IIoT Cyber Maturity Assessment

Helping you set your standard in the industrial internet of things (IIoT)

KPMG Switzerland

kpmg.ch

The convergence of Operational Technology (OT) and Information Technology (IT) grows closer so it is vital that the correct governance is in place to enable an organization to feel free to seize the opportunities this brings. KPMG's approach to Cyber Security takes a sustained, modular approach to give you confidence to automate and optimize your technology without compromising the integrity or availability of your infrastructure.

Historically Industrial Control Systems (ICS) were standalone and not connected to corporate networks or the internet. However business requirements are changing — in particular the need for real time data analysis to drive efficient operations and maximize return on investment. Today, more and more Process Control Networks (PCN) are being connected to corporate networks and the Internet. As the IIoT and Industrial Internet mature connectivity, especially wireless connectivity, will increase the amount and complexity of information flowing through process networks.

ICS require specific security solutions

Industrial Control Systems are installed in a constantly evolving cybersecurity environment, where a secure system can become a vulnerable legacy system overnight without cyber due diligence particularly with respect to lifecycle and sustainability considerations. A secure ICS design, while helpful, alone does not guarantee adequate protection against cyber attacks.

To help address these issues KPMG's IIoT Cyber Maturity Assessment (CMA) can assess the level of cyber maturity either on a site by site basis or at an enterprise level.

IIoT CMA brings the ability to identify industry good practices within an organization and provide information against peer groups and competitors and lays a framework for analyzing the cybersecurity posture of the organization's enterprise and industrial control systems, and suggests methods to evaluate options for improvement based on international standards such as ISA99/IEC 62443, NERC CIP alongside our global insight of best practice in ICS Security.

KPMG's CMA is unique in the market in that it looks beyond pure technical preparedness and takes a rounded view of people, processes and technology to enable clients to understand areas of vulnerability and to implement targeted remediation.

KPMG's IIoT CMA also allows organizations to demonstrate both corporate and operational compliance turning information risk to business advantage.

What's on your mind?

— **Are we looking to understand** our cyber security posture and prioritize areas for remediation to make quick wins and protect the "crown jewels"?

— **Are we looking for an approach** that combines international information security standards with global insight of peers best practices.

KPMG's approach to ICS cyber security

Our modular approach identifies the logical, sequential steps that should be implemented to produce increasing levels of ICS cyber security capability.

How we can help you turn risk in to advantage

The first step in protecting your ICS is by understanding your current cybersecurity capability and posture, our experienced advisors work closely with IT and OT departments, enabling them to identify and protect the "Crown Jewels" and quickly identify any tactical wins.

In developing the service, KPMG has combined international information security standards with our global insight of leading practices in risk management, ICS cyber security, governance and people processes.

Potential benefits to you

In a relatively short period of time, KPMG's IIoT CMA provides the essential foundation to:

— Assess your organization's ability to protect and manage its sensitive information assets.

— Protect your industrial control systems against likely cyber attacks.

— Identify, manage and minimize the impact should an attack occur.

In short, it provides executives with a rapid assessment of your organization's readiness to prevent, detect, contain and respond to cyber threats to Industrial Control Systems.

How we have helped others

Global oil company

Increasing demands for SCADA/DCS security highlighted the need for a large oil company in the middle east to assess their SCADA/DCS infrastructure used to control the oil drilling sites and gas plants. The client required an overall impression of the IT security within the production sites.

KPMG provided a IIoT team of both local and global Subject Matter Experts (SMEs) and conduced a Cyber Maturity Assessment of the IT environment of the Industrial Control System area to obtain a high level view on the current cyber security capabilities level and to identify gaps towards the target level.

In a subsequent step after the CMA, KPMG developed a SCADA/DCS risk control framework that was used as a reference to obtain a detailed indication of the current state of security of the various sites, allowing for an initial assessment on the readiness for an ISO27001 certification.

Global machine manufacturer

A security breach was discovered at a machine manufacturer for the automotive industry, allowing access to Industrial Control System (ICS) data. A forensic investigation was initiated and an ICS security review was requested to document the current status of the ICS security.

The manufacturer has a complex global network, with several interconnected subsidiaries and specific proprietary applications at the production facilities.

The client commissioned a security review from KPMG, supported by the clients internal audit department and local controllers. All relevant stakeholders for ICS security were identified and workshops and interviews were conducted people, process, technology and governance topics. KPMG's recommendations were based on the maturity of the company in the industry to benchmark against competitors as well as security best practice.

In a subsequent mandate KPMG conducted detailed security testing of the ICS network, systems and applications and supported in developing an ICS security strategy based on the findings and recommendations.

KPMG Cyber Security professionals believe cyber security should be about what you can do — not what you can't

KPMG is not a typical cyber security advisory organization. Instead, KPMG member firms combine deep OT and IT domain expertise with cross-functional business expertise — including financial management, risk management, organizational design and more. That means KPMG member firm professionals can advise you not only on the security of your industrial systems, but also on how to tie that security to business objectives and get the enterprise support you need.

Helping vendors build security into control systems

We recognize the challenge of trying to secure legacy control systems that weren't designed for security in a connected environment. That's why KPMG member firms are working with key vendors to build cyber security into their systems, from process controllers to robotics, so you can ensure a more resilient architecture.

Expertise in your industry

In addition to understanding your operational technology, KPMG understands the threats, trends and strategies in your specific industry. How are oil and gas companies segregating their corporate and SCADA environments? What DCS risk controls are common in high-tech manufacturing? How are power plants securing their electronic security perimeter? Drawing from industry expertise and strong market presence, KPMG member firms can benchmark your cyber security with that of other clients in the same industry.

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Matthias Bossardt
Partner, Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Roman Haltinner
Director, Cyber Security

+41 58 249 42 56
rhaltinner@kpmg.com

Michael Nordhoff
Manager, Cyber Security

+41 58 249 40 89
mnordhoff@kpmg.com