WHITE PAPER

Public and Private Sectors Join Forces to Protect Industrial Networks From Cyberattacks

Alvis Chen
Global Marketing

MOXA®

Abstract

Hundreds of thousands of people left without electricity. Global supply chains screeching to a halt. These are just some of the devastating effects of cyberattacks on critical infrastructure and manufacturing in recent years. In fact, the past 10 years have seen more cybersecurity incidents involving industrial control systems than ever before. Some of these incidents were targeted attacks, such as Stuxnet, which crippled the Iranian nuclear program, whereas others were non-targeted incidents where malware spread to industrial control systems by infecting a computer on a network.

In the Industrial Internet of Things (IIoT) era, previously unconnected systems are now connected over private or public networks in order to gain more insights and improve productivity. However, with greater connectivity comes greater exposure to cyberthreats. So how do we keep the world's critical infrastructure and manufacturing environments safe from cyberattacks?

This white paper discusses how industrial control systems are no longer immune to the growing threat of cyberattacks and how both the public and private sectors are joining forces to address one of the greatest challenges to the future of industrial automation in our increasingly interconnected world.

Industrial Control Systems Are Under Attack

In recent years, industrial automation professionals have been calling for greater attention to cybersecurity in operational technology (OT) and industrial control systems (ICS). These industry experts are not crying wolf. With the inevitable trend towards digital transformation and OT-IT convergence already in full swing, industrial networks are no longer immune—if they ever were in the first place—from the growing threat of cyberattacks.

Gone are the days of critical infrastructure and industrial networks operating in isolated 'islands of automation'. Today, nearly every critical network or manufacturing environment is connected to the Internet and exposed to cybersecurity risks in some way. In fact, cyberattacks targeting critical infrastructure and manufacturing environments around the world are becoming more frequent.

Consider the following high-profile cyberattacks that have occurred within the past few years alone.

Released on May 11, 2020

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 65 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA

In October 2019, the Nuclear Power Corporation of India Limited (NPCIL) confirmed that one of its nuclear power plant networks was infected by malware because an employee used a company network computer to connect to the Internet for administrative purposes. Although NPCIL confirmed that the infected network was isolated from critical operations and no damage resulted from the malware infection, any cyberattack on a nuclear power plant or other similarly critical infrastructure around the world is deeply worrisome because so many human lives can be at stake.

Not all victims of cyberattacks fared as well as NPCIL. In March 2019, one of the world's largest aluminum producers, Hydro Norsk, became the target of a professional ransomware attack that took down its entire global network. The company employs more than 35,000 people in 40 countries and has a highly interconnected global network for enterprise IT systems and industrial operations. This attack forced Hydro Norsk to disconnect its automation systems and switch to manual operations, costing the company around US$35 million in just one week.

Unfortunately, Hydro Norsk's story is not the only recent cyberattack that resulted in massive business losses for a global company. In August 2018, the world's largest maker of semiconductors, Taiwan Semiconductor Manufacturing Company (TSMC), was also forced to shut down several chip-fabrication production lines in response to a ransomware attack. The incident cost TSMC roughly US$86 million in lost revenue.

The following table lists some of the major OT/ICS cyberattacks over the past 10 years[1].

Year	Major ICS Security Incidents	Attack Targets / Industry / Region
2010	Stuxnet	**PLC** (Nuclear Power Plant in Iran)
2011	Duqu	**Computer/Server** (Public Utility in Multiple Countries)
2012	Disttrack/Shamoon	**Computer/Server** (Oil Company in Saudi Arabia)
2014	Sandworm	**SCADA/HMI** (Factory Floor in Multiple Countries)
2015	BlackEnergy/Killdisk	**HMI/Serial Device** (Power Grid in Ukraine)
2016	Industroyer	**Circuit Breaker** (Power Substation in Ukraine)
2017	Dragonfly	**Computer/Server** (Public Utility in US/EU)
2018	WannaCry	**Computer/Server** (Factory Machines in Asia)
2019	LockerGoga	**Computer/Server** (Aluminum Producer in Norway)
2019	DTrack	**Computer/Server** (Nuclear Power plant in India)

[1] For more information, download the Moxa white paper: Industrial Network Cybersecurity: Debunking the Myths and Adopting Best Practices

If we look more closely at the targets of these recent attacks, two types of industries emerge: Critical manufacturing and critical infrastructure.

Critical manufacturing includes large companies such as TSMC and Hydro Norsk. Because of globalization, the daily operations of these companies play an important role in the worldwide supply chain. The consequences of cyberattacks on critical manufacturing go far beyond the corporate profits of the targeted company. In an increasingly interconnected world, the global supply chain itself can also be disrupted with a click of a mouse or the tap of a key.

Critical infrastructure includes the utilities for an entire country's energy, water, and transportation operations. This infrastructure is normally owned by the government or operated by a private company under government regulation. If this infrastructure is forced to shut down due to a cyberattack, there could be widespread and devastating effects on human life and the environment. For example, a cyberattack on a Ukrainian power substation in 2016 left more than 200,000 people in the dark for up to six hours in the middle of winter. Although there were no reported casualties, we cannot assume that we will be this lucky in the future. After all, it is clear that hackers are now able and willing to take town a power grid. Imagine the consequences on hospitals and emergency services if the attack lasted longer than a few hours.

With so much at stake, it is no wonder that national governments and industry organizations around the world are beginning to heed the call to address cybersecurity vulnerabilities in both industrial networks and critical infrastructure.

Tackling the Problem on All Fronts

Now that we understand that OT/ICS networks are no longer immune to cyberthreats, the next question is: how do we protect OT/ICS systems from the growing threat of cyberattacks? Unfortunately, there is no simple answer or one-size-fits-all solution for everyone. Instead, the solution requires long-term commitment to cybersecurity from all stakeholders in both the public and private sectors.

Public Sector Push

Despite their reputation for bureaucratic inefficiency, governments around the world have actually been one of the major driving factors behind the development of new working models and best practices for improving cybersecurity in industrial control systems. This phenomenon makes sense considering how governments are the primary operators of a nation's critical infrastructure. In the past two years, many national and regional governments have even created new departments and designed new regulations to enhance cybersecurity for critical infrastructure and public utilities.

For example, consider the following timeline of recent government regulations from various regions around the world:

- In 2018, the United States government formed the Cybersecurity and Infrastructure Security Agency to coordinate efforts for protecting the nation's critical infrastructure and essential resources[2].

- In 2018, the state legislature of California passed new regulations to govern information privacy for connected devices. The law, SB-327, stipulates that IoT device manufacturers must provide proper security features to protect user privacy and the user's data stored and collected on their devices[3].

- In 2018, the European Commission passed the Cybersecurity Act to strengthen the ability of the EU Agency for Network and Information Security (ENISA), which was formed in 2017, to help EU Members tackle cybersecurity threats and attacks[4].

- In 2019, China released a new series of national cybersecurity standards called the Multi-level Protection of Information Security 2.0 (MLPS 2.0). MLPS 2.0 extends the regulatory scope of the State Administration for Market Regulation from traditional information systems to critical information systems, industrial control systems, and the Internet of Things.

Private Sector Drivers

Besides the top-down regulations initiated by governments, OT/ICS cybersecurity is also being driven by private sector OT end-users and leading solution providers. These industry players may compete with each other in traditional automation businesses. However, to tackle the growing threat of OT/ICS cybersecurity incidents, they have formed various associations and alliances to facilitate more open discussion, share expertise, and develop more useful security best practices.

Several key examples of private sector collaboration to address OT/ICS cybersecurity include the following:

- In 2019, the International Society of Automation (ISA) initiated the Global Cybersecurity Alliance (GCA). Beginning with six founding members in July 2019, the GCA now brings together around 27 members—including end-users, automation system control providers, IT infrastructure providers, service providers, and system integrators—to discuss how to address cyberthreats amid the ongoing trend towards IT/OT convergence[5].

- Also in 2019, the Operational Technology Cyber Security Alliance (OTCSA) was formed by leading industry organizations to provide comprehensive cybersecurity guidelines for operational technology. These member organizations include OT operators, such as ABB and Wärtsilä, along with IT/OT solution providers, such as Check Point, Microsoft, and Qualys[6].

[2] https://www.us-cert.gov/about-us
[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[4] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity
[5] https://isaautomation.isa.org/cybersecurity-alliance/
[6] https://otcsalliance.org/

More specifically, private sector solution providers seem to be coalescing around the ISA/IEC 62443 standards on security capabilities for control system components. These standards essentially provide a flexible framework to address and mitigate current and future cybersecurity vulnerabilities in industrial automation control systems. By developing and adopting a ‘common language’ for ICS vendors and other stakeholders, the IEC 62443 standards help simplify the process of procuring and integrating the various components of industrial control systems.

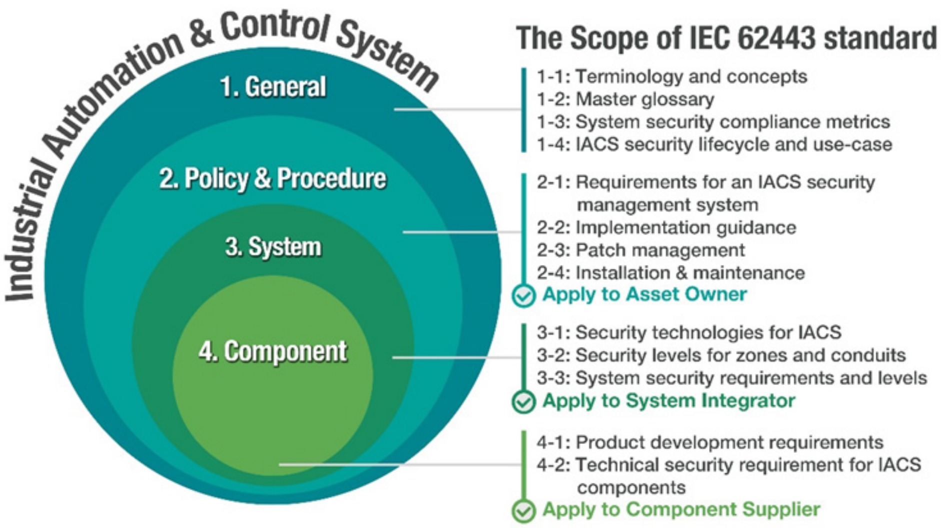
Industrial Automation & Control System
1. General
2. Policy & Procedure
3. System
4. Component
The Scope of IEC 62443 standard
1-1: Terminology and concepts
1-2: Master glossary
1-3: System security compliance metrics
1-4: IACS security lifecycle and use-case
2-1: Requirements for an IACS security management system
2-2: Implementation guidance
2-3: Patch management
2-4: Installation & maintenance
Apply to Asset Owner
3-1: Security technologies for IACS
3-2: Security levels for zones and conduits
3-3: System security requirements and levels
Apply to System Integrator
4-1: Product development requirements
4-2: Technical security requirement for IACS components
Apply to Component Supplier

Figure: The ISA/IEC 62443 standards define procedures for implementing electronically secure IACS. This guidance applies to various stakeholders in the ecosystem.

Additionally, the Industrial Internet Consortium (IIC) also publishes the **Industrial Internet Security Framework** (IISF), which brings together the collective wisdom of over 25 companies and academic institutions around the world. The IISF Technical Report includes in-depth guidelines across various industries[7]. All of these non-governmental initiatives not only validate the concerns over the growing threat of cyberattacks on industrial networks, but also reveal how we need to continue working together to keep our interconnected world safe.

Cybersecurity Is the Future of OT/ICS

With the era of digital transformation fully upon us, the world of industrial automation needs to carefully reexamine its DNA. Very few ‘islands of automation’ remain today as nearly all industrial control systems now have some degree of exposure to the Internet or unsecured networks. As illustrated by the growing number of cybersecurity incidents involving critical infrastructure and manufacturing in recent years, a concerted effort from all fronts is needed to ensure our safety now and in the future. After all, if we fail to address cybersecurity concerns for OT/ICS networks and maintain trust in our interconnected world, no amount of AI or big data can help us achieve the full promise of digital transformation.

Ingraining cybersecurity into the DNA of OT/ICS entails more than adopting a new software application or machine on your industrial network. Cybersecurity needs to be embedded throughout every aspect of an organization, from operational requirements and procedures, to

[7] https://www.iiconsortium.org/IISF.htm

the design of automation systems and network infrastructure, to the specifications of every single connected device. Fortunately, governments and private sector solution providers around the world have recognized the urgency of this issue and are using their collective wisdom to produce new industry regulations, guidelines, and requirements, and working together to push the cybersecurity agenda throughout the entire OT/ICS industry. Cyberthreats do not discriminate and any one of us could fall victim. Ultimately, the world needs more collaboration on this issue, not less.

To learn more about how Moxa can help shore up your industrial network defenses, visit www.moxa.com/Security.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.