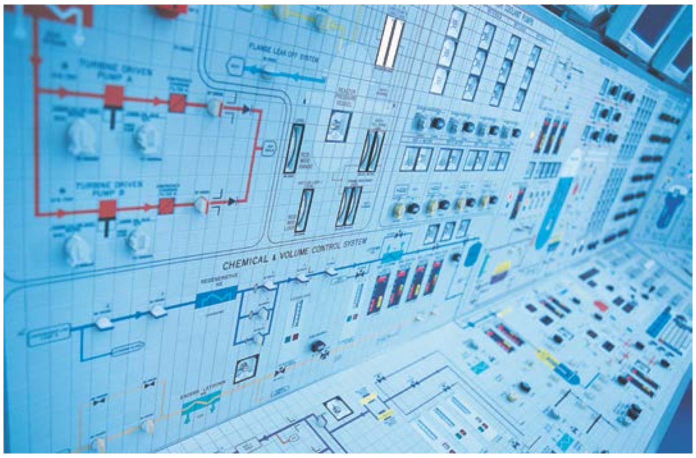
Increasing demands for security highlighted the need for a large oil and gas company in Canada to test their SCADA/DCS infrastructure used to control pipelines and gas plants in their US operations. KPMG provided a team of global and local (Canada/US) ICS security testing professionals who were able to assess, test, and review the current state of technical security found at the client's facilities. KPMG also provided risk-prioritized improvement recommendations.

Mining & Chemicals

The Management Committee of this Canadian mining and chemicals organization wanted to understand the cyber threats to their business and the state of their cyber security posture in order to start developing an overall strategy to improve the security on its IT and ICS. KPMG helped in facilitating Cyber Risk workshops to Management, while delivering a Cyber Maturity Assessment of their plants based on NIST Cyber Security Framework (CSF).

Power & Utilities

This Canadian power generation company's Internal Audit team needed to report on the cyber security their major plant's DCS. With a team of both local and global ICS security testing professionals, KPMG was able to identify several security vulnerabilities in the DCS environment and demonstrate potential avenues that could compromise or disrupt the power plant's operations. Many of the issues uncovered were unknown to their ICS vendors.



Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

We believe cyber security should be about what you CAN DO – not what you can't.

Award winning

KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 .

The KPMG Cyber team won the Canadian Lawyer Cyber Security Award 2016 .

Independent

Our recommendations and technical strategies are based solely on what is the best fit and most appropriate for your business. KPMG in Canada is not restricted to any technology or software vendor.

Collaborative

We facilitate and work with collaborative forums to bring together the best minds in the industry and collectively solve shared challenges and address emerging threats.

KPMG's I-4 Forum brings together over 50 of the world's leading organizations.

Trusted

Professionals in KPMG member firms have a long list of certifications, permits to work on engagements and a proven track record of experience working with the world's leading organizations.

Global and local resources

The KPMG network of independent member firms is a global network with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally, giving member firms the ability to strive to deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO 27001 certification.

KPMG's Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us

Jeff Thomas
Partner
T: 403 691-8012
E: jwthomas@kpmg.ca

Ivan Alcoforado
Senior Manager
T: 403 691-7923
E: ialcoforado@kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

kpmg.ca/cyber