Director Elect’s Welcome
Ray Vandale, SMV Consulting

Greetings to all CONDES and ISA members and I hope you had a great summer and are welcoming the fall colours. I would like to welcome Mr. Philip Reppert to our volunteer team. Phil will be coming on as our new Director Elect and will be succeeding me in 2022. His experience in the Automation Industry will be an asset to our Divisional Directorship.

I am excited to open the newsletter by saying that this is one of Willy’s great works. Last fall there were many fantastic papers delivered towards Cyber Security at the Montreal Symposium and I thought that it would be fitting to speak towards this aspect of our industry as it is becoming a more prevalent concern towards the protection of control systems within plants and industry.

For many years the direction of design towards control systems focused on new protocols that brought us more robust, faster and hybrid systems. Although Cybersecurity has always been a focal point within control systems, it is now a more predominant factor when accessing your risks towards safety, reputation, loss of business and environmental impact.

Cybersecurity is a global concern with governments, security elements and end users joining together to mitigate risk for the betterment and safety of mankind. Fortunately, there are standards and technologies coming to the forefront to mitigate the risks and ISA is great path to seek that knowledge.

I hope you enjoy the efforts that Willy has put into this newsletter and I am confident that you will find it very informative.

As always, we would love to hear your thoughts and ideas towards topics of interest for upcoming newsletter.

Enjoy your fall season and I look forward to our next newsletter this fall.

New Director Elect’s Personal Biography

About Upcoming Events

25-28 October 2019
Annual Leadership Conference
Paradise Point
San Diego, California, USA

4-6 November 2019
2019 ISA Process Industry Conference (PIC)
for you, in this issue you will find an interesting white paper, a description of ISA worldwide leadership in this area, about the ISA99 Committee and a description of work developed on 62443 standard series published, and ISA/IEC certificate programs, also we include all available ISA courses, webinars that are free for ISA’s members, take advantage of all this material.

As Summer finished and Falls is starting, we are thinking about the next issue, don’t hesitate to get involved, tell us which topic you like to include? Or send us a mail with some ideas of content you would like to find here, be sure they will always be welcomed.

Hope to hear from you soon and hope you can enjoy this new edition.

Director’s Last Message
J Parsons, Jacobs

Construction & Design Division,
Hi all. I guess this will be my last message out as Director. These last few years have been interesting and fulfilling and I think the division is in capable hands with Ray and Phil.

So where are we at currently... Our membership numbers have grown some, which is good. I hope that ISA starts allowing people to change their division preferences more easily. Please encourage your co-workers and other people in your section to join the division.

There will be a division report card at the ALC this year. I’ve seen the draft and while we are behind in some areas (technical content, webinars, outside engagement), we are doing good on collaboration and events. I would encourage everyone to think about the types of technical content you can bring to the membership. Even if you didn’t write it, was there a good article or paper that we can see about re-publishing here in the newsletter or inviting the author to speak at an upcoming event or webinar.

I am proud that we were once again nominated for the Division Excellence award this year. And while we didn’t win, the efforts of the team here are being recognized in ISA. And working off the success of the ISA@Montreal event we’ve been asked to participate in ISA’s first conference under the new business model announced at last year’s ALC. This will be on IIoT and Industry 4.0 and will cover both design and implementation. CONDES was instrumental in developing the programing tracks and structure of the event. The conference will be April 14-16, 2020 in Galveston, Texas. Look for more information when the official site goes live (isa.org/iiot).

We are looking for speakers, presenters, and panel members for the event, so please reach out to your network and get them involved and consider attending the event yourself.

The Annual Leadership Conference is fast approaching. Myself, Ray, and Phil will all be there. Will you? I’m always happy to meet our members and these events have plenty of time to do so. Maybe you want to get involved but don’t know where to start. This is the event for you. Check with your ISA Section or employer for funding options.

That’s all! It has been an honour serving as your Director. I will still be kicking around, so feel free to reach out with questions or find me at an ISA event and say “hi”.

New Director Elect’s Personal Biography
Phil Reppert

Phil graduated Penn State with an Assoc. Degree in Chem Eng. and got introduced to instrument design work when a friend at Gilbert Assoc. mentioned there was a job posted with an “interesting” listing. It was in the instrument group and they were looking for an electrical, mechanical or chemical engineering degree, how interesting. I applied for the job and got it and thus began my 40-year career in instrument design!

I am a past DVP of District 2 and delegate for my own Lehigh Valley Section of ISA as well as “the Bagman”, AKA treasurer, of Lehigh Valley section.

As a senior life member of ISA, I proudly tell anyone I work with about ISA, especially our S5 and S20 standards. I enjoy helping junior people at work and recently a co-op student who had just graduated from college, was hired by my current employer, Optimum Controls Corp. I was working on a piping design that needed to be automated and I helped him with the upstream and downstream instrument location problems.

We really need to make sure the “basics” get passed down to people in our field, especially in the Construction and Design of instrumentation.

I look forward to hearing some feedback from my fellow CONDES members.
About Upcoming events

Annual Leadership Conference
25-28 October 2019
Paradise Point
San Diego, California, USA

Who should attend:
Elected and appointed Department Directors, Division Directors, Assembly members, Executive Board members, Section Leaders and Delegates

ISA PIC 2019 - Process Industry Conference
4-6 November
Houston, TX USA

ISA PIC 2019 combines the technical expertise, knowledge, and experience of ISA along with leading experts across critical areas covering process instrumentation/control, cybersecurity & safety systems, open architecture & infrastructure, and operational excellence as well as robotics and subsea automation.

By offering a leading-edge technical program for addressing the demands of a changing world, ISA PIC 2019 is the process industry event that engineers, and automation professionals can’t afford to miss.

Program Benefits

- **Keynote presenters** will reflect on the imagination of today’s thought leaders and innovators and provide perspective on the latest advances and trends in manufacturing technologies and applications.

- **Comprehensive technical tracks** will cover the crucial issues facing today’s manufacturing decision-makers—and those expected to determine both success and failure in the years ahead.

- **Expert-led training courses** will provide an added advantage for professional development on topics related to industrial cybersecurity, alarm management, and safety instrumented system criticalities.

- **An exhibitor showcases** of networking and promotional opportunities providing prime access to key industry products, services, and solutions.

ISA PIC 2019- Process Industry Training

7 November
Houston, TX USA

- Introduction to Industrial Automation Security and the ISA/IEC 62443 Standards (IC32C)
- CyberSensors: Advancements in Automation CyberPhysical Security (IC87C)
- Introduction to the Management of Alarm Systems (IC39C)
- An Introduction to Safety Instrumented Systems (EC50C)
Executive Summary

Effective cybersecurity management is essential for all organizations, regardless of size. There are many standards and guidance documents available to help organizations determine a way forward.

This document is intended to provide a starting point for small- and medium-businesses (SMBs), particularly those that manage industrial processes and employ some level of automation. Specific examples include SMBs in the chemical and wastewater treatment sectors.

While it is generally accepted that Operational Technology (OT) system security requires different or additional measures than general-purpose Information Technology (IT) system security, it is also true that smaller companies might have difficulty implementing much of the available guidance.

Standards and practices are often based on the assumption that engineering and operations resources are available to define, implement, and monitor the technology, business processes, and associated controls. Unfortunately, this is often not the case.

Smaller operations are typically not staffed to include such roles. It is more common to have broadly defined staff roles, with support and operation of IT systems as only part of an individual's responsibilities.

Smaller companies may not even be fully aware of the risks they face or that they can contract for cybersecurity-related services. This guide is intended to identify the essential controls that need to be established.

SMBs need to understand their cybersecurity risk and to take action to reduce this risk, just as they do with other business risks. The absence of previous incidents, or the belief that the organization is not a likely target, is not sufficient justification for ignoring this issue.

SMBs can be at risk from a wide variety of threats, including amateur and professional hackers, environmental activists, disgruntled employees or contractors and even nation states or terrorists. In addition, many cybersecurity incidents are a result of accidents or unintentional actions. A company does not have to be a specific target to be affected.
The consequence to an SMB can vary tremendously based on the nature of operations and the vulnerabilities of each. It is essential that the underlying vulnerabilities are recognized and that these vulnerabilities be mitigated to minimize the likelihood of potentially dire events.

This document provides guidance based on well-established frameworks and standards. Further reference should be made to these frameworks and standards, focusing on the recommendations in this document.

Cybersecurity management is not a one-time activity. Like quality and safety management, cybersecurity management is an ongoing activity where continuous improvement must be made in order to manage the risks.

Why Cybersecurity Management is Important

Protecting businesses from the impact of a cybersecurity incident

Very few, if any, businesses today operate without some dependence on systems and equipment that are vulnerable to a cybersecurity incident. The impact to the business of such an incident will vary. However, this impact needs to be understood and managed accordingly if businesses are to be able to operate as expected.

There are two broad categories of systems and equipment: Information Technology (IT) and Operational Technology (OT), each with their own characteristics, as shown in the table 1 below.

Table 1 - IT and OT characteristics

<table>
<thead>
<tr>
<th>Information Technology (IT)</th>
<th>Operational Technology (OT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>Used in a business or office environment to support day-to-day activities, such as accounting, ordering, human resources, and data analysis.</td>
</tr>
<tr>
<td><strong>Examples of systems or equipment</strong></td>
<td>Used to monitor and control processes in industrial environments, such as factory floors, refineries, oil and gas platforms, and water treatment operations.</td>
</tr>
<tr>
<td>• User workstations or laptops</td>
<td>• Programmable Logic Controllers (PLCs)</td>
</tr>
<tr>
<td>• File, email, or web-servers</td>
<td>• Distributed Control Systems (DCSs)</td>
</tr>
<tr>
<td>• Databases</td>
<td>• Supervisory Control And Data Acquisition (SCADA) systems</td>
</tr>
<tr>
<td>• Network devices (routers, firewalls, switches)</td>
<td>• Historian databases</td>
</tr>
<tr>
<td>• Protocol and media converters</td>
<td></td>
</tr>
<tr>
<td><strong>Cybersecurity concerns</strong></td>
<td>System availability is the primary concern, followed by integrity of the data, and finally, data confidentiality. In OT, data integrity and confidentiality are particularly important for device logic or configuration files used in control applications.</td>
</tr>
<tr>
<td><strong>Management of Change</strong></td>
<td>Technological changes are part of the overall Management of Change process. It can be difficult to take equipment out of service to update.</td>
</tr>
<tr>
<td><strong>Other factors</strong></td>
<td>• Equipment and communications protocols tend to be proprietary, and it can be difficult to implement typical cybersecurity controls</td>
</tr>
<tr>
<td>• It is becoming more common for employees to use their own devices, especially mobile technology, to access business systems</td>
<td>• Underlying technology can be antiquated and, therefore, more vulnerable to basic cybersecurity incidents</td>
</tr>
<tr>
<td>• New technologies are being adopted with insufficient concern for security</td>
<td>• The equipment environment is almost always heterogeneous, with devices of various ages and sources</td>
</tr>
</tbody>
</table>
Risk Assessment

Cybersecurity-related risks are evaluated using a process that: systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifies loss exposures and consequences based on probability of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure.

In simple terms, risk can be defined as a function of threat, vulnerability, and consequence. Each of these elements must be assessed in order to gain a full understanding of the situation.

Table 2 - Threat examples

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amateur hackers</td>
<td>With access to many online tools and resources, anyone can find systems connected to the Internet and interfere with their operation, often for the challenge or prestige.</td>
<td>The online community HackForums.net is a popular forum for amateur hackers and is believed to be behind the PlayStation network attack on Christmas Day 2014, as well as the attack on the Internet Name Servers in the Eastern USA in October 2016.</td>
</tr>
<tr>
<td>Professional hackers</td>
<td>Hackers with more skills and resources target organizations with ransom ware and other disruptive techniques and tools for profit.</td>
<td>In 2016, the Lansing Board of Water &amp; Light was forced to pay a $25,000 ransom to unlock its internal communications systems, which were hit as part of a larger attack. The utility estimated the total cost of responding to the attack and strengthening its defenses against future attacks was $2.4M.</td>
</tr>
<tr>
<td>Environmental activists</td>
<td>Groups can work with hackers to disrupt the operations of organizations whose business practices they oppose or are contrary to their beliefs.</td>
<td>In 2011, the group Anonymous posted confidential information on 2,500 Monsanto employees and associates and shut down the company’s international websites for nearly three days.</td>
</tr>
<tr>
<td>Disgruntled employees or contractors</td>
<td>Using inside knowledge or privileged access, to gain revenge by disrupting operations or to steal confidential information to be sold to competitors</td>
<td>In 2012, a male programmer—passed over for promotions at a Long Island power supply manufacturer—created an unauthorized program to harvest employees’ logins and passwords. After leaving the company, the person used his credentials to get into the network and disrupt business and inflict damage on the company’s operations.</td>
</tr>
</tbody>
</table>
Table 2- Continuation from previous page

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation states or terrorists</td>
<td>Organizations with very large resources target critical infrastructure organizations to create instability or to influence their will.</td>
<td>In 2010, a virus known as Stuxnet compromised Iran's nuclear enrichment facility. The virus targeted the control system for the centrifuges in the facility and, while providing pre-recorded data to operators, would cause the centrifuges to operate outside of their normal envelope. Analysts suggest the enrichment program was set back several years as a result of the attack.</td>
</tr>
<tr>
<td>Accidents or unintentional actions</td>
<td>The actions of employees or contractors can inadvertently result in a cybersecurity incident.</td>
<td>In 1999, an explosion in a gasoline pipeline in Bellingham, WA, USA, killed three people, injured eight, and caused $45M in property damage. The company was fined $112M. One of the two primary causes of the incident was found to be developers making changes to a live control system.</td>
</tr>
</tbody>
</table>

Common vulnerabilities and key mitigations

A vulnerability is a deficiency that can be exploited by a threat to create an incident. The deficiency can arise from technical (such as a software error), procedural (a lack of policy or standard), or people (lack of training) issues.

A mitigation is an action or solution that is implemented to: reduce the likelihood of a vulnerability being exploited or offset the adverse effects of an incident should that vulnerability be exploited.

There are many cybersecurity vulnerabilities, and each organization possesses different ones depending on the equipment they use and the policies and procedures they have in place.

As noted previously in this article, SMBs can be impacted by a non-targeted attack, simply because they utilize equipment similar to that used by the primary target.

The table below provides a list of common vulnerabilities found in all organizations to some degree, along with key mitigations that should be implemented to control these vulnerabilities.

These key mitigations are essential for all SMBs to provide a basic level of cybersecurity management. It is highly recommended for SMBs to consider additional mitigations. Further guidance is available from several sources, including:

- International Society of Automation (ISA). The ISA/IEC 62443 standards (Security for Industrial Automation and Control Systems) provide detailed guidance on how to create a cybersecurity management system for OT environments. These standards are also available internationally as IEC 62443
- The US Chamber of Commerce, Department of Homeland Security (DHS), US Small Business Administration (SBA), National Institute of Standards and Technology (NIST), as well as many business and technology websites,
- The Center for Internet Security (CIS). CIS produces the Critical Security Controls, which identify the top 20 mitigations that reduce the likelihood and/or consequence of a cybersecurity incident. These controls are referenced in the Key Mitigations table below as CSC “xx” where “xx” is 1 to 20 (for example, CSC17)
Table 3 – Vulnerabilities and Mitigations

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
<th>Key Mitigations</th>
</tr>
</thead>
</table>
| Inadequately trained employees | Employees who have received little or no training in the risks of cyber incidents are more likely to:  
  - Be victims of social engineering, such as phishing (the use of faked email messages to extract confidential information or to gain unauthorized access to equipment)  
  - Use removable media without performing virus checks  
  - Fail to observe the signs of a cyber incident  
This is common in SMBs, where resources for training are limited.                                                                 | • Provide (internally or using external parties) a variety of training resources for employees, including classroom-based, computer-based training courses/assessments, informational videos, posters, and email newsletters (CSC17)                                                                                   |
| Inadequately secured network   | Networks that are inadequately secured can:  
  - Allow external users unauthorized access to systems and equipment  
  - Increase the chances of a cybersecurity incident extending throughout an organization  
SMBs may not have the expertise to adequately secure their network.                                                                 | • Use standards to define and implement effective network security. In particular, avoid direct connection with external networks, control traffic in and out of the internal network, and between different areas of the internal network (CSC1,2,6,12,13,15,20)                                        |
| Inadequately secured equipment | Equipment that is inadequately secured can:  
  - Lack appropriate physical security, allowing ease of access to unauthorized users and increase the likelihood of accidental actions  
  - Lack appropriate protection on physical inputs, such as USB ports and DVD drives, making it easier for malware to be transferred  
  - Contain unnecessary applications or run unnecessary services, increasing the possibilities of a cyber incident  | • Where possible, keep equipment in locked cabinets or rooms to avoid unnecessary contact  
• Where not possible, use locks (physical and electronic) to secure access to physical inputs  
• Remove unnecessary applications and disable unnecessary services on equipment (CSC1,2,3,6,7,11,13,18)                                                                                               |
| Inadequate anti-virus management | Equipment running without anti-virus protection is vulnerable to malware attack. With some malware, the infection may not be obvious, and this can lead to a spread of the malware throughout the organization.  
A failure to maintain anti-virus protection (with the latest security patches or with the latest malware signatures) makes equipment much more vulnerable to newer malware threats. | • Ensure anti-virus is operational and maintained on all equipment, where possible  
• Where not possible, ensure equipment is adequately secured to remove opportunity for introduction of viruses  
• Use standalone machine to perform virus checking on incoming machines and media (CSC8)                                                                                                                                                       |
### Table 3 – Continuation from previous page

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
<th>Key Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate change management</td>
<td>There are two important considerations for change management:</td>
<td>• All changes must be reviewed before implementation. The review must assess the potential impact on system operation (reliability, performance, etc.) as well as any changes to cybersecurity risks.</td>
</tr>
<tr>
<td></td>
<td>• Making changes to system software or hardware can introduce new vulnerabilities that, if not considered, could be exploited</td>
<td>• A change procedure must be in place that ensures that all changes are implemented with a step-by-step plan and a means to restore any equipment to its previous state, if required (CSC4,20)</td>
</tr>
<tr>
<td></td>
<td>• Inadequate change procedures can create cybersecurity incidents. For example, a failure to implement a backup before updating software could result in system unavailability if the update fails</td>
<td></td>
</tr>
<tr>
<td>Inadequate security patch management</td>
<td>Equipment running without the latest security patches is much more vulnerable to newer malware threats. The more security patches that are missed, the more vulnerable the equipment becomes.</td>
<td>• Ensure equipment is kept up to date with latest security patches from vendor(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (CSC3,11,18)</td>
</tr>
<tr>
<td>Inadequate backup management</td>
<td>Backups are essential to the restoration of failed hardware or equipment infected with malware. In order to be effective, backups must occur frequently to avoid the loss of significant amounts of data. In addition, unless backups are periodically tested, they can prove to be useless when required.</td>
<td>• Determine what needs to be backed up and how often</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maintain backups to defined regime</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Periodically test backups using a test environment (CSC10,13)</td>
</tr>
<tr>
<td>Inadequate password management</td>
<td>There are two key issues:</td>
<td>• Enforce use of strong passwords</td>
</tr>
<tr>
<td></td>
<td>• Weak passwords are easy to guess (e.g. ‘password’) or use only letters or numbers. A weak password can be determined using ‘brute force’ techniques, within 1-2 minutes</td>
<td>• Enforce periodic change of passwords (CSC5,14,15,16)</td>
</tr>
<tr>
<td></td>
<td>• Passwords that are never changed, or changed infrequently, are much more vulnerable to exploitation</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3 – Continuation from previous page

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Description</th>
<th>Key Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of shared accounts</td>
<td>There are many problems with sharing accounts between users:</td>
<td>• Avoid use of shared accounts, where possible</td>
</tr>
<tr>
<td></td>
<td>• It is no longer possible to verify who took a certain action in a system</td>
<td>• If not possible, ensure shared accounts have limited privileges</td>
</tr>
<tr>
<td></td>
<td>• Not all users may have the same privileges, so some users may have access</td>
<td>• Enforce a policy to change account details when someone leaves or moves to a new role in the organization (CSC5,14,15,16)</td>
</tr>
<tr>
<td></td>
<td>to functions or data that they should not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When someone leaves, knowledge of the account details are retained by the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>person who left</td>
<td></td>
</tr>
<tr>
<td>Use of default accounts</td>
<td>Many devices or systems have manufacturers’ default accounts. If these</td>
<td>• Remove or change default account details (username and/or password), where</td>
</tr>
<tr>
<td></td>
<td>accounts are not changed, anyone with knowledge of the default details can</td>
<td>possible</td>
</tr>
<tr>
<td></td>
<td>gain unauthorized access much more easily.</td>
<td>• If not possible (e.g. hardcoded by vendor), enforce strict physical access</td>
</tr>
<tr>
<td></td>
<td>In some cases, default account information is freely published on the</td>
<td>control on equipment (CSC5,14,15,16)</td>
</tr>
<tr>
<td></td>
<td>Internet.</td>
<td></td>
</tr>
<tr>
<td>Inadequate incident response</td>
<td>Many organizations have no plans in place to deal with a cybersecurity</td>
<td>• Create an incident response plan that identifies the possible incidents and the</td>
</tr>
<tr>
<td></td>
<td>incident.</td>
<td>appropriate response to each, as well as the key internal and external contacts</td>
</tr>
<tr>
<td></td>
<td>Organizations that have plans in place may not exercise those plans</td>
<td>• Exercise the incident response plan periodically to verify that it is effective</td>
</tr>
<tr>
<td></td>
<td>sufficiently, to validate that they are effective.</td>
<td>(CSC20)</td>
</tr>
<tr>
<td></td>
<td>Without an effective incident response plan in place, organizations can be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exposed to major consequences should a cybersecurity incident occur.</td>
<td></td>
</tr>
</tbody>
</table>
### Potential consequences of inadequate cybersecurity management

The potential consequences of a cyber incident will depend on the organization, but the following table outlines the most common consequences for IT and OT equipment and systems.

Table 4 – Potential consequences

<table>
<thead>
<tr>
<th>Consequence</th>
<th>IT/OT</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of confidential information</td>
<td>IT/OT</td>
<td>Hackers use social engineering techniques to obtain confidential information, such as usernames and passwords that can be used to gain unauthorized access to systems.</td>
<td>In 2014, payment card data for 70 million customers was stolen from Target, after hackers gained access using the credentials of a supplier, stolen in a separate phishing attack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hackers with unauthorized access to systems can extract confidential information, such as customer names, credit card numbers, trade secrets, drawings, or plans.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In OT environments, theft of control logic, recipes, production records, and other such information can yield valuable intellectual property.</td>
<td></td>
</tr>
<tr>
<td>System unavailability</td>
<td>IT</td>
<td>Computer viruses can be downloaded onto IT workstations, laptops, and servers remotely (using unauthorized access or through the use of social engineering), or using removable media, such as USB drives, CDs, and DVDs.</td>
<td>In 2012, a virus called Shamoon infected more than 30,000 office workstations belonging to Saudi Aramco. Business operations were slowed and, in some cases, paused as employees were forced to resort to manual/off-line activities and the use of personal emails for several weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Viruses can propagate across a network to infect other machines. Viruses may be used to:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Obtain confidential information (such as usernames and passwords)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cause excessive network traffic that disrupts normal operation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Wipe an entire hard disk clean</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lock a disk until a ransom is paid</td>
<td></td>
</tr>
<tr>
<td>Operations or production shutdown</td>
<td>OT</td>
<td>Since operations or production are heavily dependent on the OT systems that monitor and control them, a failure of these systems can result in a shutdown of the plant or process.</td>
<td>In 2013, a virus infected the operation-al network of the Cook County Department of Highway and Transportation in Chicago, affecting 200 computers. The department was shut down for nine days until normal service could be restored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Typical cybersecurity causes are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Viruses</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unauthorized access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lack of backup of system data, program, or settings</td>
<td></td>
</tr>
</tbody>
</table>
Table 4 – Continuation from previous page

<table>
<thead>
<tr>
<th>Consequence</th>
<th>IT/OT</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Service outage    | OT    | In a specific instance of operations or production shutdown, the result can have serious ramifications for others. For example, the loss of water or wastewater services, the loss of communications, etc. Typical cybersecurity causes are:  
  • Viruses  
  • Unauthorized access  
  • Lack of backup of system data, program, or settings | In 2015, hackers infiltrated the control system of a Ukrainian power company and took control of the electricity distribution network. Approximately 80,000 homes were left without electricity for up to six hours.          |
| Equipment damage  | OT    | Production or operational plants are connected to the monitoring and control systems that can be impacted by a cybersecurity incident.  
  Without adequate mechanical or independent shutdown systems, physical damage is possible.  
  Typical cybersecurity causes are:  
  • Viruses  
  • Unauthorized access | In 2014, hackers gained access to a steel mill in Germany and disrupted the operation of the safety system, causing massive damage to the blast furnace. |
| Environmental damage | OT   | Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to the environment. Examples include oil and gas production and wastewater treatment.  
  Typical cybersecurity causes are:  
  • Viruses  
  • Unauthorized access | In 2000, a disgruntled former contractor used stolen equipment to deliberately manipulate a wastewater control system, causing a release of 750,000 gallons of raw sewage into the environment in Queensland, Australia. |
| Injury or death    | OT    | Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to personnel or members of the public. Examples include oil and gas production, transportation, and wastewater treatment.  
  Typical cybersecurity causes are:  
  • Viruses  
  • Unauthorized access | In 2008, a 14-year old boy modified a TV remote to change the points on a train network in Lodz, Poland. Twelve people were injured, and four trains derailed. |
Essential cybersecurity activities
Numerous standards and guidance documents are available to help SMBs implement proper cybersecurity management.

The US Cybersecurity Framework, produced by the National Institute of Standards and Technology (NIST)\(^\text{vii}\), is an excellent starting point for SMBs.

The Framework identifies five core functions that encapsulate cybersecurity management. The Framework then further defines all the activities that may need to be undertaken for each function and identifies relevant standards to help identify how to implement these activities.

The table below identifies the essential cybersecurity activities that should be undertaken by all SMBs. These are described in more detail below the table.

Table 5 – Essential Cybersecurity Activities

<table>
<thead>
<tr>
<th>Framework Functions</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Create an inventory of all IT and OT assets</td>
</tr>
<tr>
<td>Protect</td>
<td>Secure network and equipment</td>
</tr>
<tr>
<td>Detect</td>
<td>Define methods for monitoring</td>
</tr>
<tr>
<td>Respond</td>
<td>Maintain an incident-response plan</td>
</tr>
<tr>
<td>Recover</td>
<td>Maintain backups of all systems and equipment</td>
</tr>
</tbody>
</table>

Identify
The identify function focuses on understanding the nature of the systems inventory owned by the SMB and what risks are associated with this inventory.

Create an inventory of all IT and OT assets
This step is essential for all SMBs. Proper cybersecurity management is impossible without a definitive understanding of the assets involved. Organizations that fail to identify equipment or systems leave themselves vulnerable to cyber incidents due to a lack of protection or monitoring.

The inventory of assets should include, as a minimum:

- Make and model of hardware
- Version number of all operating system and application software

Additionally, some organizations identify equipment location, owner, and other useful information.

Assess the risk of a cyber incident
Once an SMB understands what it is protecting from a cyber incident, it must conduct a risk assessment to identify what risks exist.

Risk assessments require the involvement of all key stakeholders (to ensure accuracy) and should identify the likely threats and the vulnerabilities in the asset base. From this, the organization should identify the potential consequences, e.g. loss of confidential information, loss of revenue, environmental impact, injury or death, and so on.

SMBs should rank their risks using a common methodology to allow the identification of risks in priority order.

Define a cybersecurity management policy
Every SMB should have a cybersecurity management policy to define:

- Those responsible for cybersecurity
management activities

- The processes and procedures required for operational activities and to reduce cybersecurity risks
- The expectations of employees (e.g. appropriate use of IT equipment, use of personal devices, etc.)

Protect

The protect function is a core cybersecurity management activity that an organization must undertake on an ongoing basis.

Secure network and equipment

Securing a network and equipment involves such actions as:

- Physically locking or disabling all equipment inputs to prevent unauthorized use, including smart device charging
- Using only dedicated devices that are kept secure, with anti-virus software scanning before and after use
- Using a quarantine area to check incoming removable devices of unknown provenance and transfer files to dedicated, known devices
- Only allowing a transfer of files from removable devices under strict supervision and in compliance with anti-virus checks
- Applying recommended patches to operating system and application software in a timely manner
- Testing patches before applying to live equipment
- Keeping anti-virus software up to date
- Performing an anti-virus scan regularly and frequently (e.g. monthly)
- Maintaining a record of all updates applied to allow for identification of issues
- Limiting external access to equipment and networks to only those authorized to access them

Protect sensitive information

Protecting sensitive information involves such actions as:

- Keeping confidential information secure (e.g. in locked cabinet or safe) and disposing confidential information in a secure manner (e.g. shredding)
- Being aware of who is around you and taking care to avoid disclosing sensitive information
- Being suspicious of emails if you do not recognize the sender
- Making sure you don’t click on links or open attachments unless you are certain the sender is trustworthy
- Making sure you do not download or install anything after following a link in a suspicious email
- Making sure you do not provide confidential information via email unless you are certain the recipient is appropriate/authorized
- Making sure a supervisor or trained expert is available for advice before individuals take any action

Manage access to systems and equipment

Managing access to systems and equipment involves such actions as:

- Maintaining physical and electronic security to ensure that only authorized persons have access to the equipment they require in performing their role
- Securing equipment in locked rooms or cabinets and monitoring access
- Performing background checks on all users before approving access
- Maintaining a register of approved users
- Preventing sharing of login credentials between users
- Removing or changing credentials when a user moves to a new role or leaves
- Removing or changing default accounts
- Enforcing strong passwords and changing regularly
- Providing temporary external access as required, supervise during use, and remove once complete

**Detect**

Having established an understanding of its asset base and the risks to it, the SMB must then have methods to monitor for incidents, so that it is able to respond promptly and effectively to minimize the impact.

**Define methods for monitoring**

Monitoring methods will vary from organization to organization, based on the particular asset base and risk assessment. In some cases, manual methods, such as checking log and system files, will suffice. For larger organizations with more electronic activity, this may be impractical and automated tools may be needed. Define responsibilities for monitoring

Having defined the methods for monitoring, the SMB must assign responsibilities for these activities.

In addition, all employees should receive awareness training, be instructed to be vigilant for signs of a cyber incident and be trained to report any type of cyber incident.

**Identify improvements**

Cybersecurity is an ever-changing situation. Threats, vulnerabilities, and risks change and SMBs need to be able to adapt. In the detect function, SMBs must regularly review their monitoring methods and adjust them to suit changing circumstances and according to incident experiences.

**Respond**

The respond function comes into effect when an incident occurs. However, preparation is essential to a successful response, and so an organization must take actions well in advance of any incident.

**Maintain incident response plan**

Key to a successful response, with minimal impact, is an effective cybersecurity incident management plan. The plan needs to identify the possible cybersecurity incidents that may occur within the organization and document the step-by-step procedures that should be followed in the event of each one. All employees should be aware of the risks of cybersecurity incidents and their role in avoiding them.

**Practice response processes**

SMBs must test their cybersecurity incident management plan on a periodic basis. The test must be realistic and exercise as many of the elements as possible, so as to be certain that established procedures will work when required.

**Identify improvements**

SMBs will need to update their incident management plans in response to changes in the cybersecurity landscape, and also as a result of their incident response tests.

**Recover**

While the respond function comes into effect when an incident occurs, the recover function comes into effect once the respond function is completed. As with the respond function, preparation is essential to a successful recovery, and so an SMB must take actions well in advance of any incident.

**Maintain backups of all systems and equipment**

Key to a successful recovery from a cybersecurity incident is having the right backups in place. Having the right back-ups in place requires an SMB to:

- Identify what needs to be backed up
- Determine back-up frequency based on operational requirements (How long can you operate without a working system? How much data can you afford to lose?)
- Store clearly labeled backups securely on-site and off-site, preferably in a fireproof safe

**Practice recovery processes**

SMBs must test their cybersecurity incident recovery processes on a periodic basis. The test must be realistic and exercise as many of the elements as possible, so as to be certain that established procedures will work when required.

**Identify improvements**

SMBs will need to update their recovery processes in response to changes in the cybersecurity landscape, and also as a result of their incident recovery tests.
Awareness and training

The importance of awareness and training for employees cannot be understated. No amount of technical and procedural mitigations will help if an employee takes an insecure action (e.g. inserting a removable drive without performing an anti-virus scan) due to lack of training or awareness.

External classroom and online training courses are recommended for SMBs to give their employees a clear understanding. Internal resources, such as assessment (surveys, tests) and awareness (videos, posters, emails) tools, should be used to complement external courses and provide a constant reminder to employees.

Effective cybersecurity management should be a high-profile business objective that is reported on by management so that employees are constantly reminded of its importance.

The International Society of Automation (ISA) provides training courses and certificate programs based on the ISA/IEC 62443 (Security of Industrial Automation and Control Systems) standard.

Assessment and continuous improvement

Self-assessment

The International Society of Automation (ISA) has produced a survey that SMBs can take to self-assess their current cybersecurity posture (as well as re-assess it after making changes).

To obtain a copy of the survey, contact ISA at info@isa.org

Third-party assessment

For a nominal fee, ISA can review an SMB’s survey responses. ISA utilizes a pool of international cybersecurity Subject Matter Experts (SMEs) to provide this service. This third-party assessment will provide a more comprehensive, and independent, review of the SMB’s cybersecurity posture, with advice on how to proceed.

Continuous improvement

Effective cybersecurity management requires continuous improvement. The essential activities outlined above are only the beginning.

For each of the five core functions of the Cybersecurity Framework, there are many degrees to which SMBs can go. For example:

- Network and equipment monitoring can be a manual activity in its simplest form, but SMBs can purchase specialty software to assist
- Third-party organizations can provide assessment services, including penetration testing, to validate the effectiveness of cybersecurity mitigations

The degree to which SMBs should go will depend on the level of risk they perceive, and this may vary with time. In addition, cybersecurity is continuously evolving, with new vulnerabilities, exploits, and threats arising all the time. SMBs must continuously review their risk and adapt their mitigations to suit this changing landscape.

References

All references related to this White paper were listed on the last page of this Newsletter.
ISA’s leadership in Cybersecurity

Source: https://www.isa.org/isa99/

ISA is a global leader behind the world’s only consensus-based industrial Cybersecurity standard, because of its expertise developing standards, knowledge of challenges for industrial applications, and high human quality of experts behind the developing of new standards.

ISA formed the ISA99 Committee as an international program to develop the ISA62443-X-Y series an extensive set of Standards for industrial automation and control systems (IACS) and critical infrastructure.

About the work of ISA 99 Committee

Who they are?

Established on 2002, growth from a couple of people to 500+ members of many companies across all industrial sectors consistent with the global reach and scope of ISA.

The ISA99 standards development committee brings together industrial cyber security experts from across the globe to develop ISA standards on industrial automation and control systems security.

This original and ongoing ISA99 work is being utilized by the International Electrotechnical Commission in producing the multi-standard IEC 62443 series.

Scope

The ISA99 committee addresses industrial automation and control systems whose compromise could result in any, or all, of the following situations:

- endangerment of public or employee safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on national security.

The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to:

- hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Physical security is an important component in the overall integrity of any control system environment, but it is not specifically addressed in this series of documents.

Work

ISA has charged with the majority of the development and the plan for the IEC is to adopt it as an equivalent IEC62443-X-Y standard.

ISA99 Committee has a formal relation with international Standards development organizations (SDOs) committees, IEC and ISO to coordinate the development of ISA62443 series avoiding the need to create duplicate committees in each organization.

In addition, the ISA99 committee has been working closely with the Joint Technical Committee or JTC of ISO and IEC to ensure that the development of Cybersecurity Standards and practices are consistent with the general cybersecurity standards in the ISO27000 series.

Within the ISA’s Automation Federation, ISA99 committee also work with the industrial Security Compliance or ISCI to ensure that ISA secure certification program remains consistent with the contents of 62443-X-Y series.

Furthermore, the ISA99 committee also maintain relationships with other ISA committees and groups as ISA84 (Instrumented Systems) and ISA100 (Wireless systems for automation) to ensure that their perspectives and needs are adequately addressed.
Work products in the ISA/IEC 62443 series

The following diagrams shows a description and the status of work products developed by ISA in the ISA/IEC 62443 series of IACS standards and technical reports.

**ISA99.00.01 - Part 1**
Terminology, concepts and models
Contains standards and reports that are in general nature and must be understood by the entire stakeholder community in order to successfully apply the standards.
- ISA-62443-1-1 Concepts and Models
- ISA-62443-1-2 Master glossary of terms and abbreviations
- ISA-62443-1-3 System security conformance metrics
- ISA-62443-1-4 IACS security lifecycle and use-cases

**ISA99.00.03 - Part 3**
Operating an Industrial Automation and Control System Security Program
Focuses on the technology related aspects of security, this includes both, an assessment of available technologies and their suitability for use within this context as well as the specific requirements related to the technical aspects of a security program.
- ISA-TR62443-3-1 Security technologies for IACS
- ISA-62443-3-2 Security risk assessment and system design
- ISA-62443-3-3 System security requirements and security levels

**ISA99.00.02 - Part 2**
Establishing an Industrial Automation and Control Security Program
Addresses the people and process aspects of an effective cybersecurity program, the audience of these documents includes people who develop and operate these programs across the entire cycle of
- ISA-62443-2-1 Security program requirements for IACS asset owners
- ISA-62443-2-2 IACS protection levels
- ISA-62443-2-3 Patch management in the IACS environment
- ISA-62443-2-4 Requirements for IACS service providers
- ISA-TR62443-2-5 Implementation guidance for IACS asset owners

**ISA99.00.04 - Part 4**
Technical Security Requirements for Industrial Automation and Control Systems
Focuses on the specific security related to technical requirements of the products and components that are used to assemble industrial control systems.
- ISA-62443-4-1 Secure product development lifecycle requirements
- ISA-62443-4-2 Technical security requirements for IACS components

**Detail of Status -mark**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Approved with changes and comments</td>
</tr>
<tr>
<td>Adopted</td>
<td>In development</td>
</tr>
<tr>
<td>Published</td>
<td>Out for comments or Vote</td>
</tr>
<tr>
<td>Under revision</td>
<td>Development planned</td>
</tr>
</tbody>
</table>
ISA/IEC 62443 Cybersecurity Certificate Programs

As part of ISA’s continued efforts to meet the growing need of industrial control systems professionals and to expand its global leader outreach into the security realm, ISA has developed a comprehensive, knowledge-based certificate recognition program designed to increase awareness of the ISA/IEC 62443 standards and the critical areas as they relate to the IACS lifecycle.

The certificate programs are designed for professionals involved in IT and control system security roles who need to develop a command of industrial cybersecurity terminology, awareness, and understanding of the material embedded in the ISA99 standards.

ISA/IEC 62443 cybersecurity certificates are awarded to those who successfully complete a designated training program and pass a comprehensive multiple-choice proctored exam offered through the Prometric testing centers.

Individuals may register to take the training course(s) only and receive continuing education units (CEUs) for completion of the training course(s), or they can register for the affiliated certificate program which includes a separate knowledge-based examination.

All certificate program exams are administered electronically through Prometric testing centers.

Certificate program applicants must successfully complete the required course prior to taking the certificate exam.

Recommended experience
There are no required prerequisites for these programs; however, it is highly recommended that applicants have:

- 3-5 years of experience in the IT cybersecurity field preferably in an industrial environment—and at least 2 years specifically in a process control engineering setting
- Some level of knowledge or exposure to the ISA/IEC 62443 standards

Program Requirements
ISA/IEC 62443 designations and certificates will be awarded to individuals who meet the following program requirements:

Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- Successful completion of two-day, classroom training course: Using the ISA/IEC 62443 Standards to Secure Your Control Systems (IC32) or its online equivalent (IC32E).
- Earn a passing score on the separate, multiple-choice electronic certificate exam.

Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- Successful completion of three-day, classroom training course: Assessing the Cybersecurity of New or Existing IACS Systems (IC33).
- Successful completion of Certificate 1 requirements.
- Earn a passing score on the separate, multiple-choice electronic certificate exam.

Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist
- Successful completion of three-day, classroom training course: IACS Cybersecurity Design & Implementation (IC34).
- Successful completion of Certificate 1 requirements.
- Earn a passing score on the separate, multiple-choice electronic certificate exam.

Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist
- Successful completion of three-day, classroom training course: IACS Cybersecurity Operations & Maintenance (IC37).
- Successful completion of Certificate 1 requirements.
- Earn a passing score on the separate, multiple-choice electronic certificate exam.

ISA/IEC 62443 Cybersecurity Expert
- Individuals who achieve all Certificates (1 through 4) are designated as ISA99/IEC 62443 Cybersecurity Experts and receive confirmation and documentation relating to same.

Learn more about these certificate programs, eligibility criteria, renewal, and upcoming courses: www.isa.org/ISA99Certificate
ISA/IEC 62443 Standards Conformance Certifications

Source: [http://www.isasecure.org](http://www.isasecure.org)

About ISA Security Compliance Institute (ISCI)

The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure™ conformance certification program.

ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities.

ISCI ® Certifications

ISCI offers three certifications with four security assurance levels (SAL) in alignment with ISA/IEC 62443.

ISASecure Embedded Device Security Assurance (EDSA) Certification

The first ISASecure certification, Embedded Device Security Assurance (EDSA) focuses on the security of embedded devices and addresses device characteristics and supplier development practices for those devices.

The EDSA certification is designed to certify to international standard IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development requirements and to the international standard IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components.

An embedded device that meets the requirements of the ISASecure EDSA specification earns the ISASecure EDSA certification; a trademarked designation that provides instant recognition of product security characteristics and capabilities and provides an independent industry stamp of approval similar to a ‘Safety Integrity Level’ Certification (ISO/IEC 61508).

ISASecure System Security Assurance (SSA) Certification

The SSA requirements for certification include all control system requirements in IEC 62443-3-3 “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels” and all process requirements in IEC 62443-4-1 “Security for industrial automation and control systems – Secure product development requirements.” The certifier also performs System Robustness Testing, which includes fuzz testing, network traffic load testing, and vulnerability scanning.

In addition, embedded devices and other components included in the control system under test must be EDSA certified or meet the EDSA requirements for certifier testing and functional assessment at the time of certification.

ISASecure Security Development Lifecycle Assurance (SDLA) Certification

ISASecure SDLA is a certification program that applies to the development lifecycle processes of suppliers for control system products. The ISASecure SDLA certification program certifies compliance to IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product lifecycle requirements (also published as ANSI/ISA-62443-4-1).

To see the complete list of certified devices, visit the ISASecure Certified Device List page.
List of Cybersecurity Technical resources available for members

You will find some ISA technical resources about Cybersecurity in the list below, every item has a link to a webpage, press [CTRL] + Click to activate it.

ISA Standards
Review the Cybersecurity Standards using your Member benefit of View ISA Standards

Industrial Cybersecurity Certificate Program
- Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist
- Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist
- ISA/IEC 62443 Cybersecurity Expert

Classroom and In-Plant training
- Introduction to Industrial Automation Security and the ANSI/ISA99 Standards (IC32C)
- Using the ANSI/ISA99 Standard to Secure Your Control System (IC32)
- Industrial Networking and Security (TS12)
- Assessing the Cybersecurity of New or Existing IACS Systems (IC33)
- IACS Cybersecurity Design & Implementation (IC34)
- IACS Cybersecurity Operations & Maintenance (IC37)

On-line training
- Cybersecurity for Automation, Control, and SCADA Systems (IC32E)

Live Webinars
- Cybersecurity Risk Assessment for Automation Systems (IC32CW1)
- Firewalls and Security Zones on the Plant Floor (IC32CW2)
- A Tour of the ISA/IEC 62443 Security Standards (IC32CW3)

FREE Pre-Recorded Web Seminars
Take advantage of this material, it is FREE for all ISA Members:
- Cybersecurity for Control Systems in Discrete Automation
- Cybersecurity for Control Systems in Process Automation
- How to Identify and Overcome Cyber Security Challenges
- How to Protect Your Industrial Control Systems / SCADA Systems using Cryptography
- Network Security Series Part 2: Firewalls and Filtering Security on the Plant Floor
- Network Security Series Part 3: Encryption and Virtual Private Networks
- PLCs with Cyber Security and Asset Management System Integration Improve Plant Uptime and Safety
- Protecting Cyber Assets and Manifest Destiny from the Industrial Internet of Threats
- The Road to Digitalization Leads Through Cybersecurity
- Understanding growing cybersecurity threats for natural gas providers

FREE Technical Papers
You could find useful White papers as FREE resource for all ISA Members:
- ISA Technical Papers

White papers
- Whitepaper: “What Executives Need to Know About Industrial Control Systems Cybersecurity” By Joseph Weiss, PM, CISM, CRISC, Managing Director ISA99, Applied Control Solutions, LLC
- Whitepaper: “The Industrial Cybersecurity Problem” By Eric Byres, PE, Chief Technology Officer, Tofino Security, A Belden Brand

Webpages
- ISA99, Industrial Automation and Control Systems Security
- Automation Federation
- ISA Security Compliance Institut (ISCI)
New ISA book introduces an inexpensive, easy-to-understand way to protect against industrial cyberattack

Adapted from News and Press Releases, 12 June 2019.

International Society of Automation News Release
Contact: Jennifer Infantino Halsey
+1 919-549-8411
jenniferhalsey@isa.org

Research Triangle Park, North Carolina USA (12 June 2019) - With their advanced, microprocessor-based technologies, today’s industrial automation and control systems (IACS) deliver much-improved performance and features compared to their analog counterparts.

Unfortunately, these newer, networked systems-with their ability to be configured remotely-are more vulnerable to cyberattack.

Security PHA Review for Consequence-Based Cybersecurity, a new book published by the International Society of Automation (ISA), introduces an easy-to-follow, cost-effective methodology for safeguarding critical infrastructure and process industry facilities from cyberwarfare and other forms of cyber-risks.

The book illustrates how a Security Process Hazards Analysis (PHA) Review identifies hackable scenarios, ranks them appropriately, and pinpoints non-hackable safeguards-such as relief valves and current overload relays-that are not vulnerable to cybersecurity threats.

Written by Edward Marszal, PE, and James McGlone-two globally recognized experts in process safety, industrial cybersecurity, and the ISA/IEC 62443 series of IACS security standards-the book is designed to deliver clarity, simplicity, and confidence to those responsible for industrial cybersecurity.

"We were prompted to write this book because the industry and the cybersecurity practitioners are still unsure of what to do and why," emphasizes McGlone.

"In addition, the current approach in industrial cybersecurity focuses on network devices such as computers, Level 3 switches, and firewalls instead of on the process and machines that could be damaged or cause damage if control is lost.

"By analyzing the cause of and safeguards for cybersecurity weaknesses," McGlone explains, "it's possible to determine consequences that are potentially unaffected by the safeguards and those that could be caused by malicious intrusion, such as hacking. Any consequence that is not protected by existing safeguards or that can be caused by a cybersecurity attack is assigned an ISA/IEC 62443-based Security Level Target to be implemented or it is assigned an alternative safeguard or redesign to eliminate all or some of the cybersecurity risk."

McClone points out that the book is targeted to a wide range of automation and process industry professionals, including:

- Instrumentation and control system engineers and technicians
- Network engineers
- Process safety, health and safety, cybersecurity, and maintenance personnel
- Executives focused on risk reduction

Security PHA Review for Consequence-Based Cybersecurity

By Edward M. Marszal and Jim McGlone

To read more about this book, look inside or purchase a copy of, click here.

For greater perspective on the value and significance of the new book as well a more detailed overview of its content, read the Q&A feature with one of the book’s authors, click here.
ISA Standards News – 1Q 2019

This ISA Standards update is made available to ISA Sections and Divisions for use as desired in newsletters, blogs, and the like.

New ISA Standards and Technical Reports

ISA-TR84.00.07
Guidance on the Evaluation of Fire, Combustible Gas, and Toxic Gas System Effectiveness is intended to help address detection and mitigation of fire, combustible gas, and toxic gas hazards in process areas. Fire and gas systems per this technical report are a subset of industrial automation and control systems that are used in the process industries to detect loss of containment of hazardous materials from a process and initiate a response to mitigate the release impact. Loss of containment can be a small leak or a catastrophic release. It can be detected by measuring the presence of the released materials or inferred from the effects of the release.

ANSI/ISA-95.00.05
Enterprise-Control System Integration – Part 5: Business-to-Manufacturing Transactions, defines transactions in terms of information exchanges between applications performing business and manufacturing activities associated with Levels 3 and 4 of the Purdue Enterprise Reference Model. The exchanges are intended to enable information collection, retrieval, transfer and storage in support of enterprise-control system integration. This part of the ISA-95 series is consistent with the ISA-95.00.02 and ISA-95.00.04 object model attributes. Also defined are transactions that specify how to exchange the objects defined in ISA-95.00.02, ISA-95.00.04 and this standard.

ISA Standards News

United Nations Recognizes ISA99
The United Nations Economic Commission for Europe (UNECE) confirmed at its year-end annual meeting that it will integrate the widely used ISA/IEC 62443 series of standards into its forthcoming Common Regulatory Framework on Cybersecurity (CRF). The CRF will serve as an official UN policy position statement for Europe. At the same time, UNECE’s Working Party on Regulatory Cooperation and Standardization Policies recognized the ISA99 standards development committee for its leading role in conceiving and developing the widely used standards.

Healthcare Consortium Applies ISA 62443 Standards to Connect Medical Devices
The Medical Device Innovation, Safety, and Security Consortium (MDISS), a nonprofit public health and patient safety organization, has announced it is developing a set of recommended practices and profiles for securing medical systems based on the normative requirements in the widely used ISA/IEC 62443 series of standards for industrial automation and control systems cybersecurity. The intent is to share the information across the network of MDISS member organizations, which includes medical device manufacturers, healthcare software companies, hospital networks, and insurance companies. Application to connected medical devices reflects the growing use of the ISA/IEC 62443 standards not only across traditional manufacturing and industrial processing sectors worldwide, but also in rail transportation, building automation, and now medical systems.

For information on the ISA/IEC 62443 series of standards and related training and learning resources, contact Charley Robinson, ISA Standards, crobinson@isa.org or 1-919-990-9213.

For information on viewing or obtaining this or any ISA standard or technical report, visit www.isa.org/findstandards.
CONDES General Contact Information
CONDES Website www.isa.org/condes/
ISA Customer Support +1(919) 549-8411
Fax +1(919) 549-8288
Email info@isa.org

The International Society of Automation
67 T.W. Alexander Drive
PO Box 12277
Research Triangle Park, North Carolina, 27709, USA

Linkedin discussion group
https://www.linkedin.com/groups/12011693/

CONDES Volunteer Leader Contacts
Director
J Parsons
Corbin Consulting Engineers
Portland, Oregon, USA
Email: j.andrew.parsons@gmail.com

Director Elect
Ray Vandale
SMV Consulting
Calgary, Alberta, Canada
Email smvconsulting@platinum.ca

Phil Reppert
New Director Elect
Optimum Controls Corp.
Email: philr@optimumcontrols.com

Newsletter Editor
Willy Garcia Porcel
Florida Power & Welding International LLC
La Paz, Bolivia
Email: wmgarciaporcel@gmail.com

Membership Chair
Clifford Wuertz
Amec Foster Wheeler
Houston, Texas, USA
Email: clifford.wuertz@amecfw.com

Web Master (www.isa.org/condes)
Glendon Shaw
Autom8enrg, LLC
Houston, Texas, USA
Email: gshaw@autom8enrg.com

Web Master (LinkedIn Discussion Group)
Diego Orduz
Schlumberger Surencor

Bogota, Columbia
Email: diego.andresot@gmail.com

Program Chair
Naidu Signampalli
Technip
Doha, Qatar
Email: sinaidu@technip.com

Section-Division Liaison
Jonathan Rodden
BP
Jakarta, Selatan, Indonesia
Email: jonathan.rodden@se1.bp.com

Facilitator
Kalpen Vachharajani
Provincial Controls Ltd.
Sarnia, Ontario, Canada
Email: kalpenv@provincialcontrols.com

Committee Member
Don Segura
Saudi Aramco
Saudi Arabia
Email: donsegura@icloud.com

Committee Member
Patrick O’Hara
Seaboard Controls
Crosby, Texas, USA
Email: patrick@seaboardcontrols.com

ISA Staff Contact
Kimberly Belinsky
Manager of ISA Technical Divisions
Email: kbelinsky@isa.org

About ISA Construction & Design Division
The Construction and Design Division (CONDES) serves practitioners in all areas of automation, bringing together professionals involved in design, construction, and commissioning activities related to all types of facilities. CONDES support development of applicable standards, recommended practices, and technical papers. Within the construction and design arenas, Division Members are involved in all facets of facility design and construction, building automation, safety and security, construction management, and commissioning of facilities and process systems. After being dormant for several years, we are pleased to announce that our Construction and Design Technical Division is now active again!


Critical Security Controls, Center for Internet Security (CIS), https://www.cisecurity.org/critical-controls.cfm

The Cybersecurity Framework, National Institute of Standards and Technology (NIST), https://www.nist.gov/cyberframework


