Tofino Security | exida Consulting LLC

White Paper

Version 1.0
Published February 16, 2012

7 Steps to ICS and SCADA Security

Contents

Authors

Eric Byres, P. Eng., ISA Fellow
CTO and VP Engineering
Tofino Security,
a subsidiary of Belden Inc.
eric.byres@tofinosecurity.com
www.tofinosecurity.com

John Cusimano, CISSP, CFSE
Director of Security
exida Consulting LLC
jcusimano@exida.com
www.exida.com

Executive Summary

The past two years have been a wakeup call for the industrial automation industry. It has been the target of sophisticated cyber attacks like Stuxnet, Night Dragon and Duqu. An unprecedented number of security vulnerabilities have been exposed in industrial control products and regulatory agencies are demanding compliance to complex and confusing regulations. Cyber security has quickly become a serious issue for professionals in the process and critical infrastructure industries.

If you are a process control engineer, an IT professional in a company with an automation division, or a business manager responsible for safety or security, you may be wondering how your organization can get moving on more robust cyber security practices. This white paper will give you the information you need to get started. It won't make you a security expert, but it will put you on the right path in far less time than it would take if you were to begin on your own.

We began by condensing the material from numerous industry standards and best practice documents. Then we combined our experience in assessing the security of dozens of industrial control systems. The result is an easy-to-follow 7-step process:

Step 1 – Assess Existing Systems

Step 2 – Document Policies & Procedures

Step 3 – Train Personnel & Contractors

Step 4 – Segment the Control System Network

Step 5 – Control Access to the System

Step 6 – Harden the Components of the System

Step 7 – Monitor & Maintain System Security

The remainder of this white paper will walk through each of these steps, explaining the importance of each step and best practices for implementing it. We will also provide ample references for additional information.

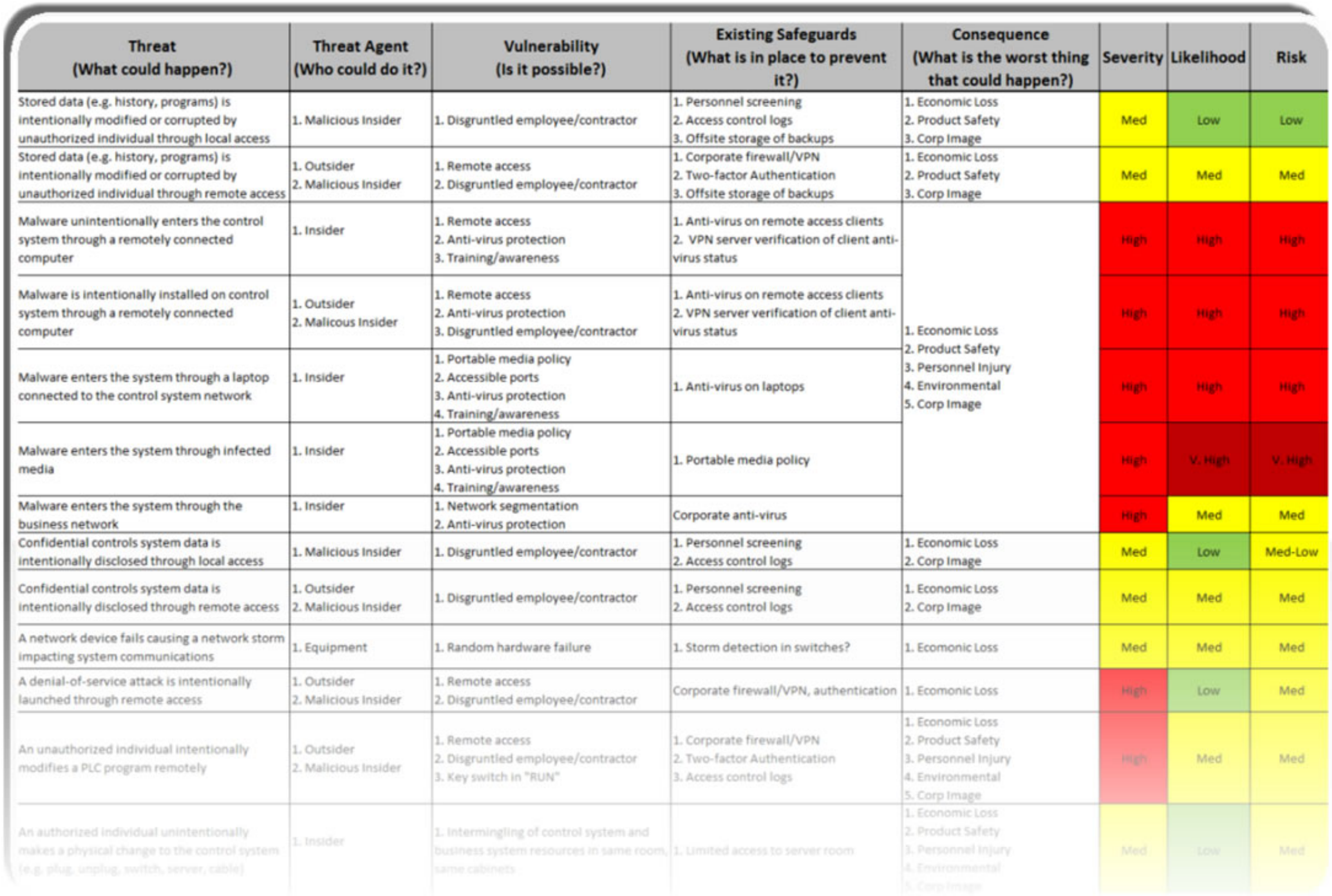
Step 1 – Assess Existing Systems

You wouldn't begin a journey until you know where you are starting from, where you want to go and how you are going to get there.

Planning the journey to secure your control systems is no different. It starts with understanding the risks that control system security (or insecurity) can have on your business. This is known as a *risk assessment* and it is used to quantify the threats that pose a danger to your business. Then you rank these risks so you know how to prioritize your security dollars and efforts.

Only when these two tasks have been completed should you start planning how to apply countermeasures to reduce the risk to tolerable levels. Far too often, we see the assessment step skipped. We have seen companies throw money into a solution for what might be a minor risk, leaving far more serious risks unaddressed. As a responsible professional in your organization, you should be advocating for taking a step back and doing the risk assessment first.

We recommend starting by performing a high-level risk assessment on each of the major control systems in your plant, company or corporation. While this may seem like a daunting task, it can be very manageable if you adopt a simple, lightweight risk assessment methodology. The purpose of such an exercise is to identify the risk of a cyber incident, as a function of likelihood and consequence, and produce a list of control systems ranked by their relative risk.



Threat (What could happen?)	Threat Agent (Who could do it?)	Vulnerability (Is it possible?)	Existing Safeguards (What is in place to prevent it?)	Consequence (What is the worst thing that could happen?)	Severity	Likelihood	Risk
Stored data (e.g. history, programs) is intentionally modified or corrupted by unauthorized individual through local access	1. Malicious Insider	1. Disgruntled employee/contractor	1. Personnel screening 2. Access control logs 3. Offsite storage of backups	1. Economic Loss 2. Product Safety 3. Corp Image	Med	Low	Low
Stored data (e.g. history, programs) is intentionally modified or corrupted by unauthorized individual through remote access	1. Outsider 2. Malicious Insider	1. Remote access 2. Disgruntled employee/contractor	1. Corporate firewall/VPN 2. Two-factor Authentication 3. Offsite storage of backups	1. Economic Loss 2. Product Safety 3. Corp Image	Med	Med	Med
Malware unintentionally enters the control system through a remotely connected computer	1. Insider	1. Remote access 2. Anti-virus protection 3. Training/awareness	1. Anti-virus on remote access clients 2. VPN server verification of client anti-virus status	1. Economic Loss 2. Product Safety 3. Personnel Injury 4. Environmental 5. Corp Image	High	High	High
Malware is intentionally installed on control system through a remotely connected computer	1. Outsider 2. Malicous Insider	1. Remote access 2. Anti-virus protection 3. Disgruntled employee/contractor	1. Anti-virus on remote access clients 2. VPN server verification of client anti-virus status		High	High	High
Malware enters the system through a laptop connected to the control system network	1. Insider	1. Portable media policy 2. Accessible ports 3. Anti-virus protection 4. Training/awareness	1. Anti-virus on laptops		High	High	High
Malware enters the system through infected media	1. Insider	1. Portable media policy 2. Accessible ports 3. Anti-virus protection 4. Training/awareness	1. Portable media policy		High	V. High	V. High
Malware enters the system through the business network	1. Insider	1. Network segmentation 2. Anti-virus protection	Corporate anti-virus		High	Med	Med
Confidential controls system data is intentionally disclosed through local access	1. Malicious Insider	1. Disgruntled employee/contractor	1. Personnel screening 2. Access control logs	1. Economic Loss 2. Corp Image	Med	Low	Med-Low
Confidential controls system data is intentionally disclosed through remote access	1. Outsider 2. Malicious Insider	1. Disgruntled employee/contractor	1. Personnel screening 2. Access control logs	1. Economic Loss 2. Corp Image	Med	Med	Med
A network device fails causing a network storm impacting system communications	1. Equipment	1. Random hardware failure	1. Storm detection in switches?	1. Ecomonic Loss	Med	Med	Med
A denial-of-service attack is intentionally launched through remote access	1. Outsider 2. Malicious Insider	1. Remote access 2. Disgruntled employee/contractor	Corporate firewall/VPN, authentication	1. Ecomonic Loss	High	Low	Med
An unauthorized individual intentionally modifies a PLC program remotely	1. Outsider 2. Malicious Insider	1. Remote access 2. Disgruntled employee/contractor 3. Key switch in "RUN"	1. Corporate firewall/VPN 2. Two-factor Authentication 3. Access control logs	1. Economic Loss 2. Product Safety 3. Personnel Injury 4. Environmental 5. Corp Image	High	Med	Med
An authorized individual unintentionally makes a physical change to the control system (e.g. plug, unplug, switch, server, cable)	1. Insider	1. Intermingling of control system and business system resources in same room, same cabinets	1. Limited access to server room	1. Economic Loss 2. Product Safety 3. Personnel Injury 4. Environmental 5. Corp Image	Med	Low	Med

Figure 1: Example of a High-Level ICS Risk Assessment

If you are responsible for more than one facility, we also recommend selecting one of your "typical" manufacturing facilities and conducting a third-party security assessment on the control systems and security practices in that facility. The purpose of such an assessment is to identify the gaps between current control systems designs, architecture, policies, and procedures and industry best practices. The assessment should also provide recommendations to address the gaps.

The results of this assessment will provide management with a solid understanding of the current situation and a path forward. Most important, it will offer a framework for prioritizing investments in control system security.

While assessments like these can be performed with internal resources, we highly recommend using an experienced third-party with expertise in control system security, for at least the first assessment. A third-party can provide an unbiased review, a recommendation based on their experience, and feedback on how your organization compares with other companies in your industry.

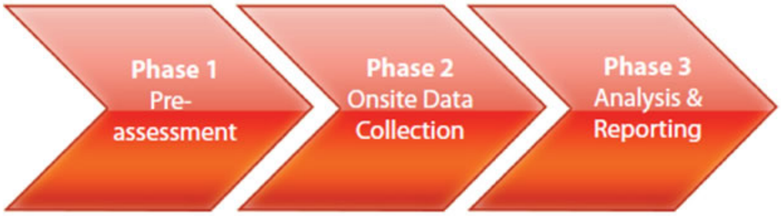


Figure 2: The Phases of a Control System Security Gap Assessment

Detailed vulnerability assessments and penetration testing are an important part of the security lifecycle, but these only make sense after your organization has first performed high-level risk assessments and gap analysis. The results of these earlier steps will help identify high-risk systems or sub-systems that require detailed analysis and testing.

Finally, it is important to understand that penetration testing of your online control system can be extremely risky. We recommend reserving this type of testing for Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT) or during a scheduled shutdown.

Step 2 – Document Policies & Procedures

Once you have a good understanding of the control system security risks facing your business you can then begin to document policies and procedures so that employees, suppliers and contractors understand your company's position on Industrial Control System(ICS) security. Many companies have existing IT security policies and standards. These documents can provide a good foundation for industrial control system-specific documents. However, IT security policies are often not applicable or optimized for the plant floor.

For this reason, we highly recommend organizations develop ICS-specific documents describing company policy, standards and procedures around control system security. These documents can, and should, refer back to the corporate IT security documents. In our experience we have found that separate ICS security documents are very beneficial in aiding those that are responsible for ICS security. It helps them to clearly understand the expectations and responsibilities they have, and how they differ from those of the people responsible for the general office environment.

You should also become familiar with applicable security regulations and standards for your industry. These provide a solid basis for development of company-specific policies, standards and procedures. A good place to start is the ANSI/ISA-99 series of standards, which address the subject of cyber security for industrial automation and control systems. The standards describe the basic concepts and models related to cyber security, as well as the elements contained in a cyber security management system for use in the industrial automation and control systems environment. They also provide guidance on how to meet the requirements described for each element.

The ANSI/ISA-99 standards provide the base documents for the ISO/IEC standards in industrial control security, known as IEC-62443. Over the next few years, these standards are expected to become the core standards for industrial control security worldwide.

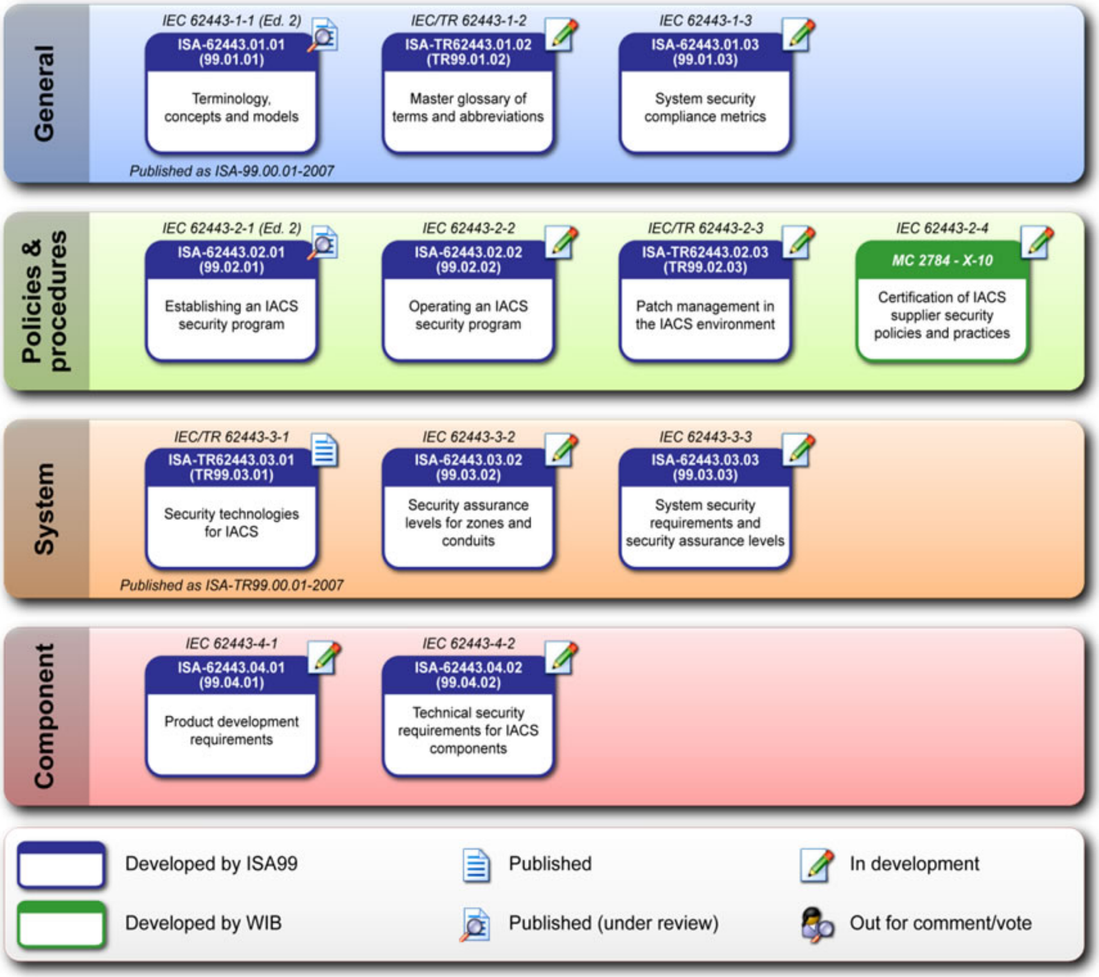

General
IEC 62443-1-1 (Ed. 2)
ISA-62443.01.01 (99.01.01)
Terminology, concepts and models
Published as ISA-99.00.01-2007
IEC/TR 62443-1-2
ISA-TR62443.01.02 (TR99.01.02)
Master glossary of terms and abbreviations
IEC 62443-1-3
ISA-62443.01.03 (99.01.03)
System security compliance metrics
Policies & procedures
IEC 62443-2-1 (Ed. 2)
ISA-62443.02.01 (99.02.01)
Establishing an IACS security program
IEC 62443-2-2
ISA-62443.02.02 (99.02.02)
Operating an IACS security program
IEC/TR 62443-2-3
ISA-TR62443.02.03 (TR99.02.03)
Patch management in the IACS environment
IEC 62443-2-4
MC 2784 - X-10
Certification of IACS supplier security policies and practices
System
IEC/TR 62443-3-1
ISA-TR62443.03.01 (TR99.03.01)
Security technologies for IACS
Published as ISA-TR99.00.01-2007
IEC 62443-3-2
ISA-62443.03.02 (99.03.02)
Security assurance levels for zones and conduits
IEC 62443-3-3
ISA-62443.03.03 (99.03.03)
System security requirements and security assurance levels
Component
IEC 62443-4-1
ISA-62443.04.01 (99.04.01)
Product development requirements
IEC 62443-4-2
ISA-62443.04.02 (99.04.02)
Technical security requirements for IACS components
Developed by ISA99
Developed by WIB
Published
Published (under review)
In development
Out for comment/vote

Figure 3: The Structure of the IEC 62443 Series of Standards

Depending on the industry you're in, you should also become familiar with industry-specific guidance which is available from organizations such as the American Petroleum Institute (API), the American Chemistry Council (ACC), and the North American Electric Reliability Corporation (NERC). You should also familiarize yourself with relevant regulatory requirements that may apply to your industry such as the Chemical Facility Anti-terrorism Standards (CFATS) from the U.S. Department of Homeland Security.

While every organization will prepare policy documents differently, there are basic principles and core content that should always be included. This includes a clear definition of scope, and identification of the portions of the organization and the types of systems covered by the policy. There should be a clear indication of senior management support for the policy. Finally, it should be clear to the reader:

- How this policy applies to their particular role in the organization
- The responsibilities they have in complying with the policies and
- The consequences for not complying.

Some specific topics that need to be addressed in an ICS security policy are:

- Remote access

- Portable media
- Patch management
- Anti-virus management
- Change management
- Backup and restore
- Incident response

Step 3 – Train Personnel & Contractors

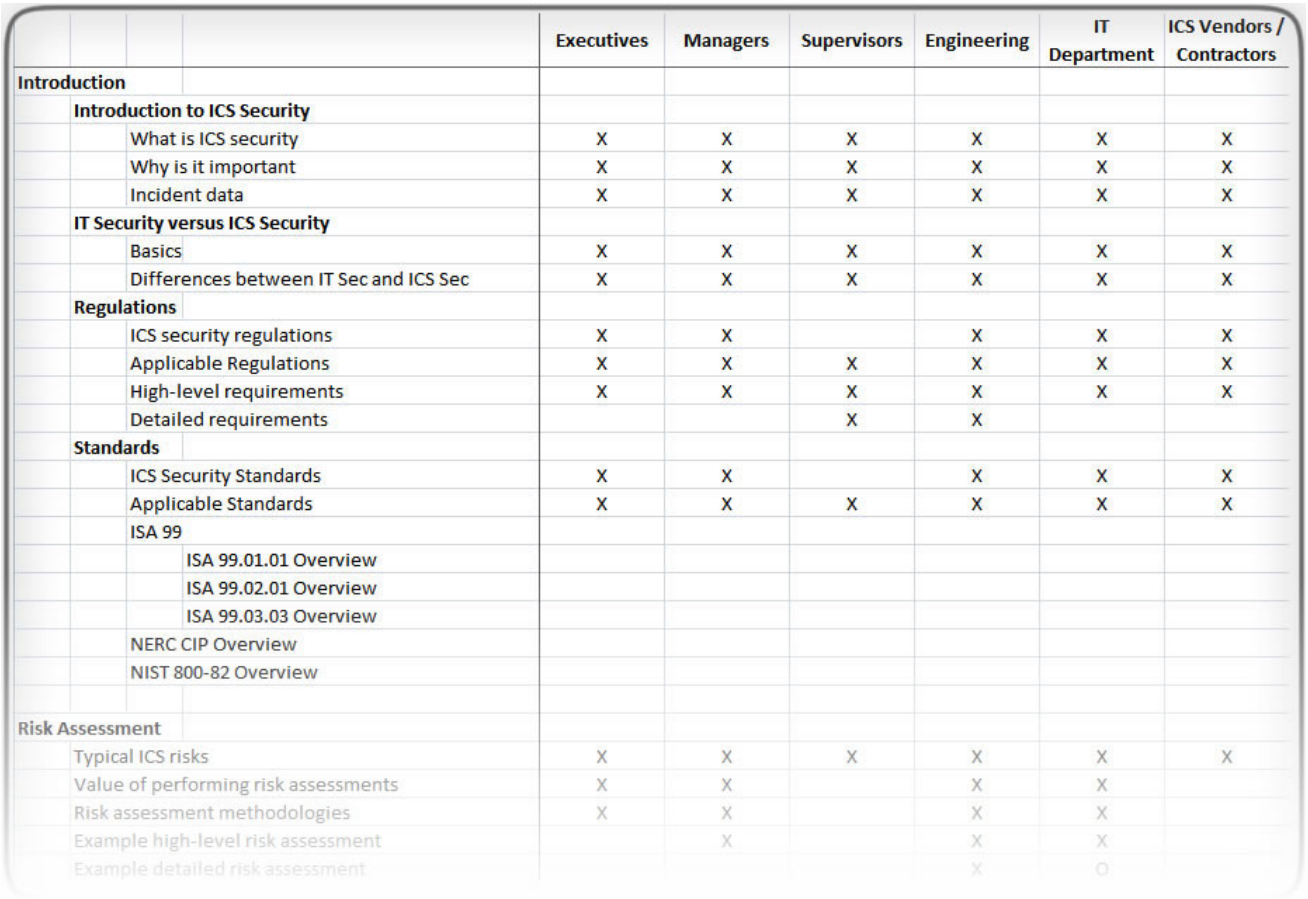
Once your organization has developed and documented its ICS security policies, standards and procedures, it is critical to make sure that personnel are aware of the existence and importance of these materials. There are two parts to such a program.

The first is to conduct an awareness program. An awareness program focuses on ensuring that personnel throughout your organization are aware of company policies, standards and best practices. To be successful, the awareness program should be communicated by senior management to all applicable employees. It should then be followed up with regular communications to continually remind people of the program.

The second is a training program that provides personnel with job-relevant information on how to apply security and what to do if they suspect there is a security breach. This training cannot be a “onesize fits all” program. Different personnel have different responsibilities and this will need to be represented in the training program. We highly recommend developing a role-based training program for control system security.

Designing a role-based training program starts with identifying the major job roles in your company. Next, the training needs are identified for each role. For example, you may identify the following main roles in your organization; visitors, contractors, operations, maintenance, engineering, management, executives, etc.

Visitor training might focus on defining allowed and prohibited activities while on site, while engineering training might focus on the secure configuration and use of key network assets. Management training might focus on how to respond when an employee reports a possible security breach. To help sort this out, we recommend developing a training matrix which lists the training topics on one axis and the roles on another.



	Executives	Managers	Supervisors	Engineering	IT Department	ICS Vendors / Contractors
Introduction						
Introduction to ICS Security						
What is ICS security	X	X	X	X	X	X
Why is it important	X	X	X	X	X	X
Incident data	X	X	X	X	X	X
IT Security versus ICS Security						
Basics	X	X	X	X	X	X
Differences between IT Sec and ICS Sec	X	X	X	X	X	X
Regulations						
ICS security regulations	X	X		X	X	X
Applicable Regulations	X	X	X	X	X	X
High-level requirements	X	X	X	X	X	X
Detailed requirements			X	X		
Standards						
ICS Security Standards	X	X		X	X	X
Applicable Standards	X	X	X	X	X	X
ISA 99						
ISA 99.01.01 Overview						
ISA 99.02.01 Overview						
ISA 99.03.03 Overview						
NERC CIP Overview						
NIST 800-82 Overview						
Risk Assessment						
Typical ICS risks	X	X	X	X	X	X
Value of performing risk assessments	X	X		X	X	
Risk assessment methodologies	X	X		X	X	
Example high-level risk assessment		X		X	X	
Example detailed risk assessment				X	O	

Figure 4: Example Training Matrix

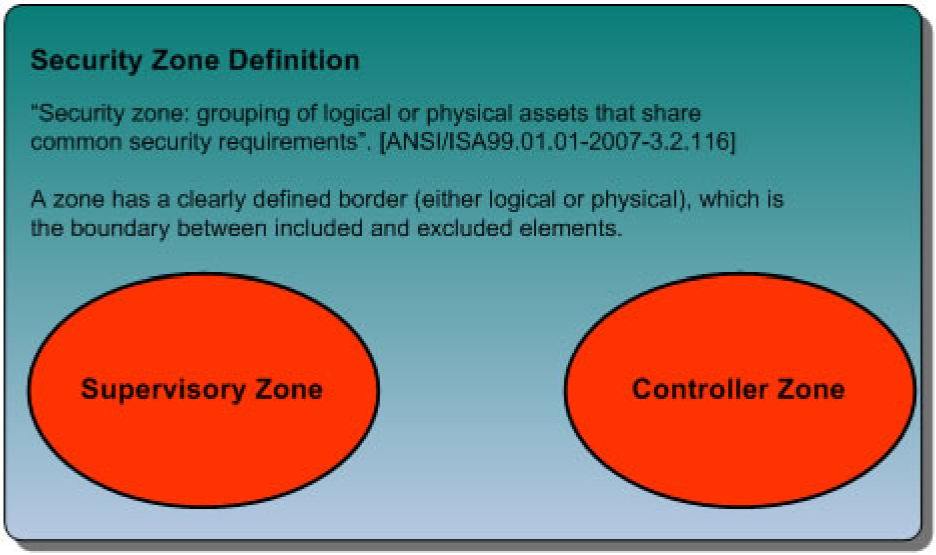
Once the matrix has been developed the training content can be designed. We find a modular approach in developing the course materials is ideal; this allows materials to be easily combined and customized for particular roles. Many organizations are using computer-based training very effectively, particularly for high-level training. Regardless of your approach, it is important to keep records of who has attended the training and to include knowledge assessments in order to ensure the information was properly understood.

Step 4 – Segment the Control System Network

Arguably the most important tactical step that can be taken to improve the security of your industrial automation system is network segmentation. The concept of network segmentation is to partition the system into distinct security zones and implement layers of protection to isolate the most critical parts of the system.

Analogous to physical security controls, such as those found in an airport, a network can be segmented into various network security zones. The most critical assets should be placed in higher security zones. As in an airport, a user wishing to access a critical asset may have to pass through several gates or screening points.

ANSI/ISA-99 introduces the concepts of "**zones**" and "**conduits**" as a way to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken.



Security Zone Definition

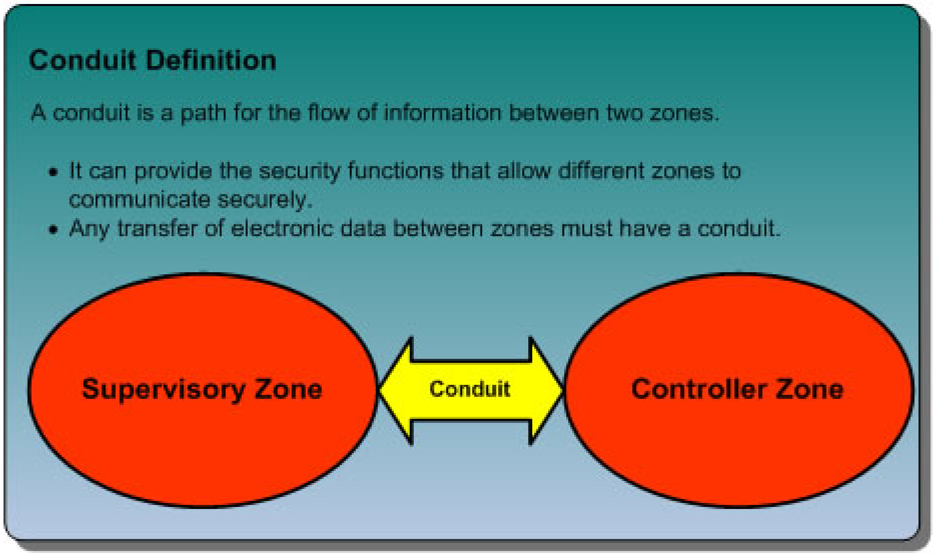
"Security zone: grouping of logical or physical assets that share common security requirements". [ANSI/ISA99.01.01-2007-3.2.116]

A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.

Figure 5: Security Zone Definition, from ANSI/ISA-99

Any communications between Zones must be conducted via a defined Conduit. Conduits control access to Zones, resist Denial of Service (DoS) attacks or the transfer of malware, shield other network systems and protect the integrity and confidentiality of network traffic.

Typically the controls on a conduit are intended to mitigate the difference between a zone's security level capability and its security requirements. Focusing on conduit mitigations is typically far more cost effective than having to upgrade every device or computer in a zone to meet a requirement.



Conduit Definition

A conduit is a path for the flow of information between two zones.

- It can provide the security functions that allow different zones to communicate securely.
- Any transfer of electronic data between zones must have a conduit.

Figure 6: Conduit Definition, from ANSI/ISA-99

Zone and conduit design starts with the facility being analyzed to identify groups of devices that have common functionality and common security requirements; these groups are the “zones” of equipment that require protection. For example, a facility might first be divided into operational areas, such as materials storage, processing, finishing, etc. Then within these areas it could be further divided into functional layers, such as Manufacturing Execution Systems (MES), Supervisory Systems (i.e. operator HMIs), primary control systems (i.e. PLCs) and safety systems. Often the models from other standards such as ANSI/ISA-95.00.01-2000 or the Purdue manufacturing model are used as a basis for this division. Vendor design documents can also be helpful.

The next step is to discover the pathways in the network through which data is passed between these zones; these are the network “conduits”. Each conduit should be defined in terms of the zones it connects, the technologies it utilizes, the protocols it transports and any security features it needs to offer its connected zones.

Typically, determining the information transfer requirements between zones over the network is straight forward. Tools like traffic flow analyzers or even simple protocol analyzers can show which systems are exchanging data and the services they are using.

It is also wise to look beyond the network to determine the hidden traffic flows. For example, are files ever moved via USB drive between the lab and the primary control systems? Do people remotely connect to the RTUs using a dial-up modem? These flows are easy to miss, but can result in serious security issues if not managed carefully.

Once the conduits and their security requirements are defined, the final phase is to implement the appropriate security technologies. Firewalls and Virtual Private Networks (VPNs) are two popular options for this stage. Industrial firewalls can be installed in these conduits and configured to pass only the minimum traffic that is required for correct plant operation, blocking all other unnecessary traffic. The firewalls should implement an alarm-reporting mechanism to alert operations or security personnel any time that abnormal behavior (i.e. – blocked traffic) is observed in the network.

Combined, the entire zone and conduit approach implements a strategy of “*defense in depth*” – multiple layers of defense distributed throughout the control network. It is a strategy that has been proven in the military, financial and IT communities as the best way to obtain the most effective security at the lowest overall cost.

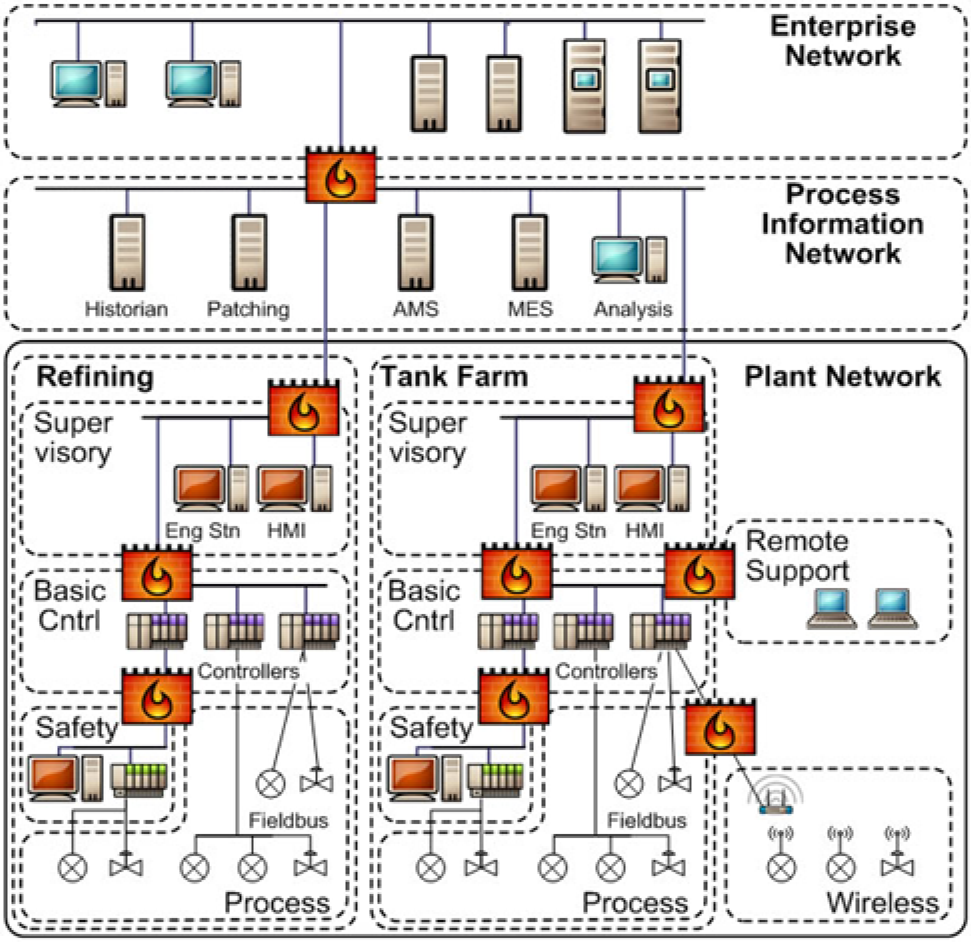


Figure 7: High Level Network Diagram of a Refinery Showing Zones (dotted lines) and Conduits (shown in orange)

Most manufacturers of integrated control system platforms such as DCS systems or PLC systems have defined reference architectures they recommend for good network segmentation with their systems. These can be useful when analyzing the systems in your plant that are based on these manufacturer's systems. However, it is important to bear in mind that each application and system is unique and that reference architectures are only meant to provide general guidance.

Step 5 – Control Access to the System

Once you've partitioned your system into security zones the next step is to control access to the assets within those zones. It is important to provide both physical and logical access controls.

Physical access controls are generally straightforward and easily understood. Typical physical access controls are fences, locked doors, and locked equipment cabinets. The concept is to limit physical access to critical ICS assets to only those who require access to perform their job. For example, the control system in a typical refinery would be protected by multiple layers of physical access - starting with the fence around the refinery, then with locked doors on the building housing the control system, then with additional locked doors for the control room and equipment rooms, and finally locked enclosures for the actual control system equipment.

Ideally, the same concepts should apply to logical access to critical control system resources. Unfortunately, too often users can remotely access critical control resources by passing through only one simple layer of authentication.

Like physical access control, logical access control starts by identifying who should have access to what resources with what privileges and how that should be enforced. Users need to be identified and authenticated to verify they are who they say they are. Once authenticated, users can be authorized to perform certain functions. Often this is determined by the role of the user.

The concept of least privilege is also important, meaning that a user is only authorized to perform the functions necessary to perform their job. Another important concept is accountability, which involves logging the actions of individual users so they can be held accountable for their actions.

Fortunately, there are many tools available to assist the control system administrator in managing logical access control, such as Active Directory. However, we often see this technology misapplied. Much of what it takes to properly apply this technology is good planning; identifying users, roles, and assigning the users to those roles is a key first step which is often skipped and or developed “on the fly”.

Step 6 – Harden the Components of the System

Hardening the components of your system means locking down the functionality of the various components in your system to prevent unauthorized access or changes, remove unnecessary functions or features, and patch any known vulnerabilities. This is especially important in modern control systems which utilize extensive commercial off-the-shelf technology. In such systems, it is critical to disable unused functions and to ensure that configurable options are set to their most secure settings.

For example, a lot can be done to harden a Windows server or workstation. There are often many unnecessary applications such as games or music players included in the default installation. These should be removed from the computer when installed as part of a control system. It is also important to disable or block unnecessary communication interfaces and the services available on these interfaces. For example, many PLCs come with web servers running on them – unless web access to a PLC is a core part of the operations, it should be turned off.

Once the computers and controllers are deployed, additional steps are necessary to maintain the security. This includes maintaining anti-virus signatures and applying security patches. It is important to remember that patches are needed for applications as well as the operating system – a common attack vector today is to exploit unpatched Acrobat Reader software running on ICS workstations.

Used properly, vulnerability scanning tools such as Nessus, along with special audit files such as Bandolier, can be very helpful in identifying the presence of known vulnerabilities. They can also verify that servers and workstations have been properly configured for security. However, as we noted earlier, live testing of a production control system can be very risky. We recommend using these tools at FAT, SAT or when production is shutdown, such as during a maintenance turnaround.

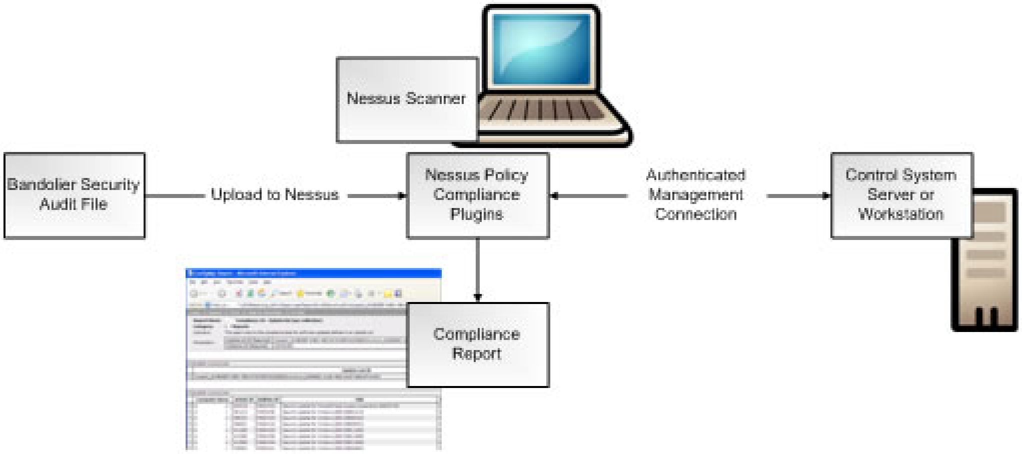

Nessus Scanner
Bandolier Security Audit File
Upload to Nessus
Nessus Policy Compliance Plugins
Authenticated Management Connection
Control System Server or Workstation
Compliance Report

Figure 8: Bandolier and Nessus Policy Compliance Process

Servers and workstations are not the only components of a control system that require hardening. Network equipment and embedded control products also require secure configurations, blocking of unused communication interfaces, and software maintenance.

We recommend working with the manufacturers of ICS components to obtain their recommendations for hardening. Many of the vendors have created useful guidelines on what works from a security point of view and will not impact their systems. This information should be documented in a security manual provided as part of the manufacturer's security certification.

Step 7 – Monitor & Maintain System Security

As an owner or operator of an industrial control system, you must remain vigilant by monitoring and maintaining security throughout the lifecycle of your system. This involves numerous activities, such as updating antivirus signatures and installing security patches on Windows servers. It also involves monitoring your system for suspicious activity.

This can take many forms, such as reviewing system logs for unauthorized or unusual activity. It can also involve technology such as Intrusion Detection Systems (IDS) that can detect malicious or suspicious network activity.

IDS technology is generally not considered to be mature enough to be deployed on control systems in a manner that would allow it to block traffic (i.e. act as an intrusion prevention system). However, the technology can be used today as part of an overall defense-in-depth strategy to, for example, validate security measures, including firewall rules.

Finally, it is important to periodically test and assess your system. Assessments involve periodic audits to verify the system is still configured for optimal security as well as updating security controls to the latest standards and best practices. More aggressive or invasive practices such as penetration testing can be performed on systems during shutdowns or turnarounds.

Summary

In Step 1 of this paper we suggested that you should not begin a journey until you know where you are starting from, where you want to go and how you are going to get there. We hope that the 7 steps described provide you with a roadmap to improve your plant's cyber security defenses.

After you complete them, however, you have really only completed the first leg of your journey.

Effective ICS and SCADA security is not a one-time project. Rather it is an ongoing, iterative process. You will need to repeat the 7 steps and update materials and measures as systems, people, business objectives and threats change.

The reward for your effort will be maximum protection against process disruption, safety incidents and business losses from modern cyber security threats.

References

General

- "ANSI/ISA-99 Standards." tofinosecurity.com, Feb. 14, 2012. <http://www.tofinosecurity.com/why/ansi-isa-99>.

- "NERC CIP Compliance." tofinosecurity.com, Feb. 14, 2012. <http://www.tofinosecurity.com/why/nerc-cip-standards-compliance>.

- Cusimano, John A. "The 7 Things Every Plant Manager Should Know About Control System Security." Functional Safety, Security, & Reliability | exida.com, Feb. 24, 2011. <http://www.exida.com/index.php/webinars/recordings/>.

- IEC 62443-2-1 ED. 1.0 EN:2010, "Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program", 2010. <http://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf>.

- ANSI/ISA 99.02.01-2009, "Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program", 2009. <http://www.isa.org/Template.cfm?Section=standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10243>.

- IEC/TS 62443-1-1 ED. 1.0 EN:2009, "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models", 2009. <http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/43215>.

- ANSI/ISA 99.00.01-2007, "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models", 2007. <http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9661>.

- Byres, Eric J. "Building Intrinsically Secure Control and Safety Systems Using ANSI/ISA99 Security Standards for Improved Security and Reliability." tofinosecurity.com, May, 2009. <http://www.tofinosecurity.com/sites/default/files/ANSI_ISA-99%20and%20Intrinsically%20Secure%20Systems%20%28May%202009%29.pdf>.

References for Step 1 – Assess Existing Systems

- ISA Automation Week presentation by John Cusimano: "Assessing the Security of ICS Systems Using Threat Modeling", Nov 4, 2011. < http://automation.isa.org/2011/11/assessing-the-security-of-ics-systems-using-threat-modeling/>.

- American Chemistry Council, Chemical Information Technology Center (ChemITC), "Report on Cyber Security Vulnerability Assessment Methodologies", Version 2.0, Nov. 2004.

- Repository of Industrial Security Incidents, Security Incidents Organization. <http://www.securityincidents.org>.

References for Step 2 – Document Policies and Procedures

- NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security", Jun. 2011. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>.

- American Petroleum Institute, API STD 1164, “Pipeline SCADA Security”, Second Edition, Jun. 2009. <http://www.securitrus.com/documents/GasandOilIndustries1164_e2_PA.pdf>.
- U.S. Dept. of Homeland Security, “Risk-based Performance Standards Guidance Chemical Facility Anti-terrorism Standards”, 2008. < http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf>.
- NERC, Reliability Standards, Critical Infrastructure Protection (CIP), <http://www.nerc.com/page.php?cid=2|20>.

References for Step 3 – Train Personnel & Contractors

- U.S. Dept. of Homeland Security, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies”, Oct. 2009. < http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf>.

References for Step 4 – Segment the Control System Network

- NISCC, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Feb. 2005. <http://www.cpni.gov.uk/docs/re-20050223-00157.pdf>.
- Practical SCADA Security: “Controlling Stuxnet – No More Flat Networks PLEASE. Let's Embrace Security Zones". tofinosecurity.com, Nov. 4, 2010 <http://www.tofinosecurity.com/blog/controlling-stuxnet-%E2%80%93-no-more-flat-networks-please-lets-embrace-security-zones>.

References for Step 5 – Control Access to the System

- NIST SP 800-82, “Guide to Industrial Control Systems (ICS) Security”, Jun. 2011. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>.

References for Step 6 – Harden the Components of the System

- "Bandolier", Digitalbond.com, Feb. 14, 2012. <http://www.digitalbond.com/tools/bandolier/>.
- ISA Secure | Home, isasecure.org, Feb. 14, 2012. <http://www.isasecure.org>.
- U.S. Dept. of Homeland Security, “Recommended Practice for Patch Management of Control Systems”, Dec. 2008. <http://www.uscert.gov/control_systems/practices/documents/PatchManagementRecommendedPractice_Final.pdf>.

References for Step 7 – Monitor & Maintain System Security

- U.S. Dept. of Homeland Security, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies”, Oct. 2009. < http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf>.

Source Material

The material for this White Paper was adapted from

- The exida training course: 7 Steps to Industrial Control System Security. <http://www.exida.com/index.php/training/onsite/>.
- and these Practical SCADA Security blog articles:
  - Getting Started on ICS and SCADA Security Part 1 of 2, Aug. 10, 2011. <http://www.tofinosecurity.com/blog/getting-started-ics-and-scada-security-part-1-2>.
  - Getting Started on ICS and SCADA Security Part 2 of 2, Aug. 17, 2011. <http://www.tofinosecurity.com/blog/getting-started-ics-and-scada-security-part-2-2>.

About Tofino Security

Tofino® Security provides practical and effective industrial network security and SCADA security products that are simple to implement and that do not require plant shutdowns.

Its flagship product, the Tofino™ Industrial Security Solution, combines security appliances with loadable software modules to protect industrial networks from external cyber threats and internal network incidents. *Tofino* is used by the process control, SCADA, manufacturing and automation industries.

www.tofinosecurity.com, www.belden.com

About exida

exida is a world leading engineering services & certification body focused on helping automation suppliers and users improve the safety, security and reliability of their industrial automation systems. Established by several of the world’s top safety, security, and reliability experts, the company is owned by these partners and independent of any vendor ownership. exida’s main offices are located in Sellersville, PA, USA and Munich, Germany with service centers worldwide.

www.exida.com