Industrial automation control systems (IACS) technologies have increasingly converged with those used by regular IT systems, including the use of Internet Protocol (IP) interconnections and Windows-based computers, with consequent growth in their technology and cybersecurity risk profile.

Incidents involving IACS are often the result of outdated security control practices, aging IT technologies, and knowledgeable internal and external attackers. Some incidents have low profiles, causing odd behaviors and small disruptions that go unexplained, and others have bigger consequences with major operational and safety impacts. The US Industrial Control Systems Computer Emergency Response Team (ICS-CERT) responded to 256 incidents in 2013 (85 percent more than in 2012). This might not seem like much when compared with the 47,000 computer incidents reported in 2013 by Verizon in its data breach report, but the consequences of a cybersecurity incident involving IACS can be disastrous. The 2012 cyberattack on Saudi Aramco, for instance, damaged 30,000 computers and was aimed at disrupting production. Luckily, it failed to affect oil and gas assets. A nonattack-related problem with a supervisory control and data acquisition (SCADA) system in the US, for instance, led to the spill of more than 1,000,000 gallons of crude oil in 2010.

Breach-disclosure regulations are usually concerned with consumer privacy and frequently do not apply to IACS because they do not normally include personally identifiable information (PII). However, in 2011, the US Securities and Exchange Commission (SEC) Corporate Finance (CF) Disclosure Guidance: Topic No. 2 broadened the understanding of disclosure obligations of public companies. Considering cyberincidents as the result of both attacks and unintentional actions, the SEC’s Division of Corporation Finance understands that companies should disclose cyberincidents “that are individually, or in the aggregate, material, including a description of the costs and other consequences.” Additionally, it requires discussion about the aspects of the “business or operations that give rise to material cybersecurity risks” and risk of incidents “that may remain undetected for an extended period.” This means that, depending on the nature of the business and its operations, cybersecurity IACS-related risk and incidents may need to be disclosed.

In a similar way, Canadian Securities Administration (CSA) Staff Notice 11-326 asks registrants to consider whether risk, incidents and controls “are matters they need to disclose in a prospectus or a continuous disclosure filing.” The CSA specifically addresses cybercrime, thus leaving out some unintentional actions, but it should consider cyberattacks involving IACS, depending on the nature of the company’s business.

Given the potential safety, environmental and operational impacts a major IACS incident may cause, management should be concerned with enhancing resiliency and response capabilities to these threats while keeping key stakeholders well informed.

**DEFINING IACS**

IACS is the term adopted by The International Society of Automation (ISA) to broadly refer to several types of components and systems in all industries. This includes, but is not limited to:

- **SCADA systems**—Used on geographically dispersed field assets where central monitoring and control are needed; frequently found in railway transportation systems and oil and natural gas pipelines
- **Distributed control systems (DCS)**—Architecture composed of subsystems responsible for controlling localized processes; often found in electrical power generation and distribution, water management, traffic management, and process-based industries such as chemicals, oil refineries, metallurgical and pharmaceutical
• Programmable logic controllers (PLC)—Computerized devices equipped with nonvolatile memory used to control equipment and processes; used extensively in several industries, including manufacturing, transportation and mining

• Safety instrumented systems (SIS)—Hardware and software controls used on hazardous processes to prevent or mitigate consequences; found in several industries and require special attention when protecting against cybersecurity risk

TYPICAL CYBERSECURITY THREATS TO IACS

Cybersecurity incidents impacting IACS may result from the following threat agents:

• Insider action—Typically employee or contractor unintentional misuse or intentional abuse resulting in disruption or circumvention of existing controls

• Industrial spies/competitive intelligence—Usually working on behalf of competitors and trying to gather information such as production capacity, technologies involved and plant architecture

• Botnet operators/spammers/phishers—People who operate schemes for hire and obtain monetary gain by executing or enabling attacks for others, usually involving, for example, denial of service (DoS) or malware distribution

• Hacktivists—Individuals motivated by political, environmental or ideological causes

• Organized crime—Groups motivated by financial gain. The threat of disruption may be used to blackmail an organization.

• Foreign governments—System attacks by foreign agents or state-sponsored groups to steal industrial secrets, disrupt production and, potentially, exploit safety hazards

• Natural—Physical events caused by nature, e.g., tornados, floods, earthquakes

These elements typically exploit IACS environments by taking advantage of control weaknesses. Figure 1 indicates potential impacts of exploiting IACS control weaknesses.

WHAT SHOULD AN IACS CYBERSECURITY PROGRAM LOOK LIKE?

All IACS programs need to take into consideration their dissimilarities from traditional IT. There are several differences, but three types are key:

1. Focus on safety and availability—In an environment where failure can result in operational disruption and loss of life, outages and variances from performance specifications are unacceptable.

2. Specialized and proprietary technologies—While IT focuses on interoperability and standardization to gain efficiencies, IACS were developed independently by multiple vendors with a focus on the challenges of individual plants or industries.

<table>
<thead>
<tr>
<th>Control Weaknesses</th>
<th>Poor physical security</th>
<th>Low security awareness</th>
<th>Weak protocol security</th>
<th>Inadequate network segregation</th>
<th>Lenient access controls</th>
<th>Component remote access/backdoors</th>
<th>Malware (including advanced persistent threats [APTs])</th>
<th>Weak audit logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Unauthorized Commands</td>
<td>Unauthorized Configuration Change</td>
<td>Information Gathering</td>
<td>Unauthorized System Access</td>
<td>Disruption/Destruction</td>
<td>Detection Evasion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Ivan Alcoforado. Reprinted with permission.
3. **Equipment lifetime**—It is not unusual to find plants with commercial lifetimes of 20, 30 or 40 years. This is particularly challenging when using IP or Windows-based components, which usually follow the typical three-to-five-year lifetime expectancy of technology.

Taking these differences into account, a robust IACS cybersecurity program should identify priorities and controls, paying special attention to critical operations and safety hazards and their associated controls. It should:

- Take a risk-based approach when assessing capabilities, identifying priorities and applicable requirements to prepare the organization. Bear in mind that, as a result of this assessment, some IACS might be identified as so critical and/or hazardous that a high-protection approach is needed, zeroing vulnerabilities and isolating components.
- Set up an IACS cybersecurity framework, leveraging broad standards such as International Electrotechnical Commission’s IEC 62443/ISA 99 and/or industry-focused standards such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), to establish objectives and then define processes, controls, technologies and teams to protect the IACS environment.
- Establish metrics and goals together with testing, monitoring, response and auditing processes to detect and respond to deficiencies and incidents.
- Integrate the organization, engaging operations personnel; automation engineers; health, safety and environment (HSE) teams; continuity management areas; and security teams through cross-functional synergies and joint processes.
- Enable the organization, raising awareness of staff on the importance of security and building the skills needed to assess, protect, detect and respond to cybersecurity incidents.
- Build a threat intelligence model and ecosystem that allow the organization to follow evolving threats and issues in the IACS world that are relevant to its operation. New threats are discovered daily and attackers need to find only one flaw to successfully execute an attack.
- Collaborate with industry organizations, component manufacturers, service providers, incident response teams and law enforcement. Industry organizations can help improve standards and learn from known incidents. Manufacturers and service providers should help organizations deal with vulnerabilities and improve the environment. Response teams and law enforcement should help organizations deal with more serious incidents. Especially when dealing with attacks perpetrated by organized crime and foreign governments, external help is needed to defend from such resourceful groups.

### UNDERSTANDING IACS SECURITY STANDARDS

One of the challenges when establishing an IACS cybersecurity framework is the lack of relevant, broad, universally accepted standards or frameworks, such as the International Organization for Standardization’s ISO 27000 series and COBIT®. Such sources can help define the components of an organization’s framework by providing a comprehensive list of activities and controls that can be tailored to a company’s particular context. As certain industry initiatives evolve, this situation should be resolved for IACS.

For example, in February 2014, the US National Institute of Standards and Technology (NIST) published the first version of its *Framework for Improving Critical Infrastructure Cybersecurity*. This framework is composed of three basic parts:

- **Core**—With a set of activities and expected outcomes that are common to critical infrastructure and IACS, this section includes useful mapping to other standards and frameworks, such as the latest version of ISO 27001 published in 2013, COBIT® 5 and ISA 62443.
- **Tiers**—Describe the degree of cybersecurity risk management practices in an organization. While not a full-fledged maturity model, the approach establishes four tiers from “partial” to “adaptive,” with the latter being the most complete level.
• **Profile**—Used to represent the current as-is state and the target to-be state to allow planning, prioritization and monitoring of progress metrics. The profile can also be used for self-assessments and communications.

Another key initiative, led by the ISA, is a set of standards, ISA/IEC 62443 (formerly ISA99, and now in collaboration with the International Electrotechnical Commission), aimed at protecting industrial automation and control systems. These standards establish good security practices for designing, building and implementing components and complete IACS and, in their operation, establish an IACS security management system.

The standards are divided into four parts and are evolving, with some documents still under development:
- **General**—Establishes the context for all standards in the series, defining concepts and terminology, as well as life cycle and compliance metrics
- **Policies and procedures**—Provides guidance for developing an IACS security management system and, in the future, certification of supplier policies and practices
- **System**—Identifies security technologies, requirements and assurance levels for IACS networks
- **Component**—Describes product development and technical security requirements for IACS equipment

As a recent and evolving standard, ISA/IEC 62443 is fairly updated with regard to current security challenges in IACS environments, and even its draft documents provide some insight into good practices and solutions. Alignment with these standards represents an important step toward compliance with industry practices and protection of critical infrastructure assets.

A number of industry-specific standards exist, such as the American Petroleum Institute (API) 1164 “Pipeline SCADA Security,” the US Transportation Security Authority (TSA) “Pipeline Security Guidelines,” and the American Gas Association Report No. 12 “Cryptographic Protection of SCADA Communications,” to address specific challenges of each vertical. One of the most complete standard sets is the NERC CIP, established in 2006. It can be viewed as covering three main aspects:
- **Management**—Establishing a risk-based approach and security policies, together with personnel security measures, from training to background checks (CIP 002 “Critical Asset Identification,” CIP 003 “Security Management Controls” and CIP 004 “Cyber Security Personnel and Training”)
- **Asset protection**—Defining logical and physical security measures to protect critical assets, including hardening, configuration management, technical assessments and monitoring (CIP 005 “Electronic Security Perimeter” and CIP 006 “Physical Security”)
- **Operations**—Identifying processes to secure critical assets and incident response and recovery procedures to handle issues (CIP 007 “System Security Management,” CIP 008 “Incident Reporting and Response Planning” and CIP 009 “Recovery Plan for Critical Cyber Assets”)

Although focused on and mandatory only for the electric sector, NERC CIP provides valuable guidance in the protection of critical assets that may be transferable to other industries.

**SETTING UP AN IACS CYBERSECURITY FRAMEWORK**

Figure 2 provides an example of an organization’s IACS cybersecurity framework, designed using standards, but tailored for the environment. For each item in the program scope there is a process, an action plan, and standard and/or control documentation. Governance and policies use existing enterprisewide structures and processes. Monitoring uses already-established areas and processes, but defines adjustments needed on each one to support the IACS cybersecurity program and perform proper reporting.

When establishing this framework, the structure of the COSO Internal Control—Integrated Framework was used as a foundation with provisions sought from other standards. Whenever a provision is not available or is considered incomplete in an IACS standard or framework, COBIT elements are used to address the gap. A summary of the standards used can be found in figure 3.

**CONCLUSION**

As more and more organizations start reporting cybersecurity risk and incidents, security professionals, internal auditors and IT auditors need to pay as much attention to IACS controls as they do to controls for traditional IT. IACS technologies are increasingly using standard IT components, and, as a consequence, the threat landscape to these environments has grown. However, IT standards and controls are not immediately applicable to IACS due to specific business and operational requirements.
Figure 2—Example of IACS Cybersecurity Framework

Governance and Policies

<table>
<thead>
<tr>
<th>Governance Practices</th>
<th>Change Management</th>
<th>Enterprise Risk Management</th>
</tr>
</thead>
</table>

IACS Cybersecurity Program

Training and Communication

- Awareness training
- Cross-area training (HSE, IT security, audit, IACS engineering)
- Skill building:
  - IACS security
  - Security testing
  - IACS audit
- Communication with industry groups

Cybersecurity Assessment

- Cybersecurity risk assessments
- Enterprise risk management linkage
- Red team technical assessments
- Standards compliance/readiness assessments

Cybersecurity Countermeasures

- Access management
- Network/Infra. security
- Change controls
- Physical security
- Backup
- Real-time monitoring
- Threat intelligence

- Encryption
- Secure development
- Third-party controls
- Personnel security
- Antimalware tools
- Component certification
- Vulnerability assessment

Incident Response Management

- Response plan and team
- Crisis management
- Investigation team
- Collaboration with:
  - Component manufacturers
  - Service providers
  - Incident response teams
  - Law enforcement

Monitoring

<table>
<thead>
<tr>
<th>Controls Assessment</th>
<th>Systems Monitoring</th>
<th>External Audit</th>
<th>Internal Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Metrics</td>
<td>Compliance/certification</td>
<td>External Reporting</td>
<td>Audit Committee</td>
</tr>
</tbody>
</table>

Figure 3—Standards Leveraged for IACS Cybersecurity Framework Example

<table>
<thead>
<tr>
<th>Governance and policies</th>
<th>NIST Framework</th>
<th>ISA/IEC 62443</th>
<th>NERC CIP</th>
<th>COBIT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and policies</td>
<td>ID.BE, ID.GV</td>
<td>2-1</td>
<td>EDM01, 03</td>
<td>AP007</td>
</tr>
<tr>
<td>Cybersecurity assessment</td>
<td>ID.AM, ID.RA, ID.RM</td>
<td>1-1, 2-1, 3-3</td>
<td>CIP-002</td>
<td>AP001, 02, 08, 12, 13</td>
</tr>
<tr>
<td>Cybersecurity countermeasures</td>
<td>PR.AC, PR.DS, PR.UP, PR.MA, PR.PT, DE.AE, DE.CM, DE.DP</td>
<td>2-1, TR 3-1, 3-3</td>
<td>CIP-003, CIP-005, CIP-006</td>
<td>BAI02, 03, 06, 07, 09, 10, DSS04, 05</td>
</tr>
<tr>
<td>Incident response management</td>
<td>RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM</td>
<td>2-1, 3-3</td>
<td>CIP-008, CIP-009</td>
<td>DSS02, 04</td>
</tr>
<tr>
<td>Training and communication</td>
<td>PR.AT, RS.CO, RC.CO</td>
<td>2-1</td>
<td>CIP-004</td>
<td>BA05, 08, DSS04</td>
</tr>
<tr>
<td>Monitoring</td>
<td>1-3 (draft 5) 2-1</td>
<td>CIP-003</td>
<td>EDM05, MEA01, 02, 03</td>
<td></td>
</tr>
</tbody>
</table>

Source: Ivan Alcoforado. Reprinted with permission.
Several IACS security standards and framework initiatives, as noted previously, have been published in recent years and can be valuable tools when establishing a company’s IACS cybersecurity framework. They constitute good references for IACS security, but might not fit directly in an organization’s control environment and need to be tailored. In a field evolving as rapidly as security, tight integration with a company’s controls and dynamic processes to keep up with threats are essential to success.

REFERENCES
National Institute of Standards and Technology, “NIST Cybersecurity Framework—ISA 99 Response to Request for Information,” The International Society of Automation (ISA), USA, 5 April 2013

ENDNOTES
6 Ibid.

_Cyber Security.pdf