ISA™

Setting the Standard for Automation™

WHITE PAPER

What Executives Need to Know About Industrial Control Systems Cybersecurity

Joseph Weiss, PE, CISM, CRISC
Managing Director ISA99
Applied Control Solutions, LLC

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

As more and more significant security breaches are discovered, the protection of information and control systems is becoming an important executive management and insurance issue. A company's Board of Directors and executive management must continuously and meticulously identify, categorize, and mitigate risks to the organization's success resulting from cyber attacks. In many cases the largest risk to the well-being of your company, your people, your processes, and your profits may be the compromise of your Industrial Control System—not a data breach.

Ask yourself the following questions about your company's exposure to Industrial Control Systems Cybersecurity vulnerabilities:

- What opportunities exist for breach?
- What risk exposure does my company have and what are the consequences of that exposure?
- What is the maximum damage that might be done if one of these breaches occur?
- What specific security deployments protect each of our assets?
- If our systems have cybersecurity vulnerabilities, how do those vulnerabilities impact our safety-related goals and initiatives?
- Who in our organization is responsible for these security measures? Are our IT and Operations teams coordinated and working together to secure our systems?
- Have we allocated the right resources, implemented the right standards, and sourced the right equipment to give us the best possible outcome?

This white paper addresses these and other questions in the context of the following objectives:

- Introduce the unique characteristics and vulnerabilities of Industrial Control Systems;
- Explore the key differences between an IT and an operations perspective on cybersecurity;
- Detail potential impacts of attack on critical infrastructure and manufacturing processes;
- Identify standards, training, and compliance programs to aid companies in their approach to these challenges;
- And offer some additional information on incidents that have already taken place.

In order to create and maintain secure systems, we have to first ensure that our processes and the communication between them is secure; Industrial Control Systems need to be targeted for more detailed review on a consistent basis. Second, we need to make sure that our operations staff have expertise in Industrial Control Systems Cybersecurity and are closely coordinating with our IT staff to protect our systems and processes. Third, we need to make sure our equipment is inherently secure and addresses known vulnerabilities by leveraging industry standards and conformance programs.

Introduction

Industrial control system (ICS) is a general term that encompasses several types of control systems used in industrial production. Several of these terms are often used interchangeably, or generalized as SCADA:

- Distributed Control Systems (DCS) that monitor and control large centralized facilities such as power plants and refineries
- Supervisory Control and Data Acquisition (SCADA) systems that monitor and control dispersed assets such as electric grids, pipelines, and water systems
- Programmable Logic Controllers (PLCs) that control individual processes
- Remote Terminal Units (RTUs) that act as data concentrators
- Field devices—such as sensors that measure the process (pressure, temperature, flow, etc.); analyzers that monitor chemical constituents; drives that open and close valves; etc.

Essentially, an Industrial Control System is a system made up of other systems, designed to monitor and control physical processes and ensure safe operations within specific known engineered states. It carefully manages transitions to control risk between operational states. These controlled states and transitions are defined to protect against random occurring failures of a component or a few components. However, focused logical attacks to push a system into known dangerous states are not commonly expected or compensated for in the normal operational parameters of Industrial Control Systems.

> *"Focused logical attacks to push a system into known dangerous states are not commonly expected or compensated for in the normal operational parameters of Industrial Control Systems."*

Differentiating between IT Cybersecurity and ICS Cybersecurity

Malicious cyber-related incidents are occurring, or being identified, on what seems like a weekly basis. Almost all of these are data breaches, compromising the confidentiality of supposedly private information. However, the consequences are not confined to data breaches and compromises of personal data.

Industrial Control Systems that are used in the critical infrastructures of electric power, nuclear plants, chemical plants, oil/gas, manufacturing, pipelines, transportation, and building controls also use computer controls. Often referred to as the "SCADA" systems, many are attached to very critical processes that modern society depends on and cannot continue to function without. They typically don't look or act like those used in the conventional business IT environment and are not being monitored for cyber threats like those in the business IT environment.

It's important to recognize and understand the differences between IT cybersecurity and ICS cybersecurity, and the table below highlights some of the most significant factors to consider.

Attribute	IT	ICS
Confidentiality (Privacy)	High	Low
Message Integrity	Low-Medium	Very High
System Availability	Low-Medium	Very High
Authentication	Medium-High	High
Non-Repudiation (Proof of the integrity and origin of data)	High	Low-Medium
Time Criticality	Days Tolerated	Critical
System Downtime	Tolerated	Not Acceptable
Security Skills/ Awareness	Usually Good	Usually Poor
System Life Cycle	3–5 Years	15–25 Years
Interoperability	Not Critical	Critical
Computing Resources	"Unlimited"	Very Limited with Older Processors
Software Changes	Frequent	Rare
Worst Case Impacts	Frequent Loss of Data	Equipment Destruction, Inquiries

Focusing on the Challenge

Cyber incidents have been defined by the US National Institute of Standards and Technology (NIST) as occurrences that jeopardize the confidentiality, integrity, or availability (CIA) of an information system. The NIST definition is a conservative approach to judging cybersecurity effectiveness. According to NIST, an incident doesn't need to be malicious to be significant and to carry risk to the process and the people involved in the process.

However, because IT is so prevalent in the cybersecurity field, cybersecurity is effectively being viewed as a malicious attack via the Internet against a Windows-based system with the intent of stealing information. Unfortunately, this paradigm does not apply to ICSs and does not address the most important aspect of ICSs—safety. Generally, IT approaches cybersecurity as an end to itself—IT works to identify cyber vulnerabilities without evaluating the consequences.

"If malicious code can affect a Programmable Logic Controller the way that it did in the Stuxnet incident, that same process can be used to attack a PLC that operates a pipeline, a power plant, a water/wastewater treatment facility, a building's security system, and more."

It is the consequences that are of the most interest when considering the security of critical control systems. Many of these are installed in facilities with an expected life expectancy of 10–25 years. The nature of their design and the close connection to the underlying process means that they often cannot be upgraded to the latest cyber technologies easily, or even patched on an expedited basis.

Many professionals working in industry report a lack of senior management attention and consequent funding to address control system cybersecurity.

Why aren't we paying closer attention and working to solve this imminent challenge facing our infrastructure? One of the biggest reasons given for this lack of attention on arguably the most critical system in a modern economy is that there have been few reported control system cyber incidents affecting these systems.

One exception to this was the Stuxnet in Iran. Unfortunately, a common response to this incident has been "Stuxnet doesn't affect us—we don't have uranium centrifuges." Nothing could be further from the truth—if malicious code can affect a Programmable Logic Controller the way that it did in the Stuxnet incident, that same process can be used to attack a PLC that operates a pipeline, a power plant, a water or wastewater treatment facility, a building's security system, and more.

The most important aspects of Industrial Control Systems are reliability and safety. Consequently, ICS personnel have different concerns; they are focused on cyber threats (malicious or unintentional) only if they affect reliability or safety. This means that the issues involved with ICS cybersecurity are not denial of service issues, but rather:

- Loss of process visibility—if I'm driving a car, are all of my displays working, and can I trust the information they're conveying?
- Loss of control—as I'm driving, do I have control of the gas pedal, the brake pedal, and the steering wheel?

Both of these issues were key factors in Stuxnet—the centrifuges were spinning out of control, and the displays told the operator there were no problems.

ICS Vulnerabilities: An Attacker's Dream and Our Worst Nightmare

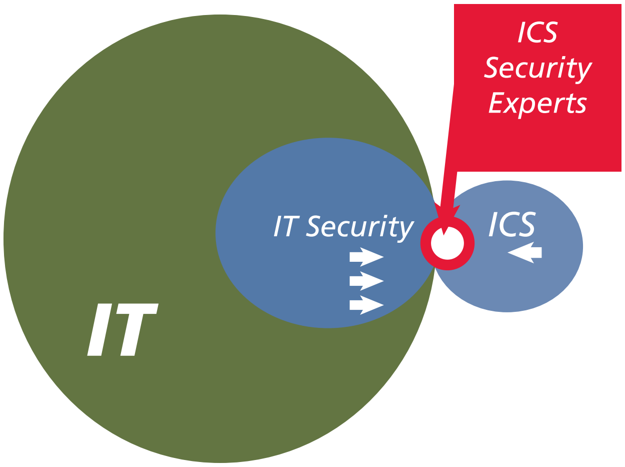
Some attackers view exploits where you can damage physical processes as the holy grail of cyber attacks—imagine the devastation, and the resulting terror, that would be caused by the damage or compromise of the power grid, or the water supply. Devices that can cause catastrophic damage through remote operation of cyber components are an ideal target for compromise.

> *"The more components that can be compromised in an ICS, the greater the risk to the operator and value to the attacker. Industrial Control Systems are not designed to ensure resilience against concerted attacks that intend to place components in dangerous operating states."*

Consequently, we should make these devices a "target" of more detailed review to a) protect them from malicious attack, and b) ensure that non-malicious actions by an insider (facility staff or contractors) do not cause unintentional cyber incidents.

The more components that can be compromised in an ICS, the greater the risk to the operator and value to the attacker. Industrial Control Systems are not designed to ensure resilience against concerted attacks that intend to place components in dangerous operating states. This is expected to be a growing area of cyber-attack and engineering research.

An Industrial Control Systems Cybersecurity Expert looks at a facility and its systems in a holistic way, identifying physical vulnerabilities of the controllers and the process and discovering ways to exploit vulnerabilities by cyber manipulations. There are very few people with the expertise to understand the physical process being controlled; the control system domain with its unique design features; and the exploitation of IT vulnerabilities. ICS Cybersecurity Experts bridge the gaps between these traditional areas of expertise.



ICS Cybersecurity Experts bridge the gap between IT Security expertise and Industrial Control Systems expertise—a rare combination of skills in high demand today.

Developing the Industrial Control Systems Cybersecurity Expert: Why it Matters

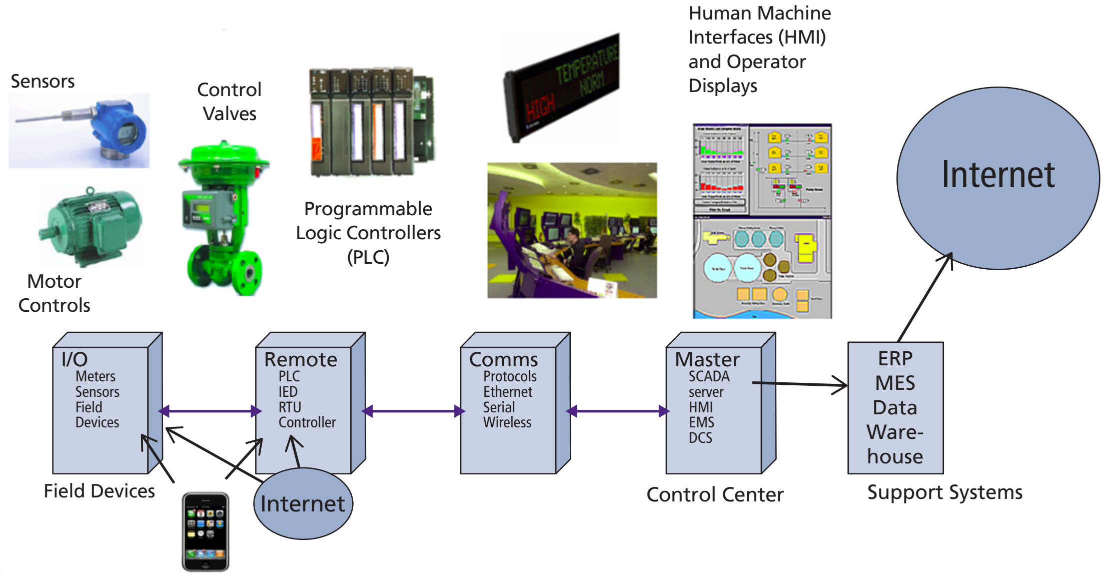
IT personnel generally have Computer Science backgrounds with minimal engineering backgrounds, whereas Operations personnel come from engineering backgrounds with minimal security training. There is a gulf between the IT and Operations organizations—and it is the responsibility of senior executives and boards to break down these organizational divides.

An Industrial Control System includes a Human-Machine Interface (HMI), a software application that presents information to an operator or user about the state of a process, and allows the system to accept and implement the operator's control instructions. HMIs are generally designed to operate on common commercial operation systems (e.g., Windows) that are understood by IT. However, the proper support of these devices also requires Operations expertise.

Traditional cyber attacks often focus on the general purpose information systems—using zero-day vulnerabilities, buffer overflows, cross-site scripting, or other vulnerabilities. These attacks generally pursue the capture of valuable data or aim to create denial-of-service incidents. Attacks targeting Industrial Control Systems can be built on top of these—but take aim at the physical process, exploiting legitimate product or system design features.

> *"There is a gulf between the IT and Operations organizations—and it is the responsibility of senior executives and boards to break down these organizational divides.*

The typical IT security function is focused on Advanced Persistent Threats (APT) and traditional insider threats, while threats such as Stuxnet and Aurora are Persistent Design Vulnerabilities (PDV) that exploit features inherent in the systems' design. We use the term "infinite day vulnerabilities" instead of "zero day vulnerabilities" when referring to ICS systems, because the vulnerabilities are a combination of new and inherent vulnerabilities of the systems.



A basic diagram showing various components of Industrial Control Systems used in many different applications across different industries

Applied Control Solutions proprietary information

IT security experts understand Windows and Internet Protocol (IP) communications and have numerous types of technologies to look for cyber threats at the Windows and IP layers, but very little understanding and very few tools "below the IP layer." Control systems personnel are typically focused on operational reliability and safety—not cybersecurity. Consequently, there are few computer forensics, and minimal training to identify ICS cyber incidents. Organizations such as Computer Emergency Response Teams (CERT) have databases of hundreds of thousands of cyber probes and attacks, but very few, if any, recorded ICS incidents. This is partially due to the lack of training and education about Industrial Control Systems; and conversely, the lack of training of Operations personnel regarding security considerations. Moreover, there are few, if any, regulations to ensure ICS cyber incidents are forensically examined to identify possible pathways to failure. The lack of appropriate forensics can call official findings on verification and attribution into question; these factors are important details for insurance and compliance purposes, and critical information as cyber technologies evolve into cyber weapons.

> *"Stuxnet was successful, in large part, because it was arguably the only instance where IT, Operations, and Physical Security teams tightly coordinated to plan and implement the attack. It is an unfortunate fact that this coordination does not happen (with very rare exceptions) when trying to protect Industrial Control Systems."*

In the IT environment, technology is available to monitor and identify cyber attacks, although there have been many cases where IT cyber compromised systems have gone unseen for months. With critical infrastructure, it is very different. When an event occurs in critical infrastructure such as an electric blackout or a pipe break, the results are immediate and the impact can't be hidden. Without the perspective of an Industrial Control Systems cybersecurity expert, it can be difficult to determine if a cyber breach is the cause of a failure incident.

Industrial Control Systems Cybersecurity Experts meet the following criteria:

- They understand the physical process being controlled
- They understand the control system domain with its unique design features
- They understand the risks and mitigations of exploitable IT vulnerabilities
- They are well versed in industry standards, and understand how they apply to people, processes, and products
- They can bridge the gap between the IT organization and the Operations organization

The culture gap that exists between the IT organization and the Operations organizations exacerbate the physical threats and make it very difficult to secure Industrial Control Systems. Stuxnet was successful, in large part, because it was arguably the only instance where IT, Operations, and Physical Security teams tightly coordinated to plan and implement the attack. It is an unfortunate fact that this coordination does not happen (with very rare exceptions) when trying to protect Industrial Control Systems.

Industry Standards and Compliance Programs: A Solid Foundation to Build a Secure Future

ICS cybersecurity is a global issue—and the challenge spans across processes, people, and equipment. In order to create and maintain secure systems, we have to ensure that our processes and the communication between them is secure; we have to make sure our people are trained and we have expertise in Industrial Control Systems Cybersecurity; and we have to make sure our equipment is inherently secure and addresses known vulnerabilities. That's a tall order, and when you multiply those challenges with the number of industries and world regions impacted, it can be overwhelming to consider how we will coordinate our response.

For hundreds of years, industries have relied on global standards to help solve difficult technical problems and ensure harmonization and consistency in process and product design. Standards Developing Organizations (SDOs) have led the charge in the consensus development of industry standards in areas like alarm management, safety, batch processing, wireless communication, and others. The International Society of Automation (ISA) is the SDO for automation and control professionals in many different industries, including oil and gas, petrochemicals, utilities, food and beverage, pharmaceutical, and many more.

ISA is the developer and applications-focused thought leader behind the world's only consensus-based industrial cybersecurity standard. The ISA99 standards development committee brings together worldwide Industrial Control Systems Cybersecurity Experts from industry, governments, and academia to develop the ISA/IEC 62443 series of standards on industrial automation and control systems security, guided by the accredited processes of the American National Standards Institute. The committee addresses industrial automation and control systems whose compromise could result in endangerment of the public or a company's employees, violation of regulatory requirements, loss of proprietary or confidential information, economic loss, or adverse impacts on national security.

The ISA/IEC 62443 standards define requirements and procedures for implementing electronically secure automation and Industrial Control Systems and security practices, and assessing electronic security performance. The ISA/IEC 62443 standards approach the cybersecurity challenge in a holistic way, bridging the gap between operations and information technology; and between process safety and cybersecurity. Given the interconnectivity of today's advanced computer and control networks—where vulnerabilities exploited in one sector can impact and damage multiple sectors—it's essential that cybersecurity standards be broadly applicable across industries or sectors. The ISA/IEC 62443 Industrial Automation and Control Systems Security series of standards is a multi-industry initiative applicable to all key industry sectors and critical infrastructure.

In order to help industry solve the "people" part of the challenge, ISA has also developed a series of courses and certificate programs based on the standards, culminating in the Industrial Control Systems Cybersecurity Expert designation for professionals who can successfully complete the courses and exams.

The final piece of the industrial cybersecurity puzzle involves the actual equipment that makes up the Industrial Control System—after all, a secure control system requires that each system, communication protocol, and communication media be secure. Unfortunately, many ICS devices, including new devices, are still insecure by design and many legacy Industrial Control Systems cannot implement IT security technologies yet won't be replaced because they still work.

In response, the Automation Standards Compliance Institute created the ISASecure® ISA/IEC 62443 conformity assessment program for commercial-off-the-shelf (COTS) Industrial Control System products. The certification program evaluates the product development practices of the supplier, along with detailed product security characteristics, with the ultimate objective of securing the Industrial Control Systems supply chain. The ISASecure® certification program is an ISO/IEC 17065 conformity assessment scheme that ensures that control systems conform to relevant ISA/IEC 62443 cybersecurity standards and it is applied using the security lifecycle concept that forms the basis of the standards. Asset owners and integrators who include the ISASecure® designation as a procurement requirement for control systems projects have confidence that the selected products are robust against network attacks and free from known vulnerabilities.

Viewpoint: An Industrial Control Systems Cybersecurity Expert Explores ICS Cybersecurity Incidents

There have been nearly 750 actual Industrial Control Systems cyber incidents, with impacts ranging from trivial to significant equipment damage; significant environmental damage; non-compliance with regulatory requirements; and deaths of people involved in the affected processes. Remember, an ICS cyber incident does not need to be malicious to create a risk to the organization with potentially catastrophic consequences.

The information from the incidents is not classified, but neither is it public. I have been studying these incidents for years, and I've created a database covering control system cyber incidents in Asia, Europe, North America, South America, and the Middle East. Following 9/11, there was supposed to be a focus on "connecting the dots," but that certainly has not happened with ICS cybersecurity. ICS incidents keep occurring, many with common threads, across multiple industries with little guidance or training.

The incident case histories that I've compiled provide an understanding of:

- What can actually happen during an incident
- The difficulty in recognizing an incident as cyber-related
- The need for appropriate policies and/or technologies to effectively mitigate the incidents
- The lack of existing regulations and appropriate guidance to prevent or mitigate the incidents
- The lack of design resiliency for systems that cannot be protected from cyber threats
- How companies have recovered and can recover from breaches

The data could also help to provide an understanding of a breadth of human factors, nation state actions, and processes being used in hostile acts against critical infrastructure such as:

- Reconnaissance and testing
- Experimental use of destructive tools to test generic attacks
- Failures from design faults of control systems at different stages of the life cycle of industrial equipment
- Combined factors, based on analysis of how different factors interact and lead to incidents initiated by failures in control systems

My goal in the analysis of the data is to identify previously unrecognizable single factor risks, unusual and previously unpredicted failures, or the as-yet-unsimulated combinations of factors causing unusual perturbations. The database identifies:

- More than 50 cases that resulted in more than 1,000 deaths combined
- More than 10 major cyber-related electric outages
- More than 60 nuclear plant cyber incidents with more than 15 resulting in reactor shutdowns
- More than 50 cases involving significant environmental releases
- More than 100 cases involving physical equipment damage (not servers or other IT equipment)
- Impacts conservatively totaling more than $30 Billion (this comes from economic estimates from major cyber-related events such electric outages, pipeline failures, dam failures, plane crashes, and train crashes) and bankruptcy of several companies as a result of these failures

Three incidents in particular come to mind when considering the potential risk to the financial well-being of organizations whose systems are compromised:

- The 2010 non-malicious natural gas pipeline rupture of a major Investor Owned Utility resulting in more than a $1.5 Billion fine and possible criminal violations
- The 2014 sophisticated malicious "spear-phishing" cyberattack at a German steel mill that caused physical damage to the furnace, and thirdly
- The on-going Volkswagen emissions scandal demonstrating that ICS cyber-issues can come from within an organization and target business considerations with billion dollar ramifications.

These incidents showcase ICS cybersecurity vulnerabilities; in some cases, incidents led to the resignation of the CEO and several billion dollars of damage; many times, incidents are caused by intentional activities but not often considered malicious in the traditional sense; and in both cases, IT has no knowledge of the relevant issues. In the case of the gas and electric company, the public utility commission is now investigating a potential splitting up of the company's assets because of the systemic safety issues stemming from the rupture. In Volkswagon's case, the company may have lost their entire diesel car market, as well as taken a serious hit to their reputation as a manufacturer of well-designed vehicles.

Recommendations and Conclusions

Industrial Control Systems cybersecurity is an issue with multiple facets, spanning technology, processes, equipment, and people—and it crosses traditional barriers of geography, industry, and application. Vulnerabilities and associated attacks, whether malicious or unintentional, can bring devastating financial, safety, and brand reputation consequences—and executive management should be carefully considering their exposure to these risks.

Culture, knowledge, and experience gaps exist between IT and Operations personnel in most companies, and the coordination of these functions with guidance from a team of Industrial Control Systems Cybersecurity Experts is critical to the success of a comprehensive cybersecurity program. Global, consensus standards focused on Industrial Control Systems cybersecurity can help to bridge the gaps between IT and Operations, and between safety and cybersecurity. These standards can be applied to processes; the associated training and certificate programs can be leveraged to train people; and the associated compliance programs can be utilized to test and certify equipment.

By using data from known incidents and vulnerabilities, and leveraging standards, training, and compliance programs, systems engineers and Industrial Control Systems Cybersecurity Experts can reduce the risks to critical infrastructure from hostile actors, human mistakes, and design flaws. We can make our systems more reliable, less sensitive to malicious or unintentional breaches, and secure the safety of our people and processes in industry and critical infrastructure.

Additional Resources

Download a brochure detailing ISA's resources for Control Systems Cybersecurity, including the ISA/IEC 62443 standards and associated training, certificate programs, books, technical papers, and more: www.isa.org/cybersecurityresources

Visit Applied Control Solutions at http://realtimeacs.com/ to learn more about Joe Weiss, the author of this white paper.

The International Society of Automation (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 36,000 members and 350,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

International Society of Automation
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE +1 919-549-8411
FAX +1 919-549-8288
EMAIL info@isa.org
www.isa.org

EP83-5472-1115