Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response Team

September 2016

Homeland Security

ACKNOWLEDGMENTS

The Department of Homeland Security (DHS)'s National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) developed this publication in cooperation in an ongoing effort to reduce risks within and across all critical infrastructure sectors and to share common control systems-related security mitigation recommendations. NCCIC wishes to acknowledge and thank the senior leaders from DHS and the Department of Energy whose industrial control systems cybersecurity specialists' dedicated efforts contributed significantly to the publication of this document.

The DHS ICS-CERT program expresses thanks to and acknowledges the contributions of Mark Fabro, Ed Gorski, and Nancy Spiers in development of this report. A special note of thanks goes to John Diedrich and David Kuipers of the Idaho National Laboratory, working under DHS's NCCIC/ICS-CERT program, for their contributions in helping to improve the content of the publication. DHS ICS-CERT also gratefully acknowledges and appreciates the significant contributions from individuals, working groups, and organizations in the public and private sectors, both nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third-party's use, or the results of such use, or any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

EXECUTIVE SUMMARY

Industrial control systems (ICSs) are an integral part of critical infrastructures, helping to facilitate operations in vital industries such as electricity, oil and gas, water, transportation, manufacturing, and chemical manufacturing. The growing issue of cybersecurity and its impact on ICS highlights fundamental risks to the Nation's critical infrastructure. Efficiently addressing ICS cybersecurity issues requires a clear understanding of the current security challenges and specific defensive countermeasures. A holistic approach—one that uses specific countermeasures implemented in layers to create an aggregated, risk-based security posture—helps to defend against cybersecurity threats and vulnerabilities that could affect these systems. This approach, often referred to as Defense in Depth, provides a flexible and useable framework for improving cybersecurity protection when applied to control systems.

The concept of Defense in Depth is not new—many organizations already employ many of the Defense-in-Depth measures discussed in this document within their information technology (IT) infrastructures; however, they do not necessarily apply it to their ICS operations. In the past, most organizations did not see a need to do so. Legacy ICSs used obscure protocols and were largely considered "hack proof" because of their separation from IT and because of having physical protection measures in place. But with the convergence of IT and ICS architectures, recent high-profile intrusions have highlighted the potential risk to control systems.

The last five years have brought a marked increase in concern regarding the potential for cyber-based attacks on critical infrastructures, and the number of cyber-based incidents across critical infrastructure sectors that asset owners reported to ICS-CERT has risen. In response, both government agencies and sector-specific regulatory authorities have issued cybersecurity guidance and imposed sanctions for noncompliance.

The threat of an intrusion by malicious actors on critical infrastructure using computer-based exploits has also grown. A number of recent high-profile incidents have increased awareness of this threat and the individuals and groups who pursue it with malicious intent. The availability of ICS-specific security solutions has not kept up with the mounting threat, so organizations must deploy a robust Defense-in-Depth solution—making their systems unattractive targets to would-be attackers.

This recommended practice document provides guidance for developing mitigation strategies for specific cyber threats and direction on how to create a Defense-in-Depth security program for control system environments. The document presents this information in four parts: 1) "Background and Overview" outlines the current state of ICS cybersecurity and provides an overview of what defense in depth means in a control system context; 2) "ICS Defense-in-Depth Strategies" provides strategies for securing control system environments; 3) "Security Attacks" outlines how threat actors could carry out attacks against critical infrastructures and the potential impact to ICSs and networks; and 4)"Recommendations for Securing ICS" provides resources for securing ICSs based on the current state-of-the-art methods and lessons learned from ICS-CERT activities, national and sector-specific standards for ICS security, and tools and services available through ICS-CERT and others that can be used to improve the security posture of ICS environments.

This version modernizes and improves the flagship document issued in 2009, reflecting the evolution of control systems management, security practices, and change management within the ICS community, as well as addressing emerging threats to critical infrastructure. It is a living document that provides an aggregated compendium of the current state of ICS security practices.

KEY WORDS

Cybersecurity, data diodes, Defense in Depth, demilitarized zones (DMZ), distributed control system (DCS), encryption, firewall, industrial control system (ICS), intrusion detection system (IDS), intelligent electronic device (IED), intrusion prevention system (IPS), patch management, policy and procedures, process control, programmable logic controller (PLC), security zones, supervisory control and data acquisition (SCADA).

CONTENTS

ACKNOWLEDGMENTS II

EXECUTIVE SUMMARY III

KEY WORDS V

ACRONYMS VIII

1.BACKGROUND AND OVERVIEW 1

1.1 ICS Communications Technology Migration 1

2.ICS DEFENSE-IN-DEPTH STRATEGIES 2

2.1 Risk Management and ICS 6

2.2 Asset Inventory and Risk Characterization 9

2.3 Physical Security 13

2.4 ICS Network Architectures 16

2.5 Security Architectures 22

2.6 Host Security 26

2.7 Security Monitoring 27

2.8 Vendor Management and Security 31

2.9 The Human Element 33

3.SECURITY ATTACKS 35

3.1 Anatomy of a Cyber Attack 35

3.2 Discovery 36

3.3 ICS Attack Methods 38

4.RECOMMENDATIONS FOR SECURING ICS 43

4.1 Proactive Security Model 43

4.2 Five Key Security Countermeasures for Industrial Control Systems 44

4.3 Security and Risk Standards 44

4.4 Tools and Services for ICS Defense in Depth 46

5.CONCLUSION 48

FIGURES

Figure 1. Defense-in-Depth planning. 3

Figure 2. Risk management tiers. 7

Figure 3. Risk Management Approach. 8

Figure 4. Simple qualitative risk analysis chart. 11

Figure 5. Recommended secure network architecture. 17

Figure 6. Zone segmentation of business & ICS architecture. 18

Figure 7. ICS irewall rule set layers. 24

Figure 8. IDS/IPS limitations. 28

Figure 9. Attack sequence of operations. 35

Figure 10. Man-in-the-Middle attack. 41

Figure 11. Proactive security as an iterative process. 43

Figure 12. CSET Assessment High-Level Process. 46

TABLES

Table 1. An organization's security functions. 4

Table 2. Defense-in-Depth strategy elements. 6

Table 3. Signature versus anomaly-based detection 29

Table 4. Detection basis considerations. 30

ACRONYMS

ACL	access control list
ALDS	application level detection system
API	application programming interface
ARP	Address Resolution Protocol
AWWA	American Water Works Association
CD	compact disk
CIP	Critical Infrastructure Protection
CISSP	Certified Information Systems Security Professional
DAR	Design Architecture Review
DCOM	distributed component object model
DHS	U.S. Department of Homeland Security
DMZ	demilitarized zone
DOE	Department of Energy
DTP	Dynamic Trunking Protocol
FTP	File Transfer Protocol
HIDS	Host-based intrusion detection system
HMI	human-machine interface
HVAC	Heating, Ventilation, and Air Conditioning
ICS	industrial control system
ICT	Information and Communications Technology
IDS	intrusion detection systems
IED	intelligent electronic device
IP	Internet Protocol
IPS	intrusion prevention systems
ISP	Internet service provider
ISSAP	Information Systems Security Architecture Professional
IT	information technology
LAN	local area network
MAC	media access control
MitM	Man-in-the-Middle

NAVV	Network Architecture Validation and Verification
NERC	North American Electric Reliability Corporation
NIC	network interface card
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OLE	object linking and embedding
OPC	OLE for process control
OS	operating system
OSI	open systems interconnection
OT	operational technology
PCS	process control system
PIN	personal identification number
PLC	programmable logic controller
RMP	Risk Management Process
RoE	rules of engagement
RPC	remote procedure call
SCADA	Supervisory Control and Data Acquisition
SIEM	security information and event management
SIS	safety-instrumented systems
SLA	service level agreement
SP	Special Publication
SSH	secure shell
SQL	structured query language
TCP	Transmission Control Protocol
TSA	Transportation Safety Administration
UPS	uninterruptible power supply
USB	universal serial bus
VLAN	virtual LAN
VM	virtual machine
VoIP	Voice over Internet Protocol
VPN	virtual private network

1. BACKGROUND AND OVERVIEW

Information infrastructures across many public and private industrial control system (ICS) domains share several common attributes regarding information technology (IT) deployments and data communications. An increasing number of organizations are using networking technologies to enhance productivity and reduce costs by increasing the integration of external, business, and control system networks. However, these integration strategies often expose mission-critical ICS to cyber threats through exploitation of existing vulnerabilities in the connected networks, thus reducing the organization's overall cybersecurity posture. This recommended practice document provides guidance for developing Defense in Depth strategies for organizations that use control system networks while maintaining multitier information architectures that include critical ICS.

1.1 ICS Communications Technology Migration

The operational technologies that support critical infrastructure industries, such as manufacturing, transportation, and energy, depend heavily on information systems for their monitoring and control. Physical separation between corporate and control domains has, traditionally, provided the primary means of protecting ICS; however, this division offers very limited means for data sharing, data acquisition, peer-to-peer data exchange, or other business operations. In addition to physical separation, the technical security of any given system within the control system domain relied on the fact that few, if any, understood the intricate architecture or the operational mechanics of the resources on the control system local area network (LAN). This "security through obscurity" concept generally worked well for environments that had no external communication connections, thus allowing an organization to focus on physical security. Modern control system architectures, business requirements, and cost control measures result in increasing integration of corporate and ICS IT architectures. Physical separation alone no longer provides a viable business option for managing, utilizing, or securing ICS.

> ***"Essentially, security by obscurity relies on the fact that a given vulnerability is hidden or secret as a security measure. Of course, if anyone or anything accidentally discovers the vulnerability, no real protection exists to prevent exploitation."***
>
> ***–Tony Bradley[1], Certified Information Systems Security Professional (CISSP), Information Systems Security Architecture Professional (ISSAP)***

While a high dependence on legacy ICS technology still exists, many critical infrastructure system asset owners are migrating to interconnected technologies. As a result, common communications protocols and open architecture standards are replacing the diverse and disparate proprietary mechanics for ICS. This replacement can have both positive and negative impacts.

On the positive side, the migration empowers asset owners to access new and more efficient methods of communication as well as more robust data collection and aggregation methods, quicker time to market, and interoperability. On the negative side, integration of control system architectures with contemporary IT-based computing and networking capabilities can introduce risks that did not previously exist with an isolated ICS. Enterprise IT protocols, communication standards, and networking technologies may provide increased interoperability in the ICS environment; however, in many cases, the migration could also increase risk exposure of the ICS through the application of the same technologies that threat actors have already exploited and compromised on the Internet and corporate networking domains. Further, common countermeasures implemented in enterprise networks to mitigate risk associated with these technologies often do not work in ICS environments. An increasing number of ICS-focused incidents have illustrated the interdependence of ICS such as those in the public utility sector.

1. Tony Bradley is Editor-in-Chief of TechSpective.net, http://bradleystrategygroup.com

2. ICS DEFENSE-IN-DEPTH STRATEGIES

An organization's cybersecurity strategy should protect the assets that it deems critical to successful operation. Unfortunately, there are no shortcuts, simple solutions, or "silver bullet" implementations to solve cybersecurity vulnerabilities within critical infrastructure ICS. It requires a layered approach known as Defense in Depth.

Defense in Depth as a concept originated in military strategy to provide barriers to impede the progress of intruders from attaining their goals while monitoring their progress and developing and implementing responses to the incident in order to repel them. In the cybersecurity paradigm, Defense in Depth correlates to detective and protective measures designed to impede the progress of a cyber intruder while enabling an organization to detect and respond to the intrusion with the goal of reducing and mitigating the consequences of a breach.

Defense in Depth is not a one-to-one exercise, where an organization deploys specific technologies to counter an equivalent risk. Defense in Depth employs a holistic approach to protect all assets, while taking into consideration its interconnections and dependencies, and using an organization's available resources to provide effective layers of monitoring and protection based on the business's exposure to cybersecurity risks.

In order to apply Defense in Depth to ICS environments, an organization must understand the relationship of intruders (threats) and vulnerabilities to the controls (standards and countermeasures) put in place to protect the operations, personnel, and technologies that make up an ICS.

A threat-actor, through intent, capability, and/or opportunity, poses a threat to an ICS by compromising an organization's systems through its operations, personnel, and/or technology and exploiting an existing weakness or vulnerability. Security countermeasures, based on best practices and standards, protect ICS critical assets through multiple layers of defense—thereby improving protection for operations, personnel, and technology. Organizations must constantly adjust and refine security countermeasures to ensure protection against known and emerging threats (see Figure 1).

Figure 1. Defense-in-Depth planning.

Because of the complexity of ICS architectures, potential vulnerabilities and/or exploits that introduce new and evolving categories of threats to the ICS environment can have lasting consequences, and without a layered, multitier strategy could result in long-term exposure without detection. The following intrusion methods could enable an advanced persistent threat that lies within the system undetected for long periods of time:

- Attacks directly from Internet to Internet-connected ICS devices.
  - Establish direct access deep into the ICS systems.
- Attacks initiated using remote access credentials stolen or hijacked from authorized ICS organization users.
  - Establish direct access deep into the ICS systems.
- Attacks on the external business web interface.
  - Leverage exploits to vulnerabilities existing in the web services.
  - Pivot into the ICS historian that provides ICS data to the web server applications.
- Attacks initiated by insertion of infected mobile media into a system component.
  - Pivot deeper into the ICS network systems as threat actors find opportunity.
- Threat actors use phishing email to establish a presence on enterprise user desktop or business computers.
  - Pivot deeper into the ICS network systems as threat actors find opportunity.

When applying Defense-in-Depth protection to ICS, one should note that several key differences exist between traditional IT environments and control system environments concerning security. Table 1 shows some of the more prominent security topics common to an organization's security function and outlines how to address them in IT domains as opposed to architectures that run ICS.

Table 1. An organization's security functions.

Security Topic	Information Technology (IT)	Control Systems (ICS)
Anti-virus and Mobile Code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based	Memory requirements can impact on ICS; organizations can only protect legacy systems with after-market solutions; usually requires "exclusion" folders to avoid programs quarantining critical files
Patch Management	Easily defined; enterprise-wide; remote and automated	Long timeline to successful patch installation; OEM-specific; may "break" ICS functionality; asset owners required to define acceptable risk
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; usually same vendor over time; product end-of-life creates new security concerns
Testing and Audit Methods	Use modern methods; systems usually resilient and robust to handle assessment methods	Tune testing to the system; modern methods can be inappropriate; equipment may be susceptible to failure during testing
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact on production
Asset Classification	Common and performed annually; results drive expenditure	Only performed when obligated; accurate inventories uncommon for nonvital assets; disconnect between asset value and appropriate countermeasures
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Focused on system resumption activities; forensics procedures immature (beyond event re-creation); requires good IT/ICS relationships
Physical and Environmental Security	Can range from poor (office systems to excellent (critical IT operations systems)	Usually excellent for critical areas, maturity varies for site facilities based on criticality/culture
Secure Systems Development	Integral part of development process	Historically not an integral part of development process; vendors are maturing but at slower rate than IT; core/flagship ICS solutions difficult to retrofit with security
Security Compliance	Definitive regulatory oversight depending on sector (and not all sectors)	Specific regulatory guidance depending on sector (and not all sectors)

Defense-in-Depth strategies applied to control systems are also dependent on business realities, including:

- The costs of securing legacy systems,
- The growing trend to connect control systems to business networks,
- The ability to provide access to business and ICS assets for remote users,
- Supply chain trust issues,
- The state of the art regarding the ability to monitor and secure ICS-specific protocols, and
- The ability to maintain up-to-date situational awareness of emerging threats to ICS.

Defense in Depth is not one thing, but a combination of people, technology, operations, and adversarial awareness. Thinking and doing solves problems, and technology enables problem solving by providing a set of tools that can reduce risk. The best technology in the world will not prevent humans from making mistakes—whether intentional or unintentional. Organizations must constantly adjust and refine security countermeasures to protect against known and emerging threats.

Applying Defense-in-Depth strategies to ICS environments improves security by raising the "cost" of an intrusion while improving the probability of detection and capability to defend against a malicious threat actor. Security countermeasures, based on best practices and standards, protect the ICS critical assets through multiple layers of defenses, thereby improving protection for operations, personnel, and technology.

The end goal is to reduce the opportunities for an adversary to take advantage of the ability to move laterally through an entity's networks/systems, and forcing the adversary to have a greater capability in order to accomplish their goal (increasing the cost of the intrusion to the threat actor). Using multiple layers helps prevent direct attacks against critical systems and greatly increase the difficulty of reconnaissance activities on ICS networks and systems while providing natural areas for the implementation of intrusion-detection technologies.

This section discusses some of the available and recommended solutions and strategies for Defense-in-Depth security, as outlined in Table 2. Organizations should use these solutions and strategies in combination to create layers of defenses, enabling ICS functionality while providing the most robust protection available for critical assets.

Table 2. Defense-in-Depth strategy elements.

Defense in Depth Strategy Elements	
Risk Management Program	· Identify Threats · Characterize Risk · Maintain Asset Inventory
Cybersecurity Architecture	· Standards/ Recommendations · Policy · Procedures
Physical Security	· Field Electronics Locked Down · Control Center Access Controls · Remote Site Video, Access Controls, Barriers
ICS Network Architecture	· Common Architectural Zones · Demilitarized Zones (DMZ) · Virtual LANs
ICS Network Perimeter Security	· Firewalls/ One-Way Diodes · Remote Access & Authentication · Jump Servers/ Hosts
Host Security	· Patch and Vulnerability Management · Field Devices · Virtual Machines
Security Monitoring	· Intrusion Detection Systems · Security Audit Logging · Security Incident and Event Monitoring
Vendor Management	· Supply Chain Management · Managed Services/ Outsourcing · Leveraging Cloud Services
The Human Element	· Policies · Procedures · Training and Awareness

2.1 Risk Management and ICS

Improving cybersecurity posture by implementing an ICS Defense-in-Depth strategy starts with developing an understanding of the business risk associated with ICS cybersecurity and managing that risk according to the overall business risk appetite. The individuals responsible for managing and maintaining the functionality of control systems need to know the methods to assess and determine cybersecurity risk and how to apply that knowledge to their unique environment. A clear understanding of the threats to the business; the operational processes and technology used within the organization; and its unique functional and technical requirements enables an organization to embed a layered approach for cybersecurity monitoring and defense into the day-to-day operation of their ICS.

An effective ICS security program depends on the willingness of the ICS operations staff to accept security as an enabler for all computer-oriented activities and their ability to apply security controls to their operational technology from a standpoint of acceptable risk. Designing an effective ICS security architec-

ture requires a risk model that maps specifically to the functional requirements for these complex systems. A control system can affect the physical world, and as a result, the definition of risk as it applies to an ICS must include considerations for potential real-world consequences. Individuals at all levels within an organization should understand ICS risks and actively engage themselves in the risk management process.

2.1.1 Multitier Risk Management Integration

To integrate ICS risk management practices throughout an organization, the entity should employ a three-tiered approach that addresses risk at the organization level (Tier 1), the mission/business process level (Tier 2), and the information system level (Tier 3), as illustrated in Figure 2. This approach is adapted from NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems—A Security Life Cycle Approach; NIST SP 800-39, Managing Information Security Risk—Organization, Mission, and Information System View; and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

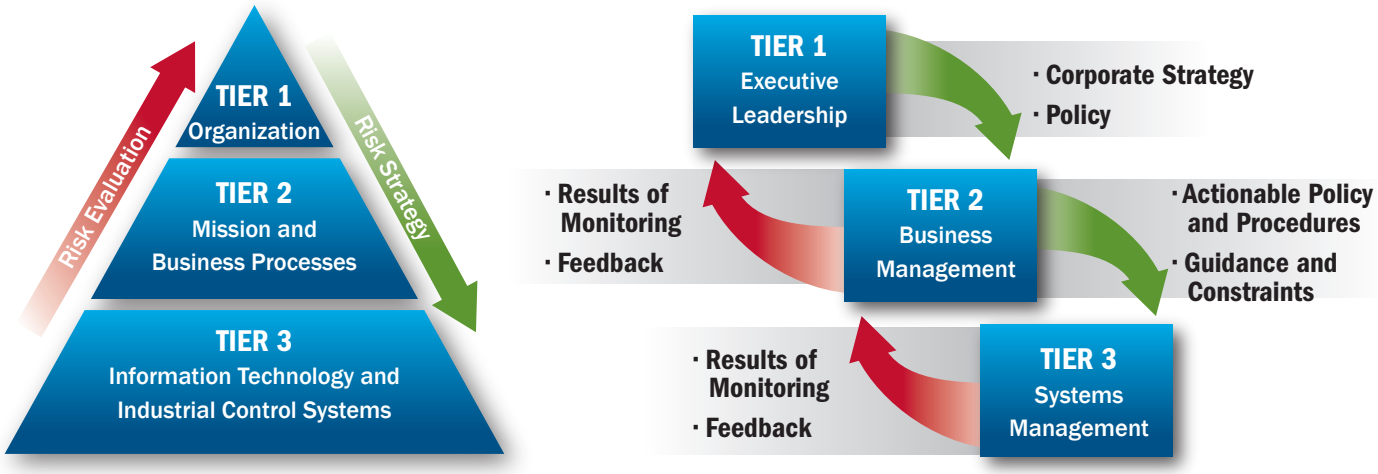

Figure 2. Risk management tiers.

Tier 1 addresses risk from an organizational perspective. At this level, the organization implements the first component of risk management—risk framing—providing the context for all risk management activities and providing the basis for risk management throughout the organization, including the operational technology (OT) space. Tier 1 activities determine:

- The techniques and methodologies used to assess information system-related security risks and other types of risk of concern from an overall business standpoint,
- The methods and procedures used to evaluate the significance of the risks identified during risk assessments,
- The types and extent of risk mitigation measures used to address identified risks,
- The level of risk the organization plans to accept (risk tolerance),
- How the organization plans to monitor risk on an ongoing basis, and
- The degree and type of oversight to ensure that the risk management strategy is being effectively carried out.

Tier 2 addresses risk from a mission/business process perspective informed by the risk context, risk decisions, and risk activities at Tier 1. Tier 2 risk management activities include:

- Defining the core ICS functions and processes that support the organization;
- Prioritizing the ICS functions and processes with respect to the overall goals and objectives of the organization;

- Defining the types of information needed to successfully execute the core ICS functions and processes and their interdependencies and information flows (information and security architecture);
- Developing an ICS information protection strategy and incorporating ICS security requirements into the operational processes; and
- Specifying the degree of autonomy with regard to assessing, evaluating, mitigating, accepting, and monitoring risk.

Tier 3 implements security at the operational level and addresses risk from an information system perspective. The risk context, risk decisions, and risk activities at Tiers 1 and 2 guide activities at this level. Tier 3 risk management activities include performing the five system-level ICS risk management functions (identify, protect, detect, respond, and recover) as part of a disciplined and structured system development life cycle process.

Applying risk management to ICS at a practical level does not depend on having all three tiers in place. Organizations can apply risk management practices to ICS at the operational level by defining a workable risk management process; ensuring that systems are inventoried, categorized, and security prioritized based on their importance and impact; identifying threats and vulnerabilities and their associated mitigation strategies; and ensuring that risk acceptance processes and approval hierarchies are defined and implemented as part of the ICS system life cycle.

2.1.2 Risk Management Approach

The attack surface for an operation includes any and all the vectors associated with gaining access to the systems or equipment considered critical to business operations. To implement controls necessary to reduce the attack surface for critical assets, an organization must first identify the systems and components they consider business or mission critical. Then they must determine the criticality of the assets based on its function and importance to business operations. The business then performs a cybersecurity risk analysis of the system to identify the current threats, vulnerabilities, and risks to the system and/or operations, and the potential impact should a threat be carried out. Figure 3 shows this process.

Figure 3. Risk Management Approach.

Organizations should apply controls at the highest security level possible while enabling uninterrupted functionality. Finally, they should monitor and adjust security controls as necessary to ensure ongoing protection against emerging threats.

Risk Analysis

- Identify the threats that face the business.
- Document the system network architecture.
- Identify technologies used in the business.
- Identify the software applications within the operation.
- Identify the human elements in the organization.
- Determine assets critical to business operation.
- Predict the likelihood of a threat actor carrying out a threat.
- Predict methods of an intrusion executed to exploit existing critical asset or process vulnerabilities.
- Prioritize risk scenarios based on impact to the business.

2.2 Asset Inventory and Risk Characterization

For ICS security to be effective, an asset owner must first identify what needs protection. Doing so establishes a baseline understanding among the stakeholders relative to the support infrastructure (both IT and ICS). Asset owners must identify and prioritize process systems (including process equipment and operations and ICS software, networks, and personnel) and analyze interconnections and dependencies based on their business impact. Understanding the business context and the resources that support critical functions and the related business risks enables an organization to focus and prioritize its efforts consistent with its risk management strategy and business needs.

Asset identification is an important step in understanding and managing ICS risk and helps to determine the basis and priorities for applying security defenses. This is also vital in determining what specific monitoring should be considered, what countermeasures are practical, what countermeasures can impede normal system behavior, and what compensating controls asset owners can deploy if there is no applicable technical countermeasure. Unlike IT, managing cybersecurity within control system domains requires consideration of unique system nuances and realistic conditions that need met for an adversary to compromise the system and cause process impact. Identifying all assets within the control system is vital to understanding the potential impact cyber-related intrusion. Assets can include systems, information, or processes (operations).

Asset Characterization

- What asset (information) needs to be protected?
- Why does the asset need to be protected?
- Who has the responsibility for managing and protecting the asset (what are the roles, responsibilities, accountabilities and authorities)?
- If the threat actor compromised the asset, what realistic worst-case scenarios would result?
- What is the value of the asset?
- What is the criticality of the process or information to the business mission?
- What are the protection levels for confidentiality, integrity, and availability?
- What interconnections are required for the systems to perform?
- What methods are currently available for user access?
- What dependencies are present for system functionality?
- How does the information flow through the system, and through what mechanisms?

The key is to identify the thread that defines assets from its mission (purpose) to the asset itself to supporting infrastructure to ICS dependencies. This thread will reveal which ICS components are more critical when applying security controls.

A current inventory that has all ICS components characterized according to their criticality to their function provides a solid basis for applying defense measures, and helps to ensure that asset owners miss no systems or leave no critical devices unprotected.

2.2.1 Inventory Assets

A comprehensive inventory of ICS assets develops a baseline understanding among all stakeholders relative to the support infrastructure (both IT and ICS). Organizations should identify systems (including hardware, software, and supporting infrastructure technologies) and analyze dependencies to understand both the function of the asset itself and the resources required to support critical functions. Organizations should couple technical network maps for all systems with the physical inventory and an operational-level of understanding of the information flows, which provide a basis for determining the protection levels for each system or subsystem and the controls to put in place to protect the system without compromising or degrading its performance. In an ICS environment, identifying both upstream and downstream dependencies is critical, as the processes involved are, many times, interdependent and potential effects subtle.

The greatest vulnerability to ICS systems occurs at any point of connection. While Internet connectivity may present the greatest vulnerability, asset owners must identify any connectivity in this step—whether currently connected or could be connected later. To leave even one potential connection undiscovered could inadvertently leave the entire system and network vulnerable. Running a scan on the network elements will identify only what is connected and on at the moment of the scan, so the organization should conduct a physical inventory as well.

2.2.2 Categorize Asset Criticality

Determining asset criticality starts with identifying the information generated, processed, stored, and disseminated on and from the ICS; the function of the ICS asset within the overall operation (keeping in mind both upstream and downstream functional impacts); and assigning a security categorization for that asset. Asset owners should rate the security categorizations based on the potential impact (low, moderate, or high) on the organization should an event occur that jeopardizes its ability to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The key is to identify the thread from the function (purpose) of the asset to its supporting infrastructure and ICS dependencies. This thread will reveal which ICSs are more critical when it comes to applying security controls.

2.2.3 Identify Security Risks

In order to define and articulate the risk to ICS, organizations must identify the potential threats to the ICS and the vulnerability of the system to those threats. This information provides the current security risk exposure for the ICS.

Security Risks

- Insider intentional threats—disgruntled employees, vendors, system integrators or anyone else with internal knowledge or access to the ICS;
- Internal unintentional threats—inappropriate system designs, policies, architectures procedures, technologies or testing;
- External nontargeted threats—maliciously designed software viruses and worms; and
- Malicious actors—“black hat” hackers, criminals, and nation-states.

The individuals most technically competent to understand the potential attack vectors and system-level consequences are typically operations line managers and operators. They understand the operational systems and the potential impact to the system should a threat actor compromise the control system. They can also help to determine the potential consequences of a system failure to the business, which may include the loss of information.

2.2.4 Determine Potential Impact

An organization can estimate the likelihood of a threat actor carrying out a threat or exploiting a vulnerability by taking into account the potential channels for threat exploitation, such as whether the system is in a higher or lower security zone on the network, its access and privilege requirements, its security configuration, and identifying any exceptions to security policy. The potential impact of a threat actor compromising or making an asset unavailable (for example, financial, damage to other systems or to the public, including human safety concerns) is based on the criticality of the system or information, the visibility of the system or the exploit, and the ability to quickly remediate any damage caused by the compromise. This step identifies both direct and collateral impacts.

For ICS environments, the impacts can also be kinetic—that is, runaway processes or system failures can have physical and environmental consequences, such as a dam opening and flooding downstream areas. Asset owners should consider any impact that could present safety concerns as high impact. Figure 4 characterizes the current risk by impact and likelihood.

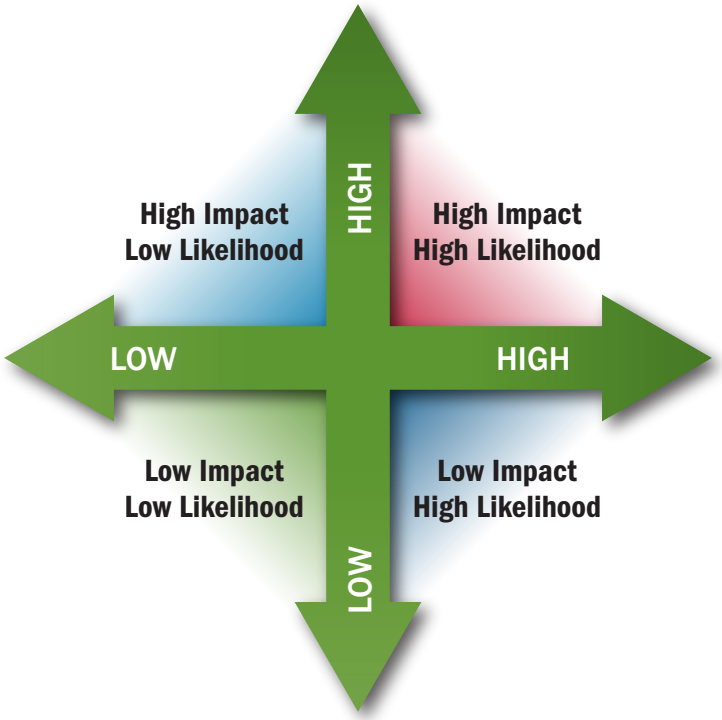

Figure 4. Simple qualitative risk analysis chart.

2.2.5 Identify and Tailor Controls

The Chief Information Security Officer or organizational equivalent usually sets baseline security controls, with input from IT and OT operations and management personnel, and based on the overall protection level (criticality). If the system is critical to the organization's mission (as identified in a Business Impact Assessment) or if the ICS controls a process with potential human safety consequences, it may require special consideration and additional controls.

In addition, security controls for ICS may be based on the regulatory requirements for the sector, some of which are discussed in Section 4.3. The National Institute of Standards and Technology (NIST), in their "Framework for Improving Critical Infrastructure Cybersecurity," has published recommended controls for organizations wishing to protect their ICS. Organizations should gear ICS controls toward reducing risk while enabling functionality.

Asset owners should tailor security controls for a particular system based on mission needs or system functionality requirements. Control tailoring may add or subtract controls from the recommended control set. Asset owners should base tailoring on a documented business need, assessed for risk, and approved prior to system or application implementation or production release.

An important part of identifying and tailoring security controls is to remember that policies and procedures are critical controls as well. Organizations should review and update policies and procedures to drive the implementation of Defense-in-Depth practices. Understand organization policies and procedures and ensure they are current and support ICS cyber risk reduction goals. Companies often have "unwritten policies" or rely on the expertise of their personnel to apply security controls, which leads to inconsistent applications. Asset owners should maintain written and formalized policies and procedures and view them as a vital part of their Defense-in-Depth strategy.

2.2.6 Implement Security Controls

Apply security controls to ICS according to priority. The most critical (high impact) and most vulnerable (high likelihood) systems should be the first priority for risk reduction and mitigation activities. Pervasive vulnerabilities, such as the use of unsupported operating systems (OS), are also a good starting point for applying security controls. Regular system updates can provide far-reaching protection and reduce risk across many systems. Security controls for the human aspect of security should include cybersecurity awareness training that undergoes regular review and frequent testing. This process significantly reduces the physical business attack surface.

Asset owners should not see security controls as an "add-on" for ICS. They should integrate security considerations and processes into existing policies and procedures and consider them an integral part of the system life cycle. No system is 100 percent secure; however, applying security controls to the systems and environment can help reduce risk to an acceptable level. This is where organizations must apply Defense-in-Depth practices.

ICS systems may have functional or operational properties that disallow the application of a security control. In these cases, a variance, waiver, or exception to a control may be in order. A control variance is a request to accept a compensating control. Compensating controls apply security protection at or above the same level as outlined in the control requirement and usually do not raise risk to the security of the system. Control waivers are requests to tailor the control out of the baseline for the system, because it does not apply to the system, its implementation, or environment. Control exceptions are requests made when the organization determines that the control applies to the system, but they will not implement them for an established business reason. ICS environments, unlike IT environments, usually require a good amount of control tailoring or may have many variances, waivers, or exceptions because of their specialized functionality, unique protocols, and specific operational requirements. When considering control exceptions, organizations should perform a risk assessment and ensure that the appropriate personnel review and accept the risk of not implementing a security control. Organizations should consider these exceptions temporary and review them periodically to ensure they address them in a timely manner.

2.2.7 Monitor and Adjust

Security for any system is never a "once and done" activity. Organizations constantly change ICS environments—adjusting settings, replacing or upgrading older systems, implementing new capabilities, releasing vendor patches—and the threats to ICSs and operations constantly evolve. Security monitoring is critical to ensure ongoing system protection.

Asset owners should review or assess the implementation status for all security controls periodically throughout the system development life cycle. This provides an important indicator of whether the controls work as intended and reduce risk. Asset owners may need additional or compensating controls to further reduce risk, so they should revisit the control selection process and properly address identified risks. The results of these assessments or reviews will provide the organization with a determination of residual risk and also provide insight into areas where they need to make security control adjustments.

This document discusses some of the technical controls that provide monitoring information; however, system monitoring only works when performed diligently and when the process in place uses the information to continually improve. Monitoring and adjustment activities such as system auditing and reviews, assessments, configuration management and change control processes, and applying lessons learned are an essential part of risk management practices.

2.3 Physical Security

Physical security measures reduce the risk of accidental or deliberate loss or damage to organizational assets and the surrounding environment. The assets being safeguarded include physical assets such as tools and plant equipment, the environment, the surrounding community, and intellectual property including proprietary data such as process settings and customer information. Physical security controls often must meet environmental, safety, regulatory, legal, and other requirements, often specific to a given environment. Organizations should tailor physical security controls, like technical controls, to the type of protection needed.

Organizations must address the physical protection of the cyber components and data associated with the ICS as part of the overall security in the ICS environment. Security at many ICS facilities is closely tied to plant safety with a primary goal of keeping people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the ICS environment. Organizations employ these measures to prevent undesirable system impact such as the following:

- Unauthorized physical access to sensitive locations;
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations;
- Unauthorized observation of sensitive information assets through visual observation, note taking, photographs, or other means;
- Unauthorized introduction of new systems, infrastructure, communications interfaces, or other hardware; and
- Unauthorized introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact such as a universal serial bus (USB) memory device, wireless access point, or Bluetooth or cellular device.

Physical Access

- Facility access controls;
- ICS control and server room access;
- Multifactor (for example, key card, card-and-personal identification number (PIN), or biometric) authentication for physical access;
- Facility monitoring using cameras, motion detectors;
- Alerting for device manipulation such as power removal, device resets, cabling changes, or the addition/use of removable media devices; and
- Visitor escort requirements and procedures.

Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. Likewise, having logical access to systems, such as command servers and control room computers, allows an adversary to exercise control over the physical process. If computers are readily accessible, and they have removable media drives (for example, floppy disks, compact disks (CD), digital video disks (DVD), Blu-Ray drives, external hard drives) or USB ports, organizations can fit the drives with locks or remove them from the computers and disable USB ports. Depending on security needs and risks, asset owners might also find it prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, place servers in locked areas and protect authentication mechanisms (such as keys). Also, locate the network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, in a secured area accessible only by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers—both active and passive—around buildings, facilities, rooms, equipment, or other informational assets establishes these physical security perimeters. Physical security controls include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by first preventing access to the facility through the use of fences, guards, gates, and locked doors.

Physical access control systems should ensure that only authorized people have access to controlled spaces. An access control system should be flexible. The need for access may depend on time (day versus night shift), level of training, employment status, work assignment, plant status, and a myriad of other factors. A system must verify that individuals being granted access are who they say they are (usually using something the person has, such as an access card or key; something they know, such as a PIN; or something they are, using a biometric device). Access control should be highly reliable, yet not interfere with the routine or emergency duties of plant personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity. Limit access to network and computer cabinets to only those who have a need such as network technicians and engineers or computer maintenance staff. Lock equipment cabinets and keep wiring neat and within cabinets. Consider keeping all computers in secure racks and using peripheral extender technology to connect human-machine interfaces (HMI) to the racked computers.

Access monitoring systems include still and video cameras, sensors, and various types of identification systems. Examples of these systems include cameras that monitor parking lots, convenience stores, or airports. These devices do not specifically prevent access to a particular location; rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. Provide adequate lighting based on the type of access monitoring device deployed.

Access-limiting systems may employ a combination of devices to physically control or prevent access to protected resources. Access-limiting systems include both active and passive security devices such as fences,

doors, safes, gates, and guards. They often get coupled with identification and monitoring systems to provide role-based access for specific individuals or groups of individuals.

Locating people and vehicles in a large installation is important for safety reasons, and, increasingly so, for security reasons as well. Asset location technologies can track the movements of people and vehicles within the plant to ensure that they stay in authorized areas, identify personnel needing assistance, and support emergency response.

In addressing the security needs of the system and data, always consider environmental factors. For example, in a dusty location, place systems in a filtered environment. This is particularly important if the dust is conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, mount systems on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (for example, backup tapes and floppy disks) should have stable temperature and humidity. An alarm to the process control system should sound when environmental specifications, such as temperature and humidity, exceed the limits.

Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during normal operation and emergency situations, which could include the release of toxic substances. Organizations should carefully design fire systems to avoid causing more harm than good (for example, to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security, and need to be protected against potential cyber incidents as well.

Reliable power for the ICS is essential, so organizations should have an uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to last for a few seconds; however, if the site relies on external power, the UPS battery life may need to last for several hours. It should be sized, at a minimum, so that the system can be shut down safely.

Physical security for the control center/control room will reduce the potential for many threats. Control centers/control rooms frequently have consoles continuously logged onto the primary control server, where speed of response and continual view of the plant is of utmost importance. These areas will often contain the servers themselves, other critical computer nodes, and sometimes plant controllers. Asset owners should limit access to these areas to authorized users only, using authentication methods such as smart or magnetic identity cards or biometric devices. In extreme cases, an asset owner could consider it necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room becomes uninhabitable.

Computers and computerized devices used for ICS functions (such as programmable logic controller (PLC) programming) should never leave the ICS area. Laptops, portable engineering workstations, and handhelds should be tightly secured and never used outside the ICS network.

Organizations should also address cabling design and implementation for the control network. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for the plant environment because of its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Use industrial registered jack (RJ)-45 connectors in place of other types of twisted pair connectors to provide protection against moisture, dust, and vibration. Fiber-optic and coaxial cables are often better network cabling choices for the control network because they are immune to many of the typical environmental conditions, including electrical and radio frequency interference found in an industrial control environment. Color code and label cables and connectors to clearly delineate the ICS and IT networks and reduce the potential for an inadvertent cross-connect. Install cable runs to limit access to authorized personnel only and install equipment in locked cabinets with adequate ventilation and air filtration.

2.4 ICS Network Architectures

The convergence of once-isolated ICSs has helped organizations simplify the management of complex environments. Connecting these networks and incorporating IT components into the ICS domain introduces vulnerabilities that asset owners must address before issues arise. Contributing factors include:

- Insecure connectivity to internal and external networks,
- Technologies with known vulnerabilities, creating previously unseen cyber risk in the control domain, and
- Lack of a qualified business case or understanding of requirements for ICS environments.

The former isolation from external (and historically untrusted) networks allowed the organization to reduce the level of ICS security to those threats associated with having physical access to a facility or a plant floor. Most data communications in the ICS information infrastructure required limited authorization or security oversight because operational commands, instructions, and data acquisition occurred in a closed environment with trusted communications. In general, when someone sends a command or instruction via the network, they anticipate that it will arrive and perform the authorized function, because only authorized operators have access to the system.

Merging a modern IT architecture with an isolated network that may not have any countermeasures in place is challenging. Using simple connectivity (that is, routers and switches) provides the most obvious way to interconnect networks; however, unauthorized access by an individual could result in unlimited access to the ICS. The diagram shown in Figure 5 depicts an integrated architecture that includes connections from external sources such as the corporate LAN, peer sites, vendor sites, and the Internet. The model comes from the International Society of Automation and provides insight into the widely accepted SP-99 (Purdue) Model of Control.

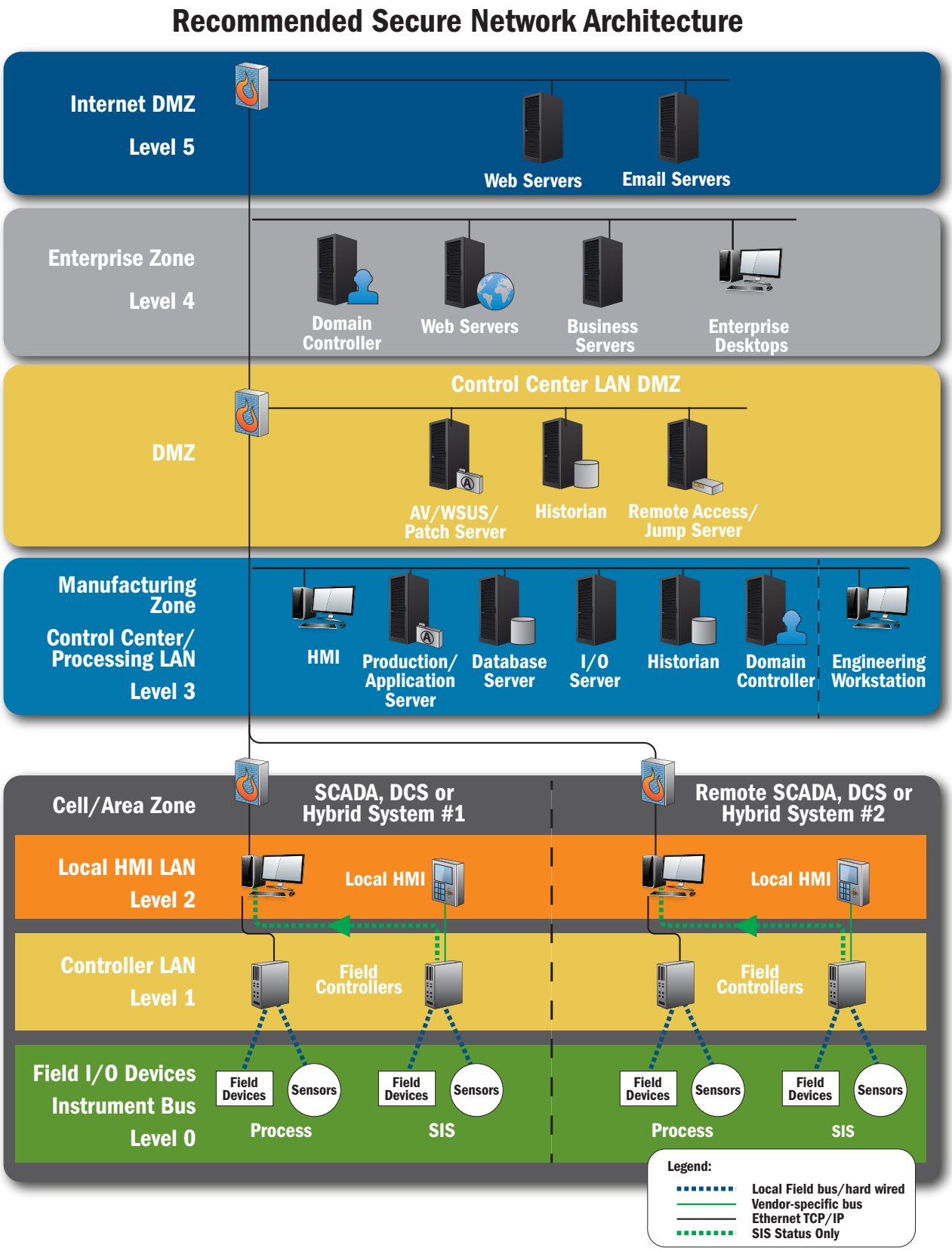

Figure 5. Recommended secure network architecture.

Integrated architectures, if compromised, could provide a threat actor with various avenues of access to critical systems—either via the corporate LAN, the control LAN, or even the communications LAN. The very nature of such architectures demands the exchange of data from disparate information sources, a factor that could be taken advantage of by an intruder. One emerging industry strategy for ICS Defense

in Depth uses concepts such as the implementation of "zones and conduits" to secure communication pathways between trusted environments.[2]

2.4.1 Common Architectural Zones

In order to create a layered defense, one must have a clear understanding of how all the technology fits together and where all the interconnectivity resides. Dividing common control system architectures into zones can assist organizations in creating clear boundaries in order to effectively apply multiple layers of defense. Understanding how to achieve network segmentation is vital to creating architectural zones and determining the best methodologies for segmenting networks within and around control system environments.

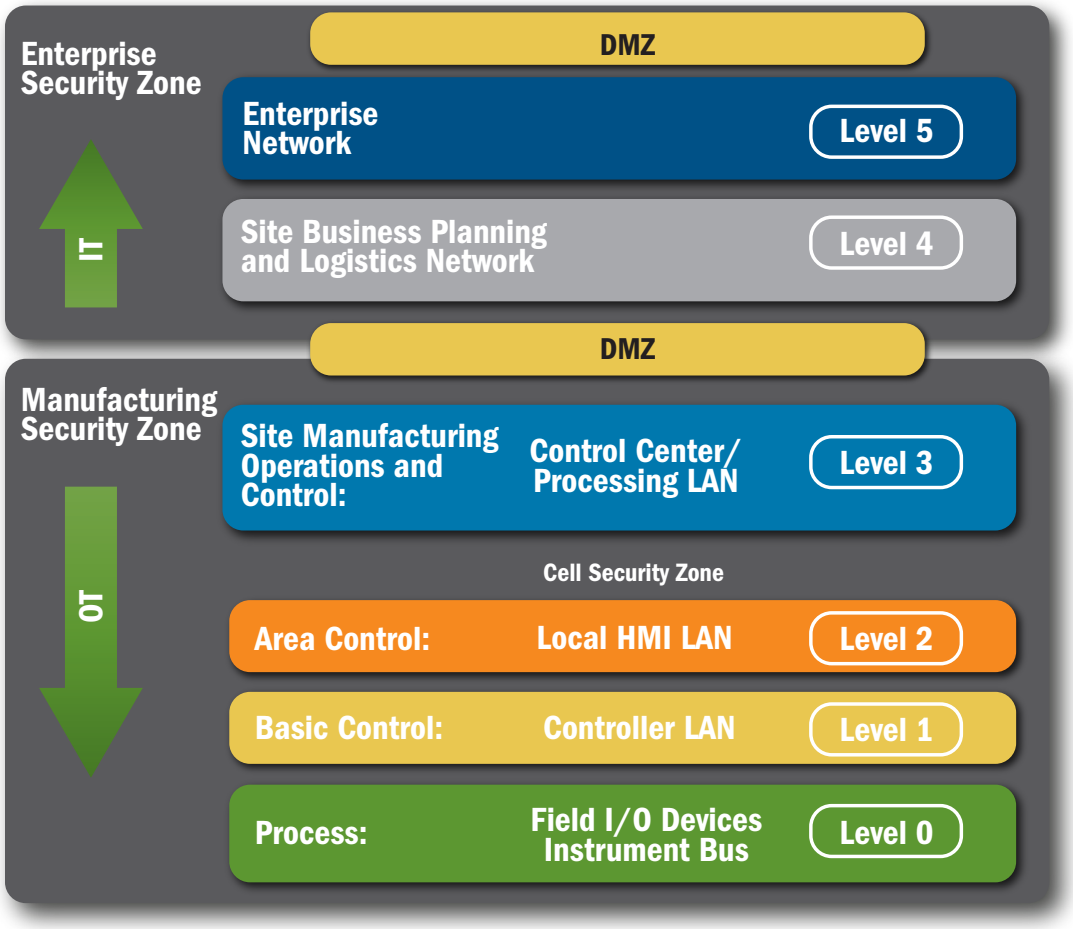

Figure 6. Zone segmentation of business & ICS architecture.

The zones depicted in Figure 6 segment business IT and OT networked information systems architecture into its basic functions:

Enterprise Security Zone: The Enterprise Security Zone includes connectivity to the Internet, peer locations, and backup or remote offsite facilities (Enterprise network connectivity–Level 5) as well as the business networks that include corporate communication, email servers, Domain Name System (DNS) servers, and IT business systems (Level 4). A wide variety of risks exist in this zone because of the amount of systems and connectivity, and from an ICS security standpoint, one should consider this zone untrusted.

2. IEC 62443-3-2; Security for industrial automation and control systems - Security Risk Assessment and System Design

Manufacturing Security Zone: This zone (Level 3) contains the area of connectivity where a vast majority of monitoring and control takes place. It is a critical area for the continuity and management of a control network. Operational support and engineering management devices are located in this zone, along with data acquisition servers and historians. The Manufacturing Zone is central to the operation of end devices and provides required connectivity to the Enterprise Zone. The priority of this area is high. Risks are associated with its direct connectivity to any external systems or networks.

Cell Security Zone: The Cell Security Zone contains systems used for local or remote area control (Level 2), such as field located HMIs, PLCs, and their controls (Level 1) and basic input/output devices such as actuators and sensors (Level 0). The priority of these zones is very high, as these are the areas where the control functions affect the physical end devices. In a modern control system network, these devices will likely have support for Transmission Control Protocol/Internet Protocol (TCP/IP) and other common protocols. It also may include safety-instrumented systems (SIS), which automatically control the safety level of an end device—elevating the risk. Ideally, one would locate the SIS on a separate network—ensuring that should an incident occur on the primary ICS network, the safety systems continue to function and are not at risk of compromise.

Each of these zones requires a unique security focus. A "peel-the-onion" analysis shows that an intruder trying to affect a critical infrastructure system would most likely go after the core control domains contained in Level 3 and below. This depends on the overall objective of the attacker. In general, complete control over core services and operational capability of the control system has high value. Manipulation of the ICS information resources can devastate an organization if this critical zone becomes compromised. In many sectors, the malicious intrusion on the control system will have real-world, physical results.

In an attack scenario, the intrusion begins at some point outside the control zone and the actor pries deeper and deeper into the architecture. Layered strategies that secure each of the core zones can create a defensive strategy with depth, offering the administrators more opportunities for information and resource control, as well as introducing cascading countermeasures that will not necessarily impede business functionality.

2.2.4 Demilitarized Zones

A demilitarized zone (DMZ) (sometimes referred to as a perimeter network) is a physical and logical sub network that acts as an intermediary for connected security devices so that they avoid exposure to a larger and untrusted network, usually the Internet. The DMZ adds an additional layer of security to an organization's LAN; an external intruder only has direct access to equipment within the DMZ, rather than any other part of the network.

The ability to establish a DMZ between the corporate and control networks represents a significant improvement with the use of firewalls. As shown in Figure 8, each DMZ holds one or more critical components, such as the data historian, the wireless access point, or remote and third-party access systems. Creating a DMZ requires that the firewall offers three or more interfaces, rather than the typical public and private interfaces. One of the interfaces connects to the corporate network, the second to the control network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points on the DMZ network.

By placing corporate-accessible components in a DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the DMZ. Most firewalls can allow for multiple DMZs and can specify what type of traffic may be forwarded between zones. The firewall can block arbitrary packets from the corporate network from entering the control network and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, one can maintain clear separation between the control network and other networks with little or no traffic passing directly between the corporate and control networks.

The primary security risk in this type of architecture comes when a threat actor compromises a computer in the DMZ and uses it to launch an exploit against the control network via application traffic permitted from the DMZ to the control network. Organizations can reduce this risk if they make a concerted effort to harden and actively patch the servers in the DMZ, and if the firewall rule set only permits connections initiated by control network devices between the control network and DMZ. Other concerns with this architecture include the added complexity and the potential increased cost of firewalls with several ports. For more critical systems, however, the improved security should more than offset these disadvantages.

Two-zone solutions (no DMZ) are marginally acceptable, but one should only deploy them with extreme care. The most secure, manageable, and scalable control network and corporate network segregation architectures typically use a system with at least three zones, incorporating one or more DMZs.

Organizations could create multiple DMZs for separate functionalities and access privileges such as peer connections, the data historian, ICS communications protocols, the Inter Control Center Communications Protocol (ICCP) server in supervisory control and data acquisition (SCADA) systems, the security servers, replicated servers, and development servers. Multiple DMZs have proven effective in protecting large architectures composed of networks with different operational mandates. The secure flow of data into and out of the different environments is critical to operations.

One must be cautious when deploying DMZ solutions to connect otherwise logically separated domains. Do not assume that the implementation of a DMZ is a panacea for preventing threat actors from penetrating deeper into critical environments. The exploitation of transitive trust across a security perimeter is a plausible intrusion vector. However, when one develops and deploys a DMZ with appropriate security, the countermeasure will increase the work effort for the adversary, provide more granular control for the asset owner, and reduce cyber risk to vital critical assets. Some high-level considerations that one can use to support an effective Defense-in-Depth strategy utilizing DMZs are as follows:

- Asset owners should limit access to an ICS DMZ to only authorized users, applications, and services. Wherever possible, asset owners should model ingress and egress traffic to and from the DMZ so that they can use additional security monitoring and anomaly detection at the payload level in addition to source/destination/service filtering.
- Access from the higher security zone (that is, from within control or operations levels) is generally to "push" data to the DMZ application and make that data available to the authorized enterprise users. Access for the enterprise user is only to pull from the DMZ application server, thereby providing further separation. It is important to create this logical separation so that a threat actor cannot exploit the trust between the corporate enclaves in the DMZ to "pivot" from the DMZ into the control system.
- Asset owners often use DMZs for remote access. Allowing remote access creates a number of issues that organizations must consider prior to documenting a policy and implementing a remote access process. Whether from the corporate network to the ICS or from the Internet to the ICS, remote access provides a serious risk to the system. An intruder can gain access to a user account at the user's home or his/her corporate office and use those stolen credentials to connect to critical ICS assets, or allow an infected computer an access channel into the ICS networks via an established virtual private network (VPN) connection. The organization must decide what, if any, access they require from remote locations; whether a particular user truly needs that access (and if so, at what level); and how to harden the access process to reduce the risk to an acceptable level.
- Asset owners should only allow authorized external users to remotely connect to intermediary authentication servers residing in a DMZ. In addition to using multifactor authentication methods, definitive rules and connection states should be clearly identified and maintained. These servers (often referred to as "jump boxes") provide connectivity to remote computers that are likely less secure than the jump boxes themselves. In addition to multifactor authentication and specific security related to user roles and least privileges, asset owners should harden jump boxes and any applications or services that do not support secure remote access removed.

2.4.3 Virtual LANs

A virtual LAN (VLAN) divides physical networks into smaller logical networks that consist of a single broadcast domain that isolates traffic from other VLANs. Using VLANs limits broadcast traffic and allows logical subnets to span multiple physical locations.

There are two categories of VLANs: static, often referred to as port-based, where one assigns switch ports to a VLAN so that it is transparent to the end user; and dynamic, where an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

One must secure VLANs used in ICS environments explicitly, because default configurations and standard network configurations are not inherently secure. Virtual networking does not come without risks, because exploits known as "VLAN" hopping can create opportunities for an adversary to move between networks that the asset owner has configured to be logically separated.

Many ICS network infrastructure designs deploy VLANs as part of segmenting network functions and capabilities. Current best practices suggest that if the information infrastructure is large, then organizations should decompose each of the contributing control system domains (such as those within a plant or energy management system) into smaller and more manageable segments and zones. This methodology facilitates easier administration and can protect against unwanted traffic artifacts from "bleeding" from one network to the other. While the VLAN approach is becoming favorable in the control system community, it is equally important to understand and protect against the most prominent intrusion vectors associated with deploying virtual networks. Cybersecurity experts refer to these exploits as "VLAN hopping," "double tagging" and "switch spoofing." The countermeasures and defensive capabilities associated with protecting against these types of intrusions have evolved significantly over the last several years. Because the countermeasures are generally not a default component of the security architecture or the security technology used to support the information infrastructure, the effectiveness of the countermeasures often becomes a function of how one configures them.

> ***"The most serious mistake that a user can make is to underestimate the importance of the Data Link layer, and of VLANs in particular, in the sophisticated architecture of switched networks. It should not be forgotten that the OSI stack is only as robust as its weakest link, and that therefore an equal amount of attention should be paid to any of its layers so as to make sure that its entire structure is sound."***
>
> ***–Virtual LAN Security Best Practices, Cisco Systems, Inc.***

The VLAN architecture needs to ensure the disabling of the Dynamic Trunking Protocol (DTP) and configure the switch ports as static access ports. This helps prevent switch spoofing exploits, because the access ports cannot handle tagged packets or become tagged ports. In addition, the unused switch ports become disabled—thus rendering them unavailable for any connectivity. When one specifically configures the port as an access port, it cannot become a trunk port and cannot send traffic to other/multiple VLANs. If DTP is disabled, an intruder cannot use any access ports configured as dynamic to create a network relationship.

System administrators can counter double tagging by removing access ports from the default (native) and designating the native VLAN on all switched trunks to "unassigned." Adversaries cannot match their port to one on a different VLAN. Administrators should always select an unused VLAN as the native VLAN for all trunks, and should not use this VLAN for any other purpose. They should prune VLAN 1 from all trunks and access ports that do not require it (including disconnected and shutdown ports). They also shouldn't use VLAN 1 for in-band management traffic and should use a different, dedicated VLAN to keep management traffic separate from user data and protocol traffic.

The following is a concise set of activities that can empower the asset owner to create manageable ICS VLANs and reduce the risks associated with them:

- Control physical access by removing console-port cables and introducing password-protected console or virtual terminal access with specified timeouts and restricted access policies.
- Use a one-to-one relationship between subnets and VLANs. This requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can route between multiple logical networks.
- Create role-based user accounts for all VLANs. Create an access-list to restrict telnet/secure shell (SSH) access from specific networks and hosts.
- Create and apply Layer 2 (L2) access control lists (ACLs) and Virtual ACLs, blocking the direct communication at L2 between a potential attacker and the attacked device. Embed more intelligence into the network so that it can check forwarded Address Resolution Protocol (ARP) packets for identity correctness.
- Use private VLANs to protect networks from unwanted traffic from untrustworthy devices.
- Enable port security.
- When feasible, prefer out-of-band management to in-band management.
- Limit the number of media access control (MAC) addresses used by a single port so the device traffic identification for a device is directly tied to its port of origin. Disable unused ports and assign them to an unused VLAN.
- Create and apply L3 ACLs by IP address (recommended for most static wired networks), MAC address filtering, port assignment, dynamic assignment (recommended for most wireless networks and shared switch port networks), protocols, and by applications. By default, treat only known and trusted ports as such, and configure all other ports as untrusted. This prevents attached devices from manipulating quality of service (QoS) values inappropriately.
- Turn off VTP/MVRP, and set DTP to "off" on all nontrusted ports. This is a best practice for using VLANs within ICS, as it can limit (or even prevent) possible undesirable protocol interactions in networkwide VLAN configurations. This precaution can also limit or prevent the risk of an administrator error propagating to the entire network.

2.5 Security Architectures

Once an organizations has designed and implemented a robust network architecture, they have established the security architecture for the network and systems. The security architecture includes the specific controls and their strategic placement within the network or systems to establish layers of security—Defense in Depth. Network diagrams and information flow diagrams that include all systems and their interconnections couple with the physical inventory to provide an operational-level understanding of the information flows within the network. Then overlay this with the protection levels for each system or subsystem that was assigned during inventory activities to help determine the controls to put in place to protect the system without compromising or degrading its performance.

System administrators must consider the application of security controls at the network, system, application, and physical layers to provide information assurance. These include policy and security management, application security, data security, platform security, network and perimeter security, physical security, and user security. The security architecture is where all the defensive mechanisms and controls come together, and overlay the network architecture. The security architecture defines where to apply Defense-in-Depth measures across the organization. NIST 800-82, "Guide to Industrial Control Systems (ICS) Security," provides a community-wide ICS security controls overlay based on the NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," security controls overlay generalized concept.

2.5.1 Perimeter Security

ICS perimeter security includes controls for both physical and logical security to protect the assets within those perimeters. The first consideration in logical perimeter protection is having a clear understanding of where the communications boundary exists. This requires evaluation to determine where threat actors could leverage potential intrusion vectors to infiltrate the ICS. Logical security includes controls such as authentication mechanisms, ACLs within network components, intrusion detection/prevention systems (IDS/IPS) signatures, situational awareness tools, and other means to protect the systems from a logical perspective. Physical perimeter security includes key cards to open doors, motion detection, cameras, security forces to respond to physical intrusion, and other mechanisms to protect physical assets.

2.5.2 Firewalls

Network security depends on multiple components, each with specific roles. Firewalls are the first line of defense within an ICS network environment. These components keep the intruder out while allowing the authorized passage of data necessary to run the organization. Thus, the concept of network segmentation applies to the network in layers to protect assets at all levels.

Firewalls act as sentinels, or gatekeepers, between zones. When properly configured, they will only let essential traffic cross security boundaries. If they are not properly configured, they could easily pass unauthorized or malicious users or content. Firewall rules monitor the network traffic and enable a trusted path to users and a trusted channel to other devices. This is only as effective as the accuracy of the rules they are configured with.

The firewall golden rule says "that which is not explicitly allowed is denied," which means that the final rule should not be "any, any," but rather "deny all."

The role of the firewall is to:

- Establish domain separation.
- Monitor (and log) system events.
- Authenticate users before they are allowed access.
- Monitor ingress and egress traffic and disallow unauthorized communications.

There are two types of firewalls—the host firewall and the network firewall. The host firewall protects a specific host. It can be part of the OS, or it can be an appliance directly in line with the host. The type of firewall used provides protection for the network using one of several techniques:

- Packet filtering
  - This type of firewall filters traffic based on rules. They control traffic based on the first three levels of the open systems interconnection (OSI) model: MAC address and IP address, with some filtering based on the transport layer (port numbers).
- Circuit level gateways
  - These types of firewalls allow only specific sessions to communicate.
- Proxy level gateways
  - This firewall provides filtering at the application layer. In other words, it limits the types of applications and protocols that communicate across security boundaries such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and so forth.
- Stateful inspection
  - Cybersecurity experts call this type of firewall stateful because it keeps track of the "state" of the connections crossing the firewall. They match the packets with the different types of connections to determine what to allow or reject.

Firewall placement should be coordinated, planned, and carefully thought through. The organization needs to ensure that placement of the firewall does not enable an individual or device to bypass the security of the firewall. For example, a computer with two network interface cards (NICs), often referred to as a "dual-homed" host, introduces cyber risk when one card connects to the corporate network and the other connects to the process control network (commonly used for the convenience of Operations Managers, ICS engineers, and so forth). Even though this type of configuration eases management and reduces complexity, it effectively bypasses perimeter protection mechanisms (such as a firewall) and can create a significant vulnerability that threat actors can exploit in virtual environments as well.

System administrators should layer the firewall rule set as shown in Figure 7 . Best practices apply at every level to ensure that only the traffic specifically allowed at each level passes through the firewall. It is also critical to keep rules up to date, because even a slight change could reduce effectiveness against current intrusion vectors/vulnerabilities. Rule changes and rule order can affect data flow permissions, so test them to ensure that the change does not negate security. Periodic reviews of firewall placement and rules will help ensure that defenses are maintained.

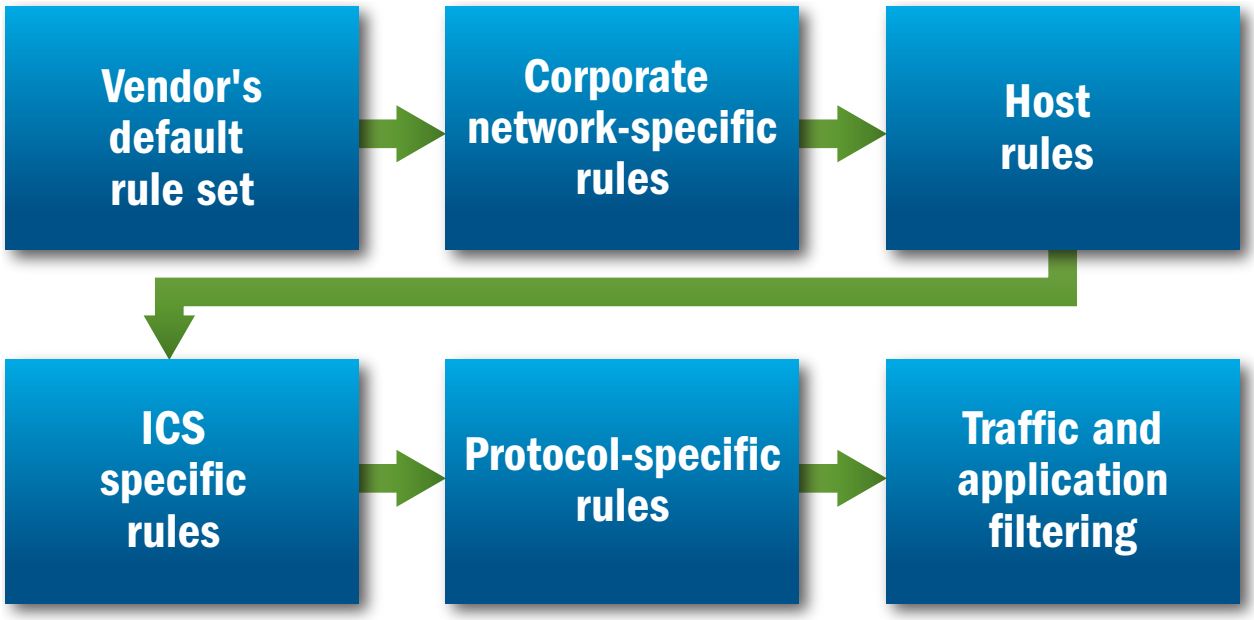

Figure 7. ICS firewall rule set layers.

Improperly placing a firewall can result in the firewall being less effective. Bypassing the firewall, whether intentional or not, is a fairly common occurrence. Modems that connect directly to process equipment, vendor VPNs that connect directly into the process control network, wireless access points, and dual-NIC computers all invalidate the effectiveness of the firewall.

2.5.3 Diodes

A unidirectional network device (also referred to as a unidirectional security gateway or data diode) is a network appliance or device that allows data to travel in only one direction. Users can find them most commonly in high security environments, such as defense, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the industrial control level for such facilities as nuclear power plants and electric power generation.

The physical nature of unidirectional networks only allows data to pass from one side of a network connection to another and not the other way around. The benefits for the users of the higher criticality (high side) network, such as an ICS segment, include the ability to share data with a lower criticality (low side) network, such as a server in a DMZ, while preventing communications access from the low side network to the ICS network. Traditionally, when the enterprise network provides DMZ server access for an authorized user, the data are vulnerable to intrusions from the enterprise network. However, with a

unidirectional network separating a high side with sensitive data and a low side with business and Internet connectivity, one can achieve the best of both worlds, enabling the connectivity required and assuring security. This holds true even if both the low and the high network are compromised, because the traffic flow control is physical in nature.

The controlled interface that comprises the send and receive elements of a unidirectional network acts as a one-way "communications protocol break" between both two-way network domains it connects. This does not preclude the unidirectional network's use in transferring protocols like TCP that require communications (including acknowledgments) between sender and receiver.

The electrical sector has used data diodes for several years, and regulators have encouraged their use to protect equipment and processes in SISs. The Nuclear Regulatory Commission (NRC) now mandates the use of data diodes and many other sectors, in addition to electrical and nuclear, also use data diodes effectively.

2.5.4 Access and Authentication Controls

In most ICS networks, many different systems are used by a number of different users, and the systems must be accessed quickly as system operations requires. Corporate authentication, authorization, and account management practices can be problematic for ICS, because ICSs are "always on," stopping the system for users to log out and log back in is usually not a viable option. Also, authentication processes provided by ICS suppliers may be limited. Managing many users in disparate locations becomes a challenge as one adds and removes system access and user roles change. The same authentication process may control access to many systems (HMIs, field devices, SCADA servers) and networks (remote substation LANs), which may require the use of shared credentials.

Asset owners can control access to ICS systems using either a distributed or centralized approach. Distributed access management requires that each system perform authentication separately. Each system uses a separate set of user accounts, credentials, and roles. This approach, while a good solution for small ICS implementations, does not scale well for large organizations.

Organizations normally use centralized account management to handle large numbers of users and accounts. Usually, it requires a central authentication system (for example, Active Directory or Lightweight Directory Access Protocol (LDAP)) to manage the accounts. An authentication protocol (for example, Kerberos, Remote Authentication Dial-In User Service (RADIUS), or Terminal Access Controller Access-Control System (TACACS)) communicates between the authentication server and the ICS. A centralized approach is scalable to large system implementations; however, it also introduces risk when used in ICS environments. The centralized servers must be highly secure because, if the authentication server becomes compromised, the entire ICS may be compromised. They are also required to be available in case of emergency, so one might need redundant servers that can be expensive.

2.5.5 Bring-Your-Own-Device

Operations, maintenance, and engineering personnel in ICS environments are implementing portable computing devices such as tablets, smart phones, and laptops. A number of organizations are actively promoting their use because of their popularity and the convenience of mobility while maintaining access. The problem with these devices stems from the fact that the organization does not typically manage them, therefore the security policies implemented by the organization do not get implemented on the portable devices. People also use these devices to access personal email, game apps, web pages, and social media applications, so the inherent security risks of public access make the Bring-Your-Own-Device (BYOD) concept inherently high risk to critical infrastructure. The organization must consider the risk and enact appropriate measures, such as mobile device management (MDM) systems, to mitigate the risk and bring it to an acceptable level.

2.6 Host Security

The host or workstation level implements another layer of security. Firewalls protect most devices within a network from intrusion from the outside; however, a good security model requires multitier layers of defense. This is particularly important for HMI clients that connect to the network from outside the trusted ICS network boundary, either via a VPN connection or any other means. Completely securing the network means securing all hosts as well.

Requirements for host security are well known in order to protect a machine/host while installing and using various operating systems and applications. The following guidelines provide some recommendations that organizations should consider as part of a security policy for system operations to help keep ICSs secure. In general, consider the following steps for every ICS host or device that is placed on the OT network, regardless of operating system:

- Install and configure a host-based firewall.
- Choose strong passwords for all accounts on the system, and change any default or well-known accounts on the device (preferably, enforce strong passwords and password expiration through operating system capabilities).

  Change passwords on a pre-defined schedule–usually every 30 and not more than 90 days.
- Install screen savers with short intervals and with a password requirement to log in where possible.
- Install and keep operating system patches and hardware firmware patches current.
- Configure and monitor logs on the device.
- Disable unused services and accounts or those that are no longer necessary.
- Replace insecure services (such as telnet, remote shell (RSH), or rlogin) with more secure alternatives such as SSH.
- Restrict access to services that one cannot disable, where possible.
- Make and test backups of the system in a consistent manner if not centrally controlled.
- Secure laptops and other portable and mobile devices not continuously connected to the network.

The same requirements as stated above apply to these devices as well, where feasible, regardless of the platforms and management techniques used.

PLCs and other operational control technologies, by and large, do not support many recommended host-based protection practices and security mechanisms. Defense-in-Depth controls for those devices usually apply at the network level. However, many HMI systems are based on common platforms and administrators should lock them down (for example, disable unneeded services, disable unneeded ports, restrict access, use kernel locking) to the fullest extent possible while ensuring continued functionality. Asset owners should remove any software installed natively on the system that they do not need or use. For example, an HMI used for command and control does not need standard corporate software packages such as word processing, spreadsheets, and email clients.

System configurations should be actively managed throughout the system life cycle. There are a number of techniques that organizations can use such as creating a secure image to configure new equipment, equipment re-builds that only contain required software, and configuration of devices with only required services and ports.

2.6.1 Patch and Vulnerability Management

Applying patches to ICS components presents a challenge to system administrators, because system updates and patches can interfere with the ICS function. A patch to an ICS component could change the way it works, resulting in component failure or loss of functionality. System administrators should test all patches off-line in a test environment that contains the same model and type of ICS to determine whether the patch has unintended consequences. Also, many ICSs utilize older OS versions, which the vendor may not support.

System designers should separate any process for applying ICS patches from the corporate patch management solution, and the application of patches to ICS should occur only during planned outages. Organizations should develop a systematic patch and vulnerability management approach for ICS and ensure that it reduces the exposure to system vulnerabilities while ensuring ongoing ICS operations.

Administrators should schedule software upgrades and patch management procedures at routine intervals. The development of procedures to incorporate security patches promptly and current software recommendations on a regular basis can substantially limit opportunities for hostile parties to target newly discovered vulnerabilities, which receive wide and immediate publicity. Organizations should institute practices to protect themselves without granting ample time for would-be intruders to apply the new knowledge against critical systems.[3]

2.6.2 Field Devices

Many field devices, such as older PLCs, remote terminal units (RTUs), and intelligent electronic devices (IEDs), are not capable of centralized management. They also may not have the security capabilities that other components such as workstations may have (for example, limited password length and characters that can be used). Most often, asset owners physically protect these devices behind fences, behind locked doors, or in locked cabinets; however, they should also lock down their configuration (for example, disable unneeded services, disable unneeded ports, restrict access, use kernel locking) to the fullest extent possible while ensuring continued functionality.

Field personnel are increasingly using portable devices such as tablets and smart phones for in-field control functionality. System administrators must secure these devices to the fullest extent possible, remove or turn off any unnecessary services (such as email capability), and keep them up to date with the latest security patches to ensure they do not introduce malicious code into the ICS. Furthermore, the company should manage any device used to interface with the ICS to ensure it meets all corporate security standards.

2.6.3 Virtual Machines

Asset owners are implementing and leveraging virtual machine (VM) technology as a method of reducing capital equipment, managing device recovery, and running multiple disparate guest operating systems on a single physical host machine. The ICS-CERT site assessment program notes that in many industry implementations asset owners apply inadequate user access security controls to the hypervisor host management interface. This provides a single point of entry that threat actors could use to control every guest VM on the host. Place these interfaces in management networks with strict and logged zone access control. When the physical host contains both DMZ and ICS servers, administrators should harden the networks and NICs and delete all others to prevent opening up a bridged scenario. Patching hypervisors is critical, and, when doing so, the OT and IT departments should coordinate to avoid impact to ICS processors.

2.7 Security Monitoring

Monitoring systems and networks for changes, anomalous behaviors, or for attack signatures can be difficult in an ICS environment; however, monitoring and detection capabilities are essential to the Defense-in-Depth concept of protecting critical assets. Having an electronic boundary around the ICS is not sufficient to protect critical assets from unauthorized access, because for each protection put into place in a network environment, threat actors can find a method around it. The concept of Defense in Depth says a system must detect and alert an organization of an intrusion early on so they can take defensive action before critical assets are breached. Most IT organizations have some level of monitoring at the corporate level, but they rarely implement it in the ICS networks.

Without system monitoring in place, intruders could breach the system and no one would know of the intrusion before they achieved their objective, if they know at all. While the ICS vendor community is

3. Caswell, Jayne, *Survey of Industrial Control Systems Security*

becoming more aware of the need for centralized monitoring of ICS security, the integration of standard monitoring capabilities into ICS is in its infancy. Asset owners can and should take action to ensure that security personnel and OT operators know of changes to systems or behaviors that indicate a potential network intrusion.

Organizations can monitor networks and collect information about networks in many ways, such as using centralized syslog servers for Linux and network devices and to centrally collect Windows Events using WinRM (Windows Remote Management) and WEVTUTIL (Windows event log tool) utilities. However, organizations must review these events (logs). Solutions, such as security information and event management (SIEM) products, combine security information management (SIM) and security event management (SEM) and can collect, log, and correlate information from multiple sources and alert on anomalous or specified activity and/or provide real-time analysis. Canaries and honeypots/honeynets can also flag any unauthorized intrusion, and asset owners should consider them for use in high criticality/high risk areas.

2.7.1 Intrusion Detection and Prevention Systems

ICS environments provide a unique opportunity when considering protection mechanisms to place on the network: despite considerable network traffic, that traffic is very predictable. For example, in a typical ICS environment, the PLC communicates in a standardized way with the HMI and the historian; all applications and services on the process control system (PCS) network are known (or should be); and the protocols, web traffic, and proprietary traffic are known and predictable.

Asset owners can use an IDS solution to easily monitor and create alarms for any traffic outside normal operations. An IDS is based on the passive monitoring of network traffic. Expected network traffic is deterministic, and deviations are used as triggers for alerting. Simple rules can be written to monitor for IP sources and destinations, protocols, lengths of packets, and so forth. Also, many ICS vendors can provide traffic signatures for their equipment.

IPS solutions are in-line with firewalls or ICS equipment and can take action by blocking traffic that does not meet the defined rules. Many vendors and asset owners become nervous about using IPS, because it has the potential to stop a process (and therefore stop operations). However, because of the deterministic nature of ICS traffic, they can be tuned to trigger only on extreme anomalies.

IDSs/IPSs are a vital part of the Defense-in-Depth strategy, because so many inherent vulnerabilities are within the ICS network, and an individual can only do so much to monitor potentially unwanted traffic. An IDS/IPS provides an automated way to watch for and respond to the unexpected. However, IDS/IPSs cannot do everything, as shown in Figure 8.

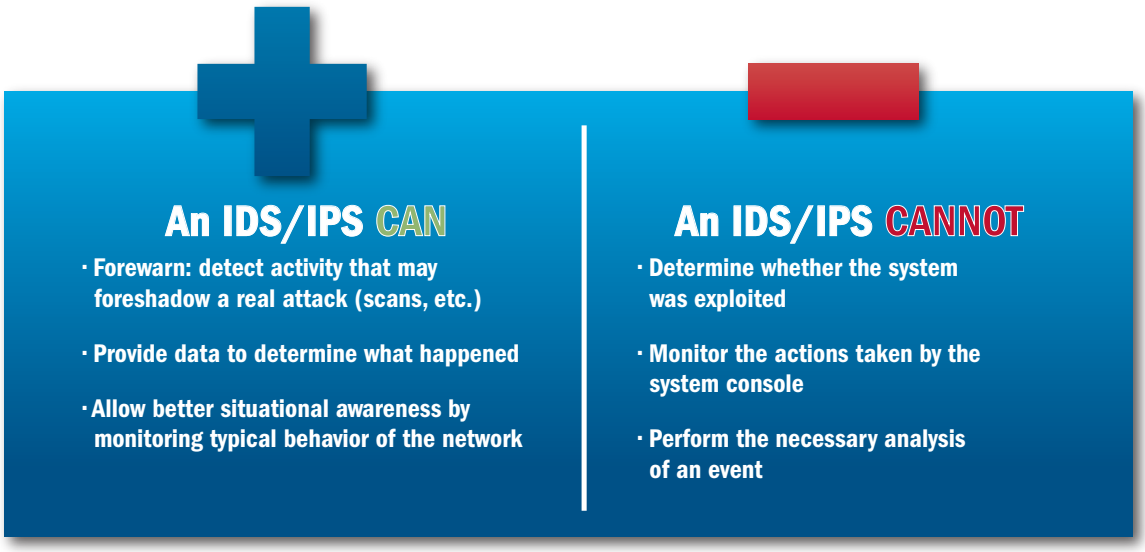

Figure 8. IDS/IPS limitations.

An IDS is not limited to being network-based. A host-based IDS (HIDS) monitors the state of the computer. Application level detection systems (ALDSs) monitor an application's state.

Using IDS to monitor the network and/or system is not a "silver bullet." An IDS is more of a warning or audit system. IDSs can alert to possible misconfigured systems on the network and will alert when an intruder is compromising a system using a known method. It often takes more than one method or device to provide the most complete information about an event. All methods of intrusion detection involve the gathering and analysis of information from various sources within a computer, network, and enterprise to identify possible threats posed by hackers inside or outside the organization. File integrity checking tools are common in most environments.

Open Source Security (OSSEC) is an Open Source HIDS that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response. It runs on most operating systems, including Linux, Mac OS, Solaris, Windows, and others. The main issue with any HIDS in any environment (especially ICS) is the computer resource penalty incurred to get a particular user required security level. Table 3 identifies signature versus anomaly detection and their characteristics.

Table 3. Signature versus anomaly-based detection.

Detection Method Characteristics	
Signature-based Detection:	· Watches for specific events · Only looks for what it has been told · Can deal with any known threat · Unaware of network configuration changes · Highly objective inspection · Predictable behavior · Easy to tune manually
Anomaly-based Detection:	· Watches for changes in trends · Learns from gradual changes · Can deal with unknown threats, but any intrusion is subject to a false negative · Sensitive to changes in network devices · Subjective, prone to misinterpretations · Unpredictable behavior · Must trust the system completely

Table 4 describes considerations for using signature-based detection versus anomaly-based detection.

Table 4. Detection basis considerations.

Selection Considerations	
Signature-based Detection:	• Scans network traffic (packets) for known patterns • Only scans traffic on or from its home network • Can scan both sides of a conversation • Could be reactive and block traffic (IPS mode) • Does not differentiate traffic - often does not know whether a system is Windows, Linux, or a PLC
Anomaly-based Detection:	• Must teach system to identify "normal" network traffic (and what if learning period includes attacks?) • Detects deviations from normal behavior • More difficult to spoof • Needs no foreknowledge of attack signatures • May raise more false positives • Very hard to implement in a dynamic environment

Like firewalls, organizations must strategically locate IDS sensors to obtain the most value. As a general rule, they should locate them in high traffic locations and/or between security boundaries or networks with sensitive information.

Network-based IDSs/IPSs scan the network topology for "bad" traffic while HIDSs/ALDSs monitor each host and report to a central logging facility. The central logging system needs to be a very secure system to prevent bypassing and perhaps inactivating the systems. Attach an NIDS/IPS to the modem pool and wireless access points. Statistically, this is the most often forgotten entry point for "bad" traffic.

Organizations should view alerts as similar to process alarms. Process alarms alert operators to process conditions that warrant attention. Likewise, intrusion detection alarms alert network operators to network conditions that warrant attention. Use basic logic when configuring alarms and alerts. For example, if a user typically logs on between 0800 and 1600, and for any reason logs on at 0300, the IDS should detect this activity and generate an alert. Anomaly detection is difficult to implement in a typical IT network because of the dynamic nature of the environment; however, ICS networks and systems' predictability lends itself well to the use of these technologies.

Potential complications with using IDS/IPS include the fact that it takes a significant amount of work to write rules and requires thorough testing to ensure that the rules function properly. In addition, an IPS can modify/drop legitimate packets if the rules are written improperly. This could prevent alarms from reaching the operator or configuration changes from reaching their intended destination; therefore, it may require great care and significant testing to ensure that unintended consequences are not introduced into the system. Many organizations use IDS that have quite sophisticated functionality for managing security zones for this purpose.

2.7.2 Security Audit Logging

Security audit logs provide information about login activity, resource use, file modifications, and other security-relevant information. Without properly configured and maintained auditing and logging practices in place, incident response teams often cannot determine the significance of a potential event. Properly configured audit logs at the network, host, and application levels provide critical information for determining how an incident occurred, the impact and scope of the issue, and how best to deter future events.

Comprehensive log management and analysis policies establish the minimum requirements for devices, operating systems, and applications. Security control settings and user access controls enforce those requirements. When asset owners do not configure systems and applications to capture key events, they fail to capture important event data, and incident response teams may not have sufficient information to determine the cause of an event. A baseline of expected traffic and process functionality for normal and off-normal operations and system use allows security, process control, and control systems operations personnel to isolate unusual data traffic or user actions that may indicate potential security-impacting events.

Newer operating systems and applications provide more detailed configuration and event auditing options than their legacy counterparts; however, using the default configuration for most operating and application logs only provides minimal audit capabilities, and organizations may miss a critical event. It is important that control system administrative and security personnel perform a review of all audit capabilities and configure the systems to provide the data needed to both capture all potentially relevant events and to ensure that the settings do not generate unneeded logs that can overwhelm system storage capacities. Also, default configurations may allow data to be overwritten; therefore, export all logs to a central server or event management capability to ensure that they are available if needed.

2.7.3 Security Incident and Event Monitoring

SIEM technologies support the incident response process, but they can support ICS operations as well. When configured and analyzed correctly, the data can assist in predicting equipment failure, equipment capacity, and failure points as well as providing security information. Asset owners can configure them to provide alerts when a potential security intrusion occurs, and they can aggregate a vast amount of audit data that accumulates from ICS components. By providing visibility into aggregated security data, SIEMs can minimize incident response time.

A SIEM centralizes data from network devices, operating systems, applications, and databases within complex environments, such as control system networks. It streamlines the audit log review process, by porting logs from multiple systems into one solution that eliminates the time and effort required for manual log reviews. Organizations can set up a SIEM to integrate multiple log formats from widely distributed sources, and collect the information both remotely and automatically. The SIEM can also integrate IDS/IPS information and scanning results and generate alerts on identified traffic patterns. A SIEM's analysis engine speeds data processing and formatting time, making it cheaper and easier to review functional, operational, and security data. In addition, using a SIEM provides the ability to select specific events for compliance reporting, root cause failure analysis, and incident detection.

2.8 Vendor Management and Security

Vendors represent a special case within the framework of a strong Defense-in-Depth program. In the last several years, vendors have become aware of the importance of cybersecurity in industrial control solutions and, in many cases, have incorporated security into their product life cycle to meet emerging market demands. Although not every vendor is taking this approach, many of the leading vendors are. They have seen the cyber vulnerabilities associated with ICSs—especially after the publicity of exploits such as Stuxnet, SQL Slammer Worm, and others. One should not assume, however, that vendors always follow stringent security practices. The organization should present and address requirements for control system security in great clarity early in the procurement process. This is not only advantageous to the asset owner but also provides the vendors specific guidance on what functionality they need.

Over the last several years, asset owners and vendors have benefited from a tremendous amount of work done in developing procurement guidance. This guidance has resulted in progress toward securing several vendor solutions applicable to many different sectors. The Department of Energy (DOE) developed procurement language considerations to help ensure that products meet requirements. This guidance document provides baseline procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process. In addition, a more generalized procurement language docu-

ment for ICS is available. Asset owners from all sectors may use this procurement language for purchasing equipment, for managing and monitoring ICS security developments, and to ensure the solution meets the organization's requirements.

2.8.1 Supply Chain Management

The supply chain represents a significant risk to ICS systems. ICS manufacturers and software developers create their products in many different locations around the world. Ensuring the security of the system or application throughout its development life cycle is impossible for most ICS operators. Purchasing commercial off-the-shelf (COTS) technologies increases the likelihood of receiving nongenuine equipment. Also, ICS-CERT is aware of reports related to equipment with embedded unauthorized code in its firmware or operating system that provides a back door into the equipment or allows the program to "call home" once installed. To help mitigate these threats, asset owners must pay careful attention to procurement contract arrangements, quality control, and validation of performance to specifications processes. In addition, exhaustive testing, including vulnerability scanning, is an important task to perform before installing systems in production environments.

NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (April 2015)," defines the supply chain compromise as, "An occurrence within the Information and Communications Technology (ICT) supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service."

Supply chain compromises have occurred in the ICS/IT environment for a number of years. A typical compromise includes some or all the following:

- Network or computer hardware with malware installed,
- Software or hardware with malware inserted by various means,
- Vulnerabilities in software applications and networks within the supply chain, and
- Counterfeit computer hardware.

Of particular concern with regard to supply chain risk is the information regarding the operation of sensitive hardware/software that vendors generally provided on their web sites. Threat actors can easily find default passwords, operational instructions, vendor manuals, and information provided by the users of software and/or hardware on the Internet (in white papers, blogs, social media, and so forth). Adversaries armed with this information are well equipped to compromise these systems.

In the long term, ICS owners should work with vendors and encourage them to design ICS using attack-resilient algorithms and architectures and to design and operate control systems to survive an intentional cyber assault with no loss of critical functions. The goal should be to design systems whereby even if intruders manage to bypass some basic security mechanisms, they will still face several control-specific security devices that will minimize the damage done to the system.

2.8.2 Managed Services/Outsourcing

Many organizations utilize managed services and/or outsourcing for functions that require highly specialized technologies and/or skills. It is not uncommon for organizations to outsource many IT security functions such as incident response forensics, cyber vulnerability assessments, risk management, supply chain management, or other functions that they rarely use or that requires expertise they don't have. The primary advantage of outsourcing is that it is cost effective to the organization. Maintaining a full-time forensics staff, for instance, is costly due to their high level of expertise, yet an organization needs them during incident investigations.

A service level agreement (SLA) is a common means of identifying the service requirements for the outsourced firm's responsibilities. If the firm does not meet the requirements of the SLA, the organization reserves the right to terminate the contract. When engaging with an outside entity for security services, it is important that both sides agree on roles, responsibilities, incident handling and reporting, and also the security of any interconnections, remote access policies and procedures, or interfaces that a user may require. In addition to the SLA, organizations should develop a memorandum of understanding/memorandum of agreement (MOU/MOA) and interconnection security agreement (ISA) to outline the specific management and technical requirements for the services.

When engaging with an outside party to perform technical assessments or testing, all parties should establish and agree on rules of engagement (RoE). Cyber vulnerability assessments typically require some level of passive or active scanning or testing on the target systems, which means the assessors must either access or watch others access critical cyber assets within the control system environment. The assessment team lead works with their organizational counterpart to ensure that the testing activities do not interfere with client operations and also to agree on actions to take and notification protocols should the activity cause any problems for the organization. The RoE includes direction about what activities may take place in what systems and who may perform those activities. It includes decisions about whether testing takes place within the primary (active production) control system or some credible substitute such as a backup or secondary control system, a test network, or stand-alone system. Avoid active scanning production control systems, as they can cause operational issues or create a denial-of-service condition. Passive activities, such as network sniffing, may be adequate. If using a substitute system, compare it to the active system to ensure that they are identical in operation. The assessment team and the organization will also need to agree on who will have their "hands on the keyboard" during testing—especially when active (production) control systems are the target. Local personnel should perform all tests on an active control system at the direction of the assessment team.

2.8.3 Leveraging Cloud Services

Some ICS organizations are using cloud services for data storage and are considering other ways to make use of them for additional services in support of their ICS architectures. From a security perspective, any portion of any externally hosted ICS architecture must provide a level of security hardening commensurate with the criticality of the function it hosts. In addition, the organization must consider ICS information integrity, security, and confidentiality, as well as the functional and operational details associated with recovery, event/incident management, failover, forensic support, monitoring, and other operational sequences that require special support by the cloud-hosting service provider. Other areas that organizations can overlook when considering shifting resources to the cloud are the reliance on Internet service provider (ISP) connections on premises and the potential bandwidth increases that can take place. Legal instruments and the use of SLAs are important because all operational support requirements must be explicitly identified to ensure that the expectations for support by the cloud providers, ISP availability, and bandwidth capacity are fully covered to avoid surprises later if an operational issue arises. There are other issues to consider as well, including the effects of load balancing and other possible impacts if the cloud provider experiences a surge in the use of their available resources.

2.9 The Human Element

Organizations face many challenges in managing the human factor within ICS organizations. Large and complex systems are susceptible to mistakes made by inexperienced or untrained personnel, as well as the activities of malicious insider threats.

2.9.1 Policies

Clear, actionable policies are necessary to lay the framework for rigorous controls that secure ICS technologies and also provide the governance needed to manage human factors. Policies lay the framework for detailed procedures and set the expectations of the organization with regard to the functions performed. Policies outline the rules with regard to securing the ICS—stating expected rules of behavior and also required controls. Policies outline what must and must not occur and set forth sanctions for non-compliance.

2.9.2 Procedures

Historically, security management was the responsibility of the corporate IT security organization, usually governed by operating plans and procedures that protect vital corporate information assets. As ICSs become part of larger conjoined network architectures, organizations must update security procedures to cover the control system domain as well.

Organizations should design procedures to state how personnel should conduct a particular process, or configure a particular system, to ensure secure functioning and provide a standard, repeatable means to accomplish a task in a safe manner. ICS security procedures also allow an organization to quickly train new personnel and to ensure that they follow all required regulations and standards uniformly across the OT space. ICS security procedures also instruct ICS operators on the steps to take in order to protect the ICS from a cyber-based intrusion. Network-based security procedures are especially important for the ICS domain, because the use of unique vendorspecific protocols and legacy systems may hamper efforts to protect mission critical systems.

2.9.3 Training and Awareness

Many organizations overlook security training and awareness activities more often than many other areas in ICS operations. OT owners and operators rely on their intimate system and process knowledge to ensure the proper functioning of the system, and they usually allocate training time and resources only for system functionality-related purposes. As ICSs become more interconnected and cyber threats and vulnerabilities rise, it is critically important for organizations to ensure that they require and support ICS security-specific training. IT implementers and OT operators should know what the indicators of potential compromise look like and what steps they should take to ensure that a cyber investigation succeeds. IT and ICS management should also know what they can do to make the system more secure so they can make informed decisions with regard to the cost/benefits of the protection measures they put into place.

3. SECURITY ATTACKS

Before deciding which Defense-in-Depth protections an organization needs for its ICS environment, it is important to understand the methods used by malicious actors to successfully attack these systems. Many of the techniques used by threat agents are the same as those used by security professionals to test networks and systems for vulnerabilities and to determine which Defense-in-Depth countermeasures to put into place. It is a constant "cat and mouse" game, and the challenge is to ensure that the information and systems accessible to infiltration are constantly monitored and updated to protect against ever-emerging threats.

3.1 Anatomy of a Cyber Attack

A cyber attack generally follows a process allowing the attacker to perform reconnaissance or discovery of the targeted business, then develops and executes the attack, and finally uses the attacker's command and control presence to extract data and/or achieve the attacker's goals on the target system. Figure 9 shows the sequence of operations for conducting an attack.

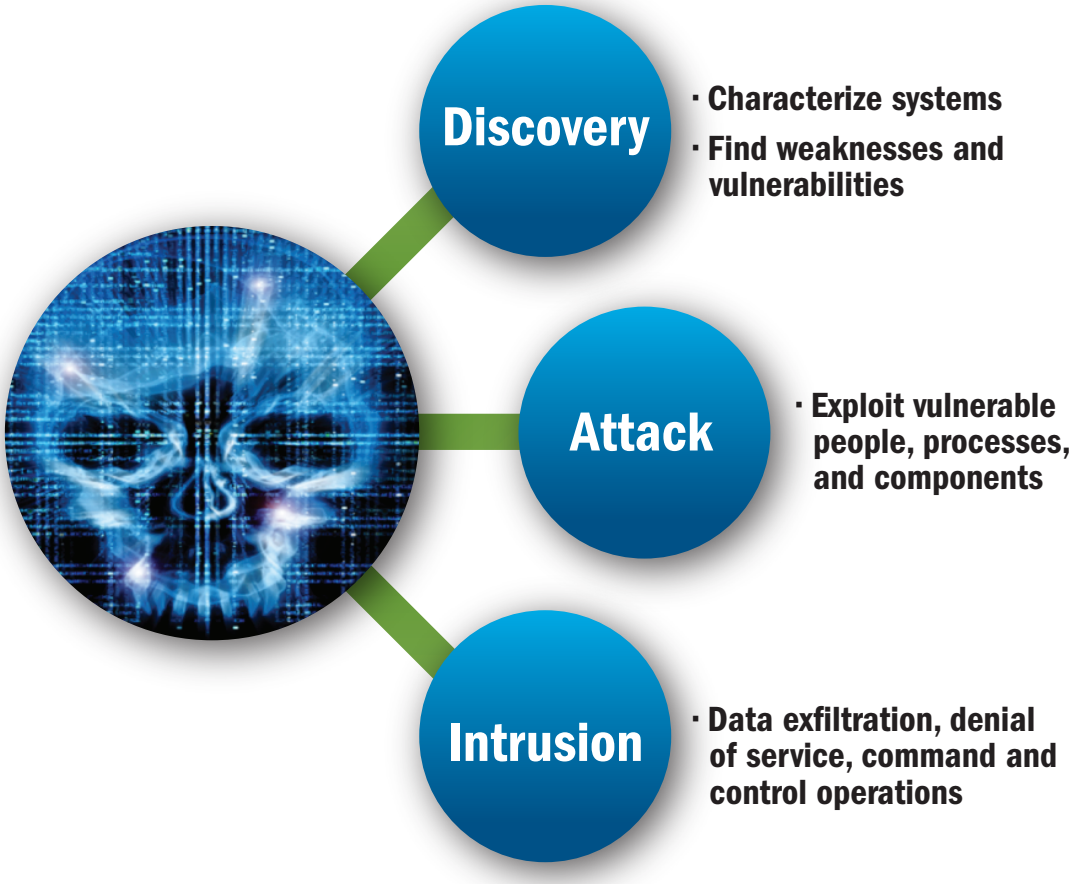

Figure 9. Attack sequence of operations.

In the discovery phase, a threat agent performs reconnaissance by probing the network perimeter to characterize the system, that is, determine if there is a firewall (and what type), what types of web or other Internet facing servers are used, and whether there are any open communication ports. The goal is to find any way possible to get into the system. They may also harvest publicly available corporate information (company principal's names and email addresses, photos that may show physical security barriers, support personnel names and numbers) to gain any advantage they can for social engineering or email-based attacks. Once they find a way in, they select an attack method and begin the actual attack.

Potential intrusion vectors can range from technical brute-force hacking using exploit tools to showing up at a site dressed as a worker. At this point, the goal is to exploit any and all vulnerable people, processes, or components to gain entry. Adversaries may have a direct target in mind or merely wish to deposit code on any available machine in order to maintain a presence on the network or system and to allow for future unauthorized access. Generally, the goal at this point is to maintain continued surveillance using a light footing, many times covering their attack tracks as they go.

Once they have found their access point, intruders can accomplish their intent through network intrusion—whether it is data exfiltration, creating a denial of service, or taking over command and control of the process, system, or the entire network. Many intruders leave residual back doors, accounts, or port openings for future or continued access. Once they have compromised a system, they may access it multiple times and may also use it to access other systems.

This section outlines how these elements are executed in a control system context, and also describes some common attack scenarios that intruders have used or can use against ICS environments. Some are well known in the IT security community as "tried and true" attack methods, and some are unique because the intruders specifically designed them for attacking critical infrastructure.

3.2 Discovery

Asset discovery allows a potential intruder to decide what systems to target, to gauge how easy it will be to launch an attack on a particular entity, and to find weaknesses in the target's security, which allows them to determine the best method for launching a successful attack.

3.2.1 System Characterization

Many ways are available to gather information about a site and its systems. Physical surveillance, public domain information aggregation, and scanning are the three most common methods in this phase.

Physical characterization methods can range from simply looking at the facility (looking for cameras, locks, fences, guards) to bolder approaches such as walking into the facility and asking for a tour or posing as a vendor, maintenance person, or even an employee's visiting friend. It is amazing how much information one can gather this way. A pile of boxes outside a facility can give a would-be intruder insight into what new equipment the asset owner is installing. Tours can provide a wealth of information, including how well an organization has physically protected a particular site; what systems are on site and where they are located; and how the operations are conducted. Another way to get information is to befriend an insider. A seemingly innocent conversation about work can allow an intruder to gather a wealth of information about the control systems at a site and how well the organization protects them.

Electronic asset discovery methods can range from simply collecting and aggregating seemingly random information accessible through the public domain to using freely available tools to fingerprint systems.

Public domain information, such as lists of locations, vendor partnership announcements, requests for proposals, lists of company principals and their contact information, contact lookup engines, job openings, and even holiday closure calendars, can provide an intruder with spear-phishing targets and content, times/dates when a plant or office is unattended (and, therefore, not closely monitored), device-specific intelligence, and also gaps in a company's skill sets or planned system- or security-focused projects.

Threat actors can easily obtain IP address ranges through domain registry searches. Crafting an Internet query designed to return an error message can also yield information about the system (for example, database errors often indicate that someone is using the database). Free tools, such as nMap (Network Mapper), can tell an intruder what devices, ports, protocols, and services are open; whether a firewall is in place; what type of firewall they use; and even the name of the network where they keep it.

Intruders use "war dialing" to scan a range of telephone numbers for modem connections. Attackers can use a range of potential telephone exchanges common to an area or published on a company web

site to pinpoint the systems. "War driving," which is riding or walking around a facility and scanning for unsecured wireless access points, is a combined electronic/physical discovery method that a would-be intruder can also use.

3.2.2 Determine Weaknesses and Vulnerabilities

Once the attacker has determined potential intrusion vectors, they determine what weaknesses and vulnerabilities are inherent in the targeted system. Many well-known security challenges inherent in control system environments provide an intruder with a "target-rich environment" to choose their intrusion vectors.

Poor configuration management is one of the most common ways that an attacker can find an opening into the control system domain. General purpose OS platforms provide numerous processor and network services that automatically run by default. The result is unmonitored, open ports that are vulnerable to network exploits and actively executing code that may be subject to attacks such as buffer overflows. Leaving these unneeded ports and services active allows easy access for would-be intruders.

Because of the high or constant availability and critical response time requirements inherent in ICS, any change to the system necessitates exhaustive testing for software and security updates. Schedule all patching or update activities far in advance and permit them on a very infrequent basis. In addition, ICS components may not tolerate security software because of critical timing requirements. Control system components are often so processor-constrained that running security software itself creates unacceptably high delays in response, threatening system stability. The result is outdated OS revision levels and outdated or no malware protection software. Even if antivirus software is up to date and configured for proper execution, ICSs built on standard platforms are vulnerable to newly discovered malware threats that, once again, cannot be patched in a timely fashion.

Technology-related vulnerabilities within TCP/IP-based control system environments leave critical networks and systems open to compromise. Examples of vulnerabilities in IT system technologies that could migrate to control system domains include the susceptibility to malicious software (including viruses, worms, and so forth), escalation of privileges through code manipulation, network reconnaissance and data gathering, covert traffic analysis, and unauthorized intrusions into networks, either through or around perimeter defenses. System vulnerabilities also include hostile mobile code such as malicious active content involving JavaScript, applets, Visual Basic (VB) Script, and Active-X. With a successful intrusion into ICS networks come new issues such as reverse engineering of control system protocols, exploits leveraging vulnerabilities on operator consoles, and unauthorized access into trusted peer networks and remote facilities.

Outdated, inherently insecure protocols, such as FTP and Telnet, are generally used for ICS operations. Personnel often send passwords in the clear. One standard protocol for data communication between control devices, object linking and embedding (OLE) for process control (OPC), must run without authentication. SCADA and ICS communication protocols for control devices, such as Modbus/TCP, Ethernet/IP and DNP3, do not typically require authentication to remotely execute commands on a control device, and no encryption options are available.

Most devices lack even the most basic access control separating system software mode versus application program mode. Server and terminal authentication is often nonexistent or completely ineffective. Differentiation of access privileges between administrators and end users is also generally unavailable or not implemented.[4]

Sometimes threat actors will plan a multi-pronged attack. For example, an intruder may decide to use a targeted spear-phishing attack to infiltrate the corporate network and use it as a vector into the control system architecture. The intruder may use both war dialing and war driving to find open modem connections and wireless networks connected to ICS and then use common vulnerabilities in the operating systems, applications and/or databases discovered while scanning to use specific exploits tailored for a particular system.

4. Caswell, Jayne, *Survey of Industrial Control Systems Security*

3.3 ICS Attack Methods

This section describes some common intrusion methods, many of which intruders have launched against critical infrastructure sectors across the world. The ICS-CERT 2014 Year in Review reports the following vectors as the most prevalent for that fiscal year:

- Weak authentication,
- Network scanning/probing,
- Removable media,
- Brute force intrusion,
- Abuse of access authority,
- Spear phishing, and
- Structured query language (SQL) injection.

3.3.1 BlackEnergy

BlackEnergy is a crimeware toolkit that has evolved significantly since it emerged in 2007. Recent versions of the toolkit use social engineering to trick a user into opening an email or a document attachment that drops a Trojan or infected legitimate executable file on the target computer which results in the installation of a malicious software component. The malware can infect a system by exploiting a standard feature in Windows that elevates the user privilege of a system file, allowing execution of the command executable with administrative privilege—even if the user is not a member of the administrator group.

This attack scenario is targeting various specific vendor HMI products. Organizations with HMI systems directly connected to the Internet are the most susceptible. The malware is highly modular, and threat actors can customize it for deployment to each victim site. Once an HMI host becomes infected, a command and control component executes to perform additional attack operations, as well as communicate back to the attacker with data gathered and to obtain additional attack modules that search out additional resources within the network for new targets of opportunity.

An alert posted by the DHS ICS-CERT provides detection and mitigation recommendations to determine if an intruder has infected a system with BlackEnergy. From a Defense-in-Depth perspective, users should follow guidelines provided in the alert to address the security practices needed to protect the business from this and other attack campaigns.

3.3.2 Unauthorized Access Attacks

Many control system architectures are designed to have remote connections using either publicly accessible telephone networks or dedicated lines for modem access. When left unsecured, an attacker can connect remotely with little effort, and the remote connection may be difficult to detect (assuming little or no monitoring or logging). Secured modems configured with user IDs and passwords are still susceptible to compromise through the use of war dialing and brute-force cracking, because it is often the case that there are no automated account lockouts based on repeated unsuccessful login attempts. This was once considered an obsolete reconnaissance method; however, it is seeing a rapid resurgence due to the use of Voice over Internet Protocol (VoIP) or legacy systems using dial-up for remote control on many critical systems. Published tools have created software leveraging VoIP systems that can war-dial up to a thousand numbers hourly.

In addition, field devices are part of an internal and trusted domain, and thus access into these devices can provide an intruder with a vector into the control system architecture. By gaining access into a field device, the intruder can use the trusted relationship associated with the sensor network to tunnel back into the control system network. Recognizing that field devices are an extension of the control domain, intrud-

ers can add these field devices to their list of viable targets to investigate during the reconnaissance and scanning phases of the attack. Although such attacks are not considered possible across serial connections, the increasing use of standard networking protocols in remote devices requires attention.

If an intruder compromises a device and can exert control over the device, he or she can begin to execute a number of procedures including scanning back into the internal control network, altering the data that go to the control master, or changing the behavior of the device itself. If the intruder decides to scan back into the control network, which capitalizes on the trust between resources, it may be possible to use the actual communications protocols for the entire control system domain. This is of particular advantage to the intruder because asset owners do not usually monitor the device-level connections for malicious or suspect traffic. Some intrusion detection systems (IDSs) can be updated with industrial control systems signatures to help defend control domains. Usually, these systems are signature-based and will trigger on seeing recognized malicious traffic. In lieu of viable signature, IDS can be deployed to trigger on nonspecific traffic, or upon seeing traffic that is not expected or unusual.

3.3.3 Database and SQL Data Injection Attacks

Database applications have become core application components of ICSs and their associated record keeping utilities. Traditional security models attempt to secure systems by isolating core components and concentrating security efforts against threats specific to computers or software, not taking the database into consideration. Databases within ICSs use generally independent systems that rely on one another for proper functionality. The high level of reliance between the two systems creates an expanded threat surface.

Databases used by ICSs often connect to databases or computers using web-enabled applications located on the business network. Virtually every data-driven application has transitioned to some form of database, most using SQL, with many having web interfaces that may be vulnerable to typical web exploits like cross-site scripting (XSS) or SQL injection.

The information contained in databases makes them high-value targets for any attacker. When control system databases connect to business or financial databases or to computers using applications to access the data, attackers can exploit the communications channel between the two networks and bypass the security mechanisms used to protect the control system environment.

Malicious code injected into a database with valuable data can have far-reaching effects, especially in a control system environment where data accuracy and integrity are critical for both business and operational decision-making. The cascading effect of corrupted database content can impact data acquisition servers, historians, and even the operator HMI console. ICSs are more adversely affected by SQL injection than are many general IT databases, because they are so reliant on data availability and integrity. Moreover, compromise of key trusted assets, such as a database, creates additional resources the threat actors can use for both reconnaissance and code execution.

Given the reliance of ICS on the storage, accuracy, and accessibility of command and control data, as well as the prevalence of SQL databases on these types of networks, standard SQL injection techniques used against control system components pose a major threat to control system security.

3.3.4 OPC/DCOM Attacks

A campaign called Operation Dragonfly utilized a multi-pronged intrusion chain to establish a presence on the network, perform reconnaissance, and establish a command and control capability to phone home to the intruder and allow them to launch other specific attack tools. It employed the "Havex" Remote Access Trojan (RAT) within targeted spear-phishing campaigns against industry asset owners, and it used a watering hole campaign to circumvent the normal practice of users accessing vendor resources. The next stage in the intrusion involves the enumeration of the asset owners' OPC servers, specifically targeting a vulnerability in the OPC Classic protocol. This provided the threat actor with the potential capability of performing deep discovery into the ICS, often finding legacy equipment and software and using the information to support the development of additional intrusion vectors that the intruder could use.

Over the last several years, more and more organizations have started to use underlying services in these environments, some of them being the OLE, distributed component object model (DCOM), and remote procedure call (RPC). OPC is a real-time data communications standard based in these services. Many installations are moving away from the Microsoft-based OPC model; however, many still commonly use OPC for efficient connectivity with diverse ICS equipment. Also, organizations still widely deploy OPC on mission critical components of a control system environment, such as HMI workstations and historians, highlighting a continued dependency on OPC. A recent study showed that many ICSs and their processes would have permanent historical data and production time loss if an OPC service was to become unavailable.

OPC standards and application programming interfaces (APIs) that are common in control system environments are OPC Data Access, OPC Alarms, OPC Data Exchange, and OPC Data-XML. All OPC standards and APIs are widely supported and used in Windows editions, and there are a wide variety of security implications and vulnerabilities associated with the use of OPC services and standards. Vulnerabilities range from simple system enumeration and password vulnerabilities to more complex remote registry tampering and buffer overflow flaws. These vulnerabilities expose many ICSs to critical risks such as the installation of undetected malware, denial-of-service attacks, escalated privileges on a host, and/or the accidental shutdown of ICSs because of an overload flaw.

Even though many of these vulnerabilities have recommended alternate solutions or available workarounds, their deployment within ICS architectures have not always resulted in success. For example, Microsoft has updated its recommended practice for distributed programming toward a service-oriented architecture based on the .NET framework; however, the long life cycles of ICSs result in organizations still using OPC and DCOM without vendor support.

3.3.5 Man-in-the-Middle Attacks

ICS environments have traditionally been considered protected because they are in a completely separate environment from IT systems ("air gapped"). In ICS networks, asset owners often do not secure the data that flow between servers, resources, and devices because they assume the data reside on a "protected" network. With more and more organizations connecting ICS networks with business systems, security issues arise from this assumed trust, including the ability for an attacker to reroute data in transit on a network, to capture and analyze critical traffic in plaintext format, or the ability to reverse engineer control protocols in order to gain command over control communications. By combining all these, an attacker could assume exceptionally high control over the data flowing in a network and ultimately direct both real and "spoofed" traffic to network resources in support of the attacker's desired outcome. To accomplish this, the attacker executes a Man-in-the-Middle (MitM) attack, as Figure 10 shows.

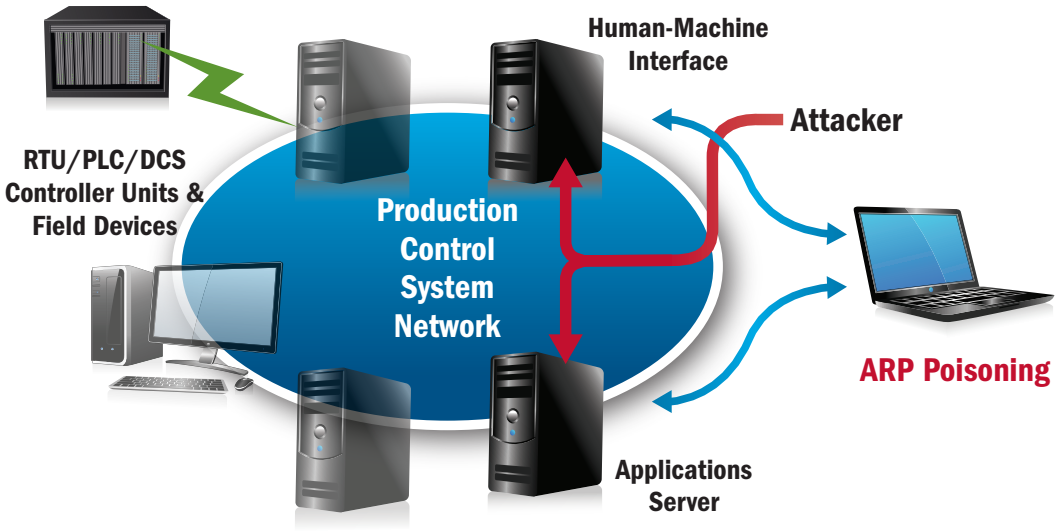

Figure 10. Man-in-the-Middle attack.

The management of addresses in a network, be it a control system or a business LAN, is critical to its effective operation. Address Resolution Protocol (ARP) maintains correct routing by mapping network addresses to physical machine addresses (MAC addresses). Using ARP tables in each of the network devices ensures that computers and other devices "know" how to route their traffic when requesting communication. Manipulation (or poisoning) of the ARP tables is the key goal of the threat actor, because poisoning the ARP tables can force the routing of all network traffic (including control traffic) through the computer the attacker has compromised. This forces all resources on the network to "talk" to the rogue device that the intruder is using instead of the proper machine or device without knowing they are communicating with the attacker. Moreover, the intruder can see, capture, replay, and inject data into the network and have it interpreted as though it were authorized and originating from a trusted source.

Assuming a threat actor has gained access onto the control systems network using any of the aforementioned attacks or others, they will use network reconnaissance to determine what resources are available on that network. If the goal of the intrusion is to gain access to and compromise the control domain, the asset owner can capture (sniff) plaintext traffic and take it offline for analysis and review. This allows the intruder to view and re–engineer packet and payload content, modify the instruction set to accommodate the goal of the intrusion, and re-inject the new packet into the network.

By using ARP poisoning to collect traffic, the threat actor can establish and maintain control over the communications within the network. If the intruders choose, they can acquire and analyze unique control system protocols, and can see, capture, and manipulate control data. The time required to reverse engineer key control data and to manipulate that data for nefarious purposes can vary depending on the skill of the threat actor and the complexity of the data. By taking the data offline, the intruder is now able to work at a tempo that is most appropriate for him or her.

In any environment, MitM exploits are exceptionally dangerous; in the ICS networks, this mode of attack could be catastrophic. Common vulnerabilities in ICSs such as weak authentication protocols or poor integrity checking in firmware could be exploited by a MitM exploit. By assuming control of a key information resource and performing a MitM exploit, an unauthorized intruder could:

- Stop operations.
- Capture, modify, and replay control data.
- Inject inaccurate data to falsify information in key databases, timing clocks, and historians.
- Replay normal operational data to the operator HMI while executing a malicious exploitation of the field device (including preventing the HMI from issuing alarms).

3.3.6 Social Engineering Attacks

As a general rule, most people trust other people—and the "black hat" hacker community knows it. They have learned to prey on the positive and very human response to personal contact, whether by sending an email that seems to be legitimate but contains an embedded malicious payload or posing as a trusted vendor or fellow employee in order to gain access to a system. When asset owners kept ICSs contained within a stand-alone environment, they did not consider malicious code much of a risk; but as ICS becomes more and more interconnected, ICS operators and administrators need to become more and more vigilant to ensure that they do not accidentally unleash a potentially devastating virus or worm into the system.

Malicious actors increasingly use phishing and spear-phishing (directed email) exploits to target control system managers and operators with the intent of introducing malicious code into the ICS environment. It has become critical for system designers to segregate and control any connectivity between business functions such as email and ICS operations.

Equally important is ensuring the physical security of the ICS by not allowing "piggybacking" (an unauthorized person entering a secure area without showing proper credentials); checking to make sure that maintenance workers and vendors provide proper identification before allowing them into an area that contains ICS and monitoring their activities while on site; and disallowing the use of any unverified foreign media (for example, USBs, CDs) on the system.

4. RECOMMENDATIONS FOR SECURING ICS

To reduce risk to ICS networks and systems simply by deploying IT security technologies into a control system environment may not be a viable solution. Although newer ICSs often use the same underlying protocols that are used in IT and business networks, the nature of the control systems' reliance on functionality (combined with operational and availability requirements) may make even ubiquitous security technologies, such as antivirus, inappropriate. Some sectors, such as energy, transportation, and chemical, have time-sensitivity requirements, so latency and throughput issues introduced by security solutions may cause unacceptable delays and degrade or prevent optimal system performance.

As control networks evolve from stand-alone domains to interconnected networks that coexist with corporate IT environments, system administrators must apply countermeasures that do not impede functionality. Understanding vulnerabilities and the associated intrusion vectors and how to exploit them are essential to building an effective security mitigation strategy.

4.1 Proactive Security Model

When protecting any information infrastructure, sound security practices start with a proactive security model (see Figure 11). Most security programs are reactive—applying security architectures and controls after an incident or compromise, which can be expensive and usually interrupts operations.

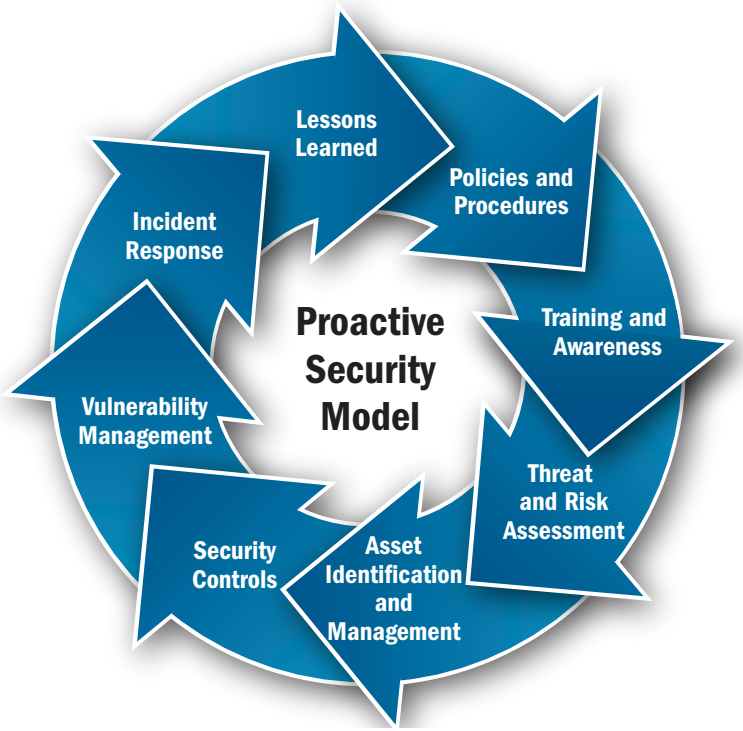

Figure 11. Proactive security as an iterative process.

The development of a robust Defense-in-Depth strategy begins with ensuring that policies and procedures are in place to guide expected behaviors and set guidelines to train individuals to ensure they do their jobs securely. A robust Defense-in-Depth strategy would identify threats and risks and assess those threats and risks for impact. The strategy would also map ICS architecture and develop a comprehensive inventory of all ICS assets. Having an accurate and well-documented inventory enables an organization to perform a realistic risk analysis of system operations, then apply security controls based on asset priority, and deploy effective security countermeasures to manage vulnerabilities. Asset owners should manage

incidents according to their impact and incorporate lessons learned throughout the process, making ongoing program and security control adjustments to ensure continuous improvement in the face of emerging threats and system modifications.

4.2 Five Key Security Countermeasures for Industrial Control Systems

Here are five key countermeasures that organizations can use to drive activities in ICS environments. Applying these steps will pave the way toward a more robust security environment and significantly reduce the risk to operational systems.

1. Identify, minimize, and secure all network connections to the ICS.
2. Harden the ICS and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
3. Continually monitor and assess the security of the ICS, networks, and interconnections.
4. Implement a risk-based defense-in-depth approach to securing ICS systems and networks.
5. Manage the human—clearly identify requirements for ICS; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide ICS security training for all operators and administrators.

4.3 Security and Risk Standards

There are a number of existing security and risk standards and guidance that organizations can use as a basis for securing and managing ICS. Depending on the critical infrastructure sector, these standards will apply to an organization as required by law or the authoritative governing body for that sector. Others standards and guides can help organizations develop a robust ICS security and risk management program based on industry best practices.

4.3.1 NERC-CIP

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system.

The NERC Critical Infrastructure Protection (CIP) standards provide a set of requirements and considerations for protecting bulk power system assets, but they are also applicable to other industries as best practices for protecting ICS.

4.3.2 NIST ICS Framework

NIST released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" on February 12, 2014. The framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to better manage cyber-related risk.

The NIST ICS framework provides a comprehensive set of recommendations for securing ICS. Organizations can use it alone or in conjunction with other NIST standards, such as its Special Publication (SP) series, notably:

- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach,"
- NIST SP 800-39, "Managing Information Security Risk – Organization, Mission, and Information System View,"
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and
- NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security."

4.3.3 Specific Subsector Guides

Many critical infrastructure subsectors have created guides to use when applying security solutions to ICS environments. These guides provide requirements and direction for protecting ICS assets that support specific functions within each sector.

4.3.3.1 Electricity Subsector Risk Management Process

DOE developed the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline in collaboration with NIST, NERC, and broad industry participation. The RMP is written with the goal of enabling organizations—regardless of size or of organizational or governance structure—to apply effective and efficient risk management processes and to tailor them to meet their organizational requirements. Organizations can use this guideline to implement a new program within an organization or to build on an organization's existing internal policies, standard guidelines, and procedures.

4.3.3.2 AWWA Process Control System Security Guidance for the Water Sector

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project to address the absence of practical, step-by-step guidance for protecting water sector PCSs from cyber attacks. The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber attacks. In an effort to provide water utilities with actionable tasks, they developed a Cybersecurity guidance tool to present recommended controls to users in a concise, straightforward manner. The AWWA guidance tool represent a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council.

4.3.3.3 Chemical Facility Anti-Terrorism Standards

DHS has released a final rule that imposes comprehensive federal security regulations for high-risk chemical facilities. This rule establishes risk-based performance standards for the security of our Nation's chemical facilities. It requires covered chemical facilities to prepare security vulnerability assessments, which identify facility security vulnerabilities, and to develop and implement site security plans, which include measures that satisfy the identified risk-based performance standards.

4.3.3.4 TSA Pipeline Security Guidelines

The Transportation Safety Administration (TSA) developed the Pipeline Security Guidelines with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties to provide guidance for securing natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. In addition, the guidelines apply to pipeline systems that transport materials categorized as toxic inhalation hazards (TIH).

4.4 Tools and Services for ICS Defense in Depth

DHS's ICS-CERT provides subject-matter expertise, tools, and services to assist organizations associated with all critical infrastructure sectors in the improvement of the security posture of their ICS assets. ICS-CERT provides evaluations and assessments at no cost to organizations. Depending on the complexity of the system, ICS-CERT can combine assessments during a single visit. ICS-CERT is not a regulatory agency, and therefore all assessments are considered collaborative exercises toward a common goal—raising the cybersecurity posture of critical infrastructure across the US.

4.4.1 CSET®

ICS-CERT offers the Cyber Security Evaluation Tool (CSET®), a self-assessment software tool for asset owners to conduct cybersecurity assessments. DHS developed the CSET for users to evaluate their cybersecurity posture based on standards and practices best suited to their sector. CSET maps user input to questions associated with selected cybersecurity standards and best practices. Multiple reporting options are available to meet the user's facilitated CSET assessments in partnership with various critical infrastructure stakeholders.

The CSET assessment process serves as an introductory-level baseline assessment within the ICS-CERT portfolio, but is not a prerequisite for more in-depth assessments. The CSET is available to asset owners as a no cost, downloadable, self-assessment tool that an organization can use on its own without the assistance of ICS-CERT personnel.

Figure 12 shows the high-level process that CSET assessments follow. To maximize the effectiveness of the CSET evaluation process, the asset owner should include subject matter experts from various disciplines to conduct the guided discovery-oriented evaluation of the entity's underlying control processes, procedures, policies, methodologies, and protective and detective security controls. These comprise the cybersecurity foundation for ensuring the availability and integrity of the control process.

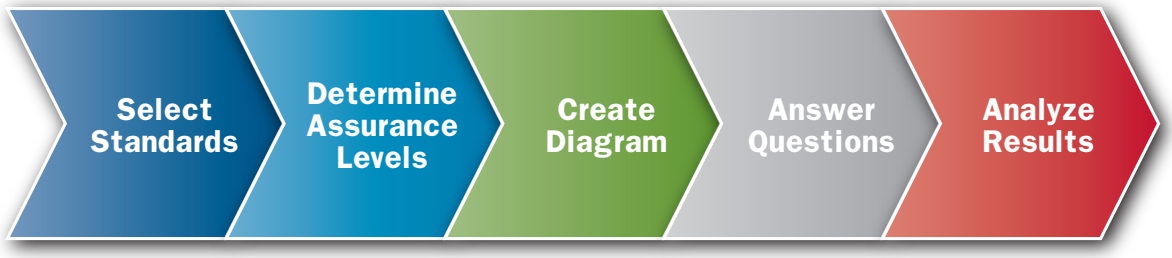

Figure 12. CSET Assessment High-Level Process.

CSET users answer a series of questions based on user-selected cyber security standards or best practice (NIST SP 800-82, NIST SP 800-53, CFATS, NRC, NERCCIP, and so forth) and the tool uses the answers to develop a report that baselines the cybersecurity posture of the target system.

A CSET evaluation usually takes about 1 day. An ICS-CERT subject matter expert will work with organizations to teach them how to use the tool and spend the day helping to answer any questions about the assessment and results. Typically, the CSET assessment includes both a key requirements assessment and a component assessment. The tool uses integrated network maps to provide a visual representation of the current security state of the system, identify the component targets for the assessment, and provide guidance on where to place cybersecurity protection mechanisms to provide the most value to the organization.

4.4.2 Design Architecture Reviews

A Design Architecture Review (DAR) is an assessment facilitated by ICS-CERT assessment team personnel who work interactively with the user to perform a deep-dive manual assessment and analysis of the operational process. The assessment focuses on the underlying ICS network architecture, integration of IT and OT teams, vendor support, monitoring, cybersecurity controls, and a review of internal and external connections utilized within the control systems environment. The DAR focuses heavily on three key areas:

1. ICS Network Architecture,
1. Asset Inventory, and
2. Protective and Detective Security controls.

DAR assessments generally take 2 days to complete (per control system architecture). ICS-CERT can conduct DARs independently of or in conjunction with CSET assessments; however, the DAR is more effective following a structured CSET assessment. A DAR is a comprehensive evaluation and discovery process, focusing on Defense-in-Depth strategies associated with an asset owner's specific control systems network. It provides the asset owner with a thorough evaluation of system interdependencies, vulnerabilities, and mitigation options. It examines information related to key ICS external connections and includes an in-depth review of control systems design documents, drawings, and architectures. The DAR process provides a detailed final report to the user that captures the key discoveries identified by the team and provides potential impact and recommended mitigations for each.

4.4.3 Network Architecture Verification and Validation

The Network Architecture Validation and Verification (NAVV) assessment entails the analysis of network traffic (passively captured) occurring within the ICS network. Using a combination of both open-source and commercially available tools, ICS-CERT is able to strategically visualize and perform analysis on the network traffic and device-to-device communications occurring within various ICS network segments to identify potential unauthorized or suspect communications. Threat data analysis of the traffic evaluates for indicators of known unauthorized attacks in the user's network.

NAVV assessments enable asset owners to:

- Verify the accuracy of ICS network diagrams.
- Identify potentially rogue/misconfigured devices or malicious data communications.
- Analyze data flows to ensure that boundary protection devices work as designed.
- Identify opportunities or areas to improve zoning and perimeter protections.
- Baseline the ICS network (including a protocol hierarchy and organization of network traffic).
- Gain practical knowledge of how to passively monitor and verify the communications occurring within their ICS networks.

The NAVV provides organizations with a view of network communication occurring within the ICS network infrastructure, in addition to those communications sourced from or destined to ICS network segments. ICS-CERT typically provides NAVV reviews as an extension to DARs, although this service is also offered independently.

5. CONCLUSION

As ICSs grow in complexity and connect to business and external networks, the number of potential security issues and their associated risks grows as well. The wide variety of attack vectors that target multiple resources on control systems can give rise to asynchronous attacks over an extended period of time and could target multiple weaknesses within a control system environment. Organizations cannot depend on a single countermeasure to mitigate all security issues. In order to effectively protect ICSs from cyber-based attacks, organizations must apply multiple countermeasures—thus reducing risk using an aggregate of security mitigation techniques. One should note that Defense-in-Depth measures do not and cannot protect all vulnerabilities and weaknesses in an ICS environment. They are applied, primarily, to slow down an attacker enough to allow IT and OT personnel to detect and respond to ongoing threats, or to make the effort on the attacker's side so cumbersome that they decide to put their effort toward easier prey.

Department of Homeland Security

Office of Cybersecurity and Communications

National Cybersecurity and Communications Integration Center

1-888-282-0870

Industrial Control Systems Cyber Emergency Response Team