**CHAPTER 28**

**Industrial Control Systems**

Industrial controls systems (ICSs) is a broad term used to describe several electronic control systems used in industrial manufacturing, power generation, water infrastructures, petroleum industry, and heating, ventilation, and air conditioning systems. Industrial control systems are subject to attack and exploitation because of the nature of how they were originally designed and operated. ICSs are used to control city water supplies, enrich uranium, and deliver oil around nations. ICSs control the valves, pumps, locking systems, doors, and devices of numerous automated systems.

ICS of the past were often designed with a life expectancy of ten years or longer. Where most information technology is designed to depreciate in value to zero over the course of just a few years, investment in industry is often expected to be depreciated and productive over the course of decades. This means information technology designed and implemented ten years ago may still be in operation today. The issue is that most if not all legacy ICSs and most modern ICSs were not designed with robust security in mind.

Many devices were developed with default administrative credentials that cannot be changed or web service portals subject to buffer overflow attacks and cross-site scripting. In addition to these design issues, the ICSs are typically not updated in a timely manner…if they are capable of being updated at all!

**Overview of the Information Assurance Approach**

The information assurance approach involving industrial control systems focuses largely on ensuring defense in depth by isolating and protecting vulnerable devices with more robust infrastructure. Allowing unfettered ICS connectivity to the open Internet is a recipe for disaster. The information assurance approach must focus on the device function and the need to protect the services the ICS supports. The ICS itself should be analyzed to determine what if any security features are available and if they are configured correctly. From there, securing the ICS is almost totally dependent on ensuring a strong information assurance program, ensuring strong continuous monitoring, ensuring strong information assurance integration into change management and configuration management, and ensuring several layers of managerial, operational, and technical controls exist between the ICS and the outside world.

• **Confidentiality** Many ICSs function as sensors and provide information about processes and operations to a central reporting hub. The impact of disclosing this information to the public or an adversary must be determined through an impact analysis.

• **Integrity** Integrity for a vast majority of ICSs is everything. The accuracy of a command or instruction to an ICS cannot be incorrect, and sensor information coming from an ICS must be correct. Information assurance teams reviewing ICSs must pay special attention to integrity impacts.

• **Availability** Also critically important to the vast majority of ICS is availability. While some ICSs such as SCADA systems are designed to be operated in environments with poor connectivity, the information assurance team must understand through a business impact analysis how much downtime can be tolerated and how much information can be lost.

• **Authentication** Authentication is becoming more important for ICSs. A decade or more ago, many ICSs did not have any authentication at all or only a rudimentary authentication such as a username. Today, ICSs must be protected as well if not better than network servers and bank accounts. The need to bring aging ICSs and ICSs that were not designed with security in mind into compliance is a real challenge.

• **Nonrepudiation** ICSs were not originally designed with nonrepudiation in mind. They were developed to ensure information was read or actions were performed. Many systems do not contain the logging and auditing required to provide the nonrepudiation of actions. This is another area the information assurance team will need to review and then determine the best approach to implement compensating nonrepudiation controls if needed.

**Industrial Control–Specific Language**

As noted earlier, ICS covers several areas of control families.

• **SCADA** Supervisory control and data acquisition system. SCADA systems are often found in oil, gas, pharmaceutical, and energy applications. They are used when there is a need to utilize poor-quality links such as those with high latency or low bandwidth.

• **DCS** Distributed control systems. These systems often refer to ICSs designed to operate in industrial settings such as chemical, pharmaceutical, and mining. They gather data and control systems located throughout large physical areas in real time. They are designed to be high-bandwidth and low-latency devices providing near-real-time reporting and action.

• **PLC** Programmable logic controllers. PLCs largely replaced lattices of relays that formed logic circuits for ICS. PLC is most commonly used for binary operations where speed is critical.

• **Field devices** ICS devices such as valves and sensor operating away from the central control system.

**Information Assurance Management**

image

ICS requires a robust approach for information assurance management. Since ICSs are used for mission-critical operations, it is important the information assurance management team understands the mission of the ICS prior to performing any risk analysis. ICSs are also extremely hard to analyze in their production environment because they are often relied on continuously, and doing any action such as vulnerability scanning that could interfere with their operation is generally more harmful than helpful.

**Personnel**

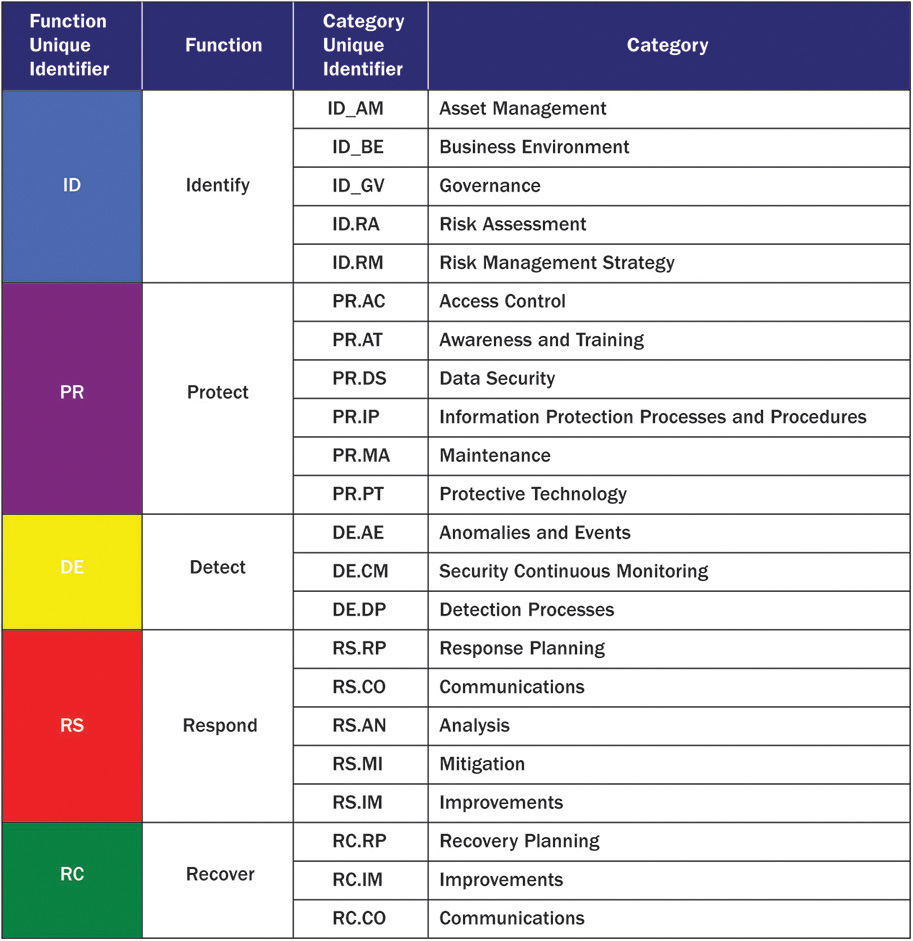
Managing information assurance for ICS requires a working knowledge of industrial processes, electronics, pneumatics, physics, and in some cases special industries, such as pharmaceutical manufacturing. When considering information assurance professionals for these areas, organizations should consider those with a CISSP, SSCP, CSSLP, or CISA, with a blended background in industrial systems. These individuals should also be subject to background investigations and reviews, should they be involved in systems considered critical infrastructure.

**Management Approach**

ICSs mandate a top-down approach to information assurance management. Since ICSs require several compensating controls and defense-in-depth, organizations must ensure senior management has made a commitment to information assurance and provided the authority and resources to protect the mission and services ICSs support. Organizations attempting to manage and protect industrial control systems through a bottom-up approach will be faced with several varieties of implementations and controls throughout the ICS and supporting network infrastructure.

**Regulations and Legal Requirements**

ICS have little in the way of laws that regulate them directly; however, there are several guidance documents available throughout the world to assist organizations in protecting ICSs. U.S. Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” was issued February 12, 2014. It provides a framework for organizations to adopt that is based on an Identity-Protect-Detect-Respond-Recover framework. Each major section is subdivided into categories, subcategories, and informative references. [Figure 28-1](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch28.html#ch28fig1) shows an example of the framework.



**Figure 28-1** U.S. cybersecurity framework example

The framework is designed to be flexible and accommodate all aspects of an organization’s existing use of frameworks, such as ISO and CoBit. Organizations must be cautious and ensure they have a strong information assurance team when using the framework because nothing is prescribed as a minimum baseline and everything must be developed from existing frameworks to fill in the function areas.

**Information Assurance Risk Management**

ICS information assurance risk management must focus on understanding the inherent weaknesses found in ICS implementations. ICSs were once isolated systems on dedicated leased lines that have now been migrated to insecure common public networks for costs and efficiency reasons. By connecting ICS to the Internet, these devices are being exposed to attacks and technologies they were never designed to defend against.

**Assets**

The asset identification for ICS is crucial in determining an appropriate information assurance approach. The information assurance team must be able to identify clearly and accurately the mission or function the ICS serves and the implications of a loss of confidentiality, integrity, availability, nonrepudiation, authentication, or availability. Will people be harmed or die? Will catastrophic explosions occur because of valves not opening to release pressure? Will a city’s potable water system become contaminated with coli bacteria because a pump didn’t turn on to pump sewage out of a system during a treatment process? The information assurance team must accurately discover not only the ICS assets but also, more importantly, the assets the ICS supports.

The U.S. Department of Defense’s Defense Security Service describes the following as attractive targets of espionage and hacking:

The term *trade secret* means all assets such as financial, business, scientific, technical, engineering, or economic information. This includes patterns, plans, compilations, program devices, prototypes, formulas, design, procedures, methods, techniques, codes, processes, or programs—whether tangible or intangible and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing if

• the owner has taken reasonable measures to keep such information secret; and

• the information derives independent economic value (actual or potential) from not being generally known to, and not being readily ascertainable through proper means by, the public.

• Such assets may include, but are not limited to,

• People

• Government personnel

• Contractors

• Military personnel

• Activities/operations

• Intelligence collection/analysis

• Sensitive movement of operations/personnel/property

• Conduct of sensitive training

• Communications/networking

• RDT&E and sensitive technology

• Production of sensitive technology

• Protection of nuclear/chemical/biological materials

• Protection of weapons, explosives, and equipment

• Information

• Classified

• Sensitive compartmented information

• Top secret

• Secret

• Confidential

• Unclassified

• System designs

• Intellectual property

• Patents

• System capabilities/vulnerabilities

• Sensitive methods

• Sensitive financial data

• Facilities

• Industry sites

• Headquarters

• Field offices/administrative buildings

• Training facilities

• Contractor facilities

• Storage facilities

• Production facilities

• R&D laboratories

• Power plants

• Parking facilities

• Aircraft hangars

• Residences

• Equipment/materials

• Transportation equipment/vehicles

• Maintenance equipment

• Operational equipment

• Communications equipment

• Security equipment

• Weapons

• Automated information systems equipment

The information assurance team should interview line management, middle management, and even operational staff to understand clearly the implications of the ICS. They need to ask questions such as “What if this failed to work?” and “What would happen if the ICS operated at the wrong time with the wrong instructions?” Leading questions can greatly help the information assurance team gather accurate asset and impact information.

**Threats**

ICSs are targeted by terrorists, extortionists, nation states, organized crime, and black-hat hackers. In perhaps one of the best known stories about ICS hacking, the Stuxnet malware infected versions of PLCs including the Siemens S7, PCS7, and WinCC systems. The malware was designed to specifically target high-frequency drives controlling uranium enrichment in Iran. While the high-frequency drives may have been the target, the malware spread throughout the world, infecting any controller meeting the description programed within but lying dormant until called to action. Large organizations utilizing the targeted controllers have spent tremendous amounts of resources cleaning Stuxnet from their system even though they were not the intended target.

Stuxnet is also innovative in how it spreads. Many ICS owners believe “air gap” measures put in place are sufficient to protect their ICSs. Stuxnet relied on this belief and replicated through USB drives, external hard drives, laptops, and even infected files to get to its target. Reliance on a single protective measure is insufficient to ensure ICS attacks are detected and prevented. You can find more information about threats in [Chapter 4](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch4.html#ch4).

**Vulnerabilities**

ICSs are inherently vulnerable because of their design and implementation. When ICSs were designed, the technologies, bandwidth, and attack methodologies of today were not available and therefore were not considered. Because many ICSs have a life span of years or even decades, the companies that supplied them may no longer be in business to support the securing of the ICS, and, in some cases, even if the company does exist, the ICS was not designed to be updated with new features and security patches.

If an organization does not have a mature configuration management, change management, and associated processes, the ability to patch vulnerabilities becomes difficult. Patching on production systems without testing can lead to system failures and possible new vulnerabilities if not properly deployed.

**Risk Assessment**

ICS-reliant organizations must adopt risk assessment procedures that assess risk not only from an information technology perspective but also from an organizational or mission risk perspective. The senior leadership of ICS organizations should strongly consider bringing in outside assessors or auditors specifically trained in ICS assessment to confirm the organization’s information assurance program has the sufficient authority, skills, knowledge, and technical capability to provide visibility into risk and mitigate it where possible. ICS organizations should carefully consider the credentials of the assessor they choose. Not all assessors understand the business or mission of the ICS organization. While any organization can run a vulnerability scan, understanding the assets and impacts of ICS environments is critical for understanding risk. The impact of a vulnerability changes from one organization to another and sometimes within the same organization.

When choosing an assessor, organizations should demand to see past work and also interview the assessor to determine how much about ICS and the organization they actually know. Additionally, asking the assessor how they plan on gathering initial information about the organization and its ICS will help understand their assessment approach. Are they simply asking for a network map, a range of IP addresses, and any machines they can’t take down? Are they claiming they will do a comprehensive “pen test” and don’t need any information about the organization’s business? Assessors may not be best suited to give an honest risk assessment if they lack interest in the business of the organization. An assessor asking questions regarding data flows, business operations, business partners, data interconnections, and business impact assessments point to a more qualified assessor.

**Risk Mitigation**

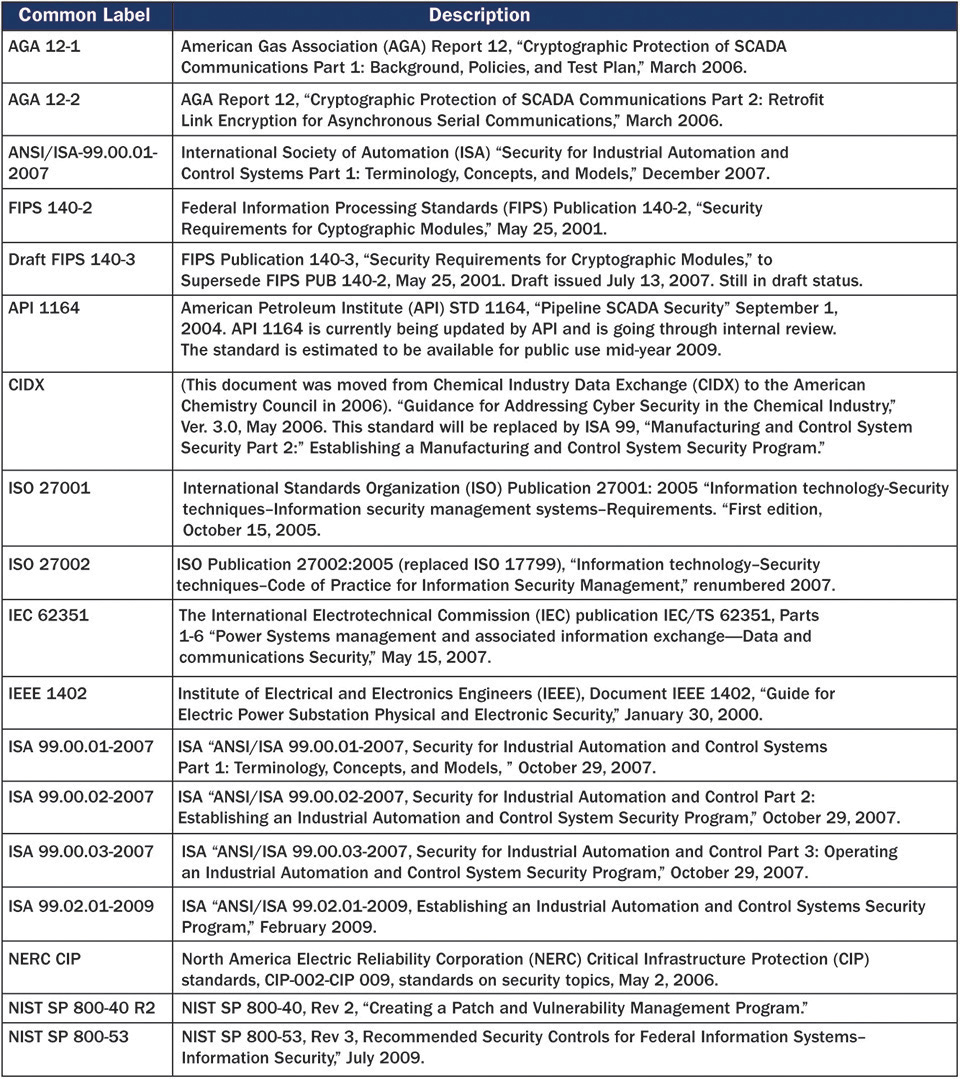
An ICS requires a layered approach to risk mitigation because typically the ICS can’t be upgraded easily and doesn’t support many security features. A defense-in-depth approach incorporating people, processes, and technology will provide the best risk management posture for the organization. ICSs often require special segmentation of networks and sometimes physical segmentation or “air gapping” to ensure they are protected against attacks through the network. Even in these extreme situations, organizations must continue their diligence because malware such as Stuxnet can “jump the gap” and find ICSs that are seemingly isolated.

**Policy, Procedures, Standards, and Guidance**

Organizations working with ICSs have an added burden of ensuring any new technology won’t introduce additional risk. The organization should ensure its policy sets senior managers’ expectations around the protection of ICSs and protection of the mission they serve. Policies must address any industry, legal, or regulatory requirements the organization may have in ensuring information assets are protected. The organization should consider developing specific information assurance standards for any ICS in operation. The standard should contain hardened configurations, setup specifications, physical security measures, interconnection requirements, scanning requirements, patching requirements, and segmentation requirements.

Procedures should focus on ensuring ICSs are monitored for vulnerabilities and ensure mitigation actions such as patches are deployed in a meaningful time with acceptable disruption to the organization. Guidance should be developed to ensure that new procurements meet the standards and procedures identified prior. Guidance should assist personnel in understanding the unique requirements ICS pose and what resources are available to help ensure they are secured and monitored.

[Figure 28-2](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch28.html#ch28fig2) from ICS-CERT lists several of the most commonly used ICS standards.



**Figure 28-2** ICS security standards (Source: ICS-CERT)

**Certification, Accreditation, and Assurance**

Certification can provide a necessary framework for ensuring ICSs meet and maintain the information assurance policies, standards, and procedures developed by the organization. Independent assessors with knowledge in ICS should be consulted to provide thorough assessments of existing ICS and also ICS systems prior to development. Accreditation provides a means to deliver risk information to the business or mission owner to ensure all parties are aware of the risk being accepted by implementing an ICS.

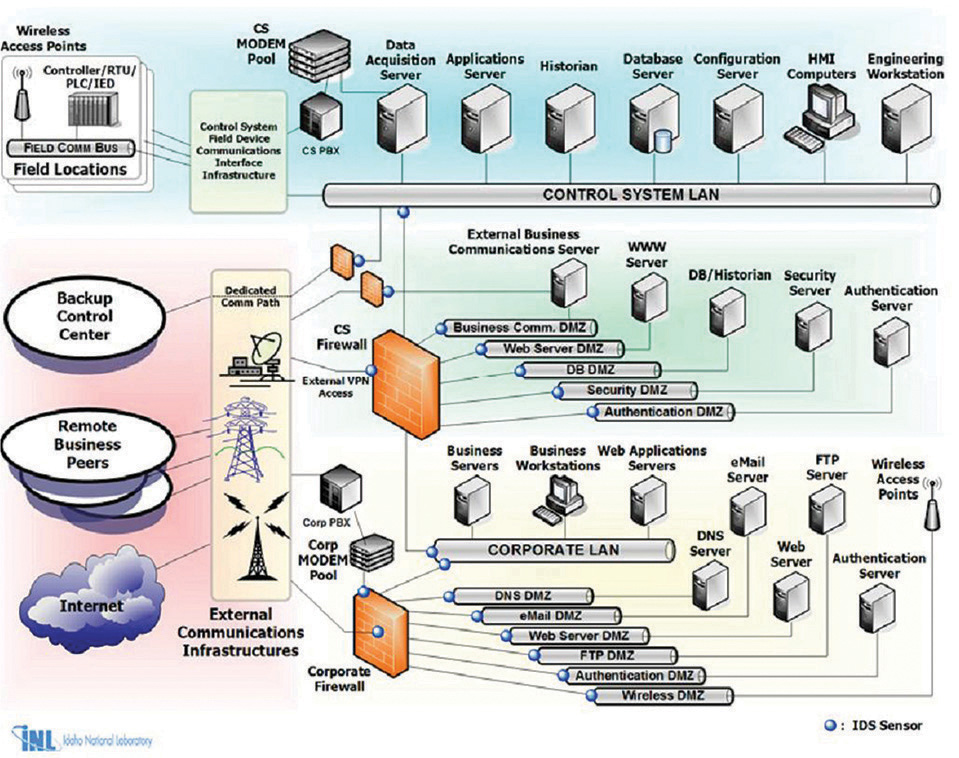
**Human Resources**

Hiring information assurance professionals to work in ICS environments can be challenging. They should be able to pass a background investigation and also possibly hold a national security clearance if they will be working on classified critical infrastructure projects. As part of the onboarding process, nondisclosure agreements and, if applicable, organizational conflict of interest statements should be completed by new hires.

All new hires regardless of area should be subject to information assurance training including specific training about the ICS. Those involved in the administration or operation of the ICS should receive additional training regarding ICS secure development, deployment, architecture, assessment, incident response, and decommissioning. Ongoing training must be enforced throughout the organization to ensure all employees maintain awareness and those with specialized roles have recurring specialized training for the ICS. Training must specifically include information about potential weaknesses such as bringing USB drives across an “air-gapped” system.

**Information Assurance in System Development and Acquisition**

ICSs rely almost entirely on their host network and systems. Therefore, ensuring information assurance is included in any procurement policies, standards, procedures, or documents is crucial. As noted in [Figure 28-3](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch28.html#ch28fig3), from the U.S. Idaho National Laboratory (INL), the ICS should be segmented and protected from the rest of the network environment.



**Figure 28-3** INL defense-in-depth network (Source: U.S. Idaho National Laboratory)

Procurement and acquisition processes must ensure the information assurance team is involved as new technologies such as cloud and mobile devices are being procured. The information assurance team can ensure the technology being procured is supported in the existing security architecture and can give recommendations for products that may meet the security and architecture requirements of the organization.

ICS procurements and development must involve the information assurance team. The information assurance team should ensure security requirements are clearly identified in any ICS development project or procurement action. If enough organizations demand secure ICS, it is only a matter of time before the market provides a hardened ICS system.

**Physical and Environmental Security Controls**

Because ICSs are notoriously weak in the logical or network sense, you may think they are physically quite strong and robust. Unfortunately, physical access to an ICS should be treated as administrative access to the device. This is extremely challenging because many organizations use ICS in remote or hostile environments where implementing physical protection would be impractical or dangerous. The information assurance team can assist the organization in these situations by assessing locations that provide the highest risk of access. An ICS in the middle of a hostile area controlling a low-value valve does not have the same risk as an ICS server sitting on a factory floor unprotected and running all the robotic controls for an assembly plant. The information assurance team can provide recommendations and a risk management approach to determine the appropriate physical and environmental protection necessary for the ICS.

**Awareness, Training, and Education**

Awareness, training, and education should focus on ensuring every member of the organization has a basic understanding about the ICSs supporting the organization and the impact they may have on assets, the mission of the organization, or even human life. In addition to the training and awareness noted in the earlier “Human Resources” section, organizations involved in critical infrastructure may also consider counter-intelligence training. Counter-intelligence training aims to protect an organization and its assets against industrial spies and nation-state hackers. In addition, selected individuals should be afforded the opportunity to participate in Cyber Defense Simulations (CDS) containing ICS components. This will afford them time to gain experience.

**Access Control**

Access control at the network and infrastructure level is crucial for organizations using ICS. As part of a defense-in-depth approach, organizations should protect vulnerable assets with firewalls, terminal servers, network segmentation, and multifactor authentication inasmuch as a risk assessment will support. Because availability and integrity are often much more important than confidentiality in an ICS, the information assurance team must be careful regarding the specific controls they advise for ICS environments. The U.S. National Institute of Standards and Technology Special Publication 800-82 has several recommendations regarding ICS access control including, but not limited to, the following:

• Default passwords must be changed, and strong passwords should be in place for each modem.

• Modem callback systems should be used when dial-up modems are installed in an ICS. This ensures that a dialer is an authorized user by having the modem establish a working connection based on the dialer’s information and a callback number stored in the ICS-approved authorized user list.

• Modems in use should be physically identifiable to control room operators.

• Modems should be disconnected when not in use, or this disconnection process should be automated by having modems disconnect after being on for a given amount of time (if feasible). It should be noted that sometimes modem connections are part of the legal support service agreement with the vendor (for example, 24/7 support with a 15-minute response time). Personnel should be aware that disconnecting/removing the modems may require that contracts be renegotiated.

• Remote control software should be configured to use unique usernames and passwords, strong authentication, encryption if determined appropriate, and audit logs. Use of this software by remote users should be monitored on an almost realtime frequency.

• VLANs have been effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches.

• Wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible) connections to the ICS network.

• Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, enable MAC filtering, and employ WPA2 encryption with a strong key at a minimum.

• Wireless device communications should be encrypted and integrity-protected. The encryption must not degrade the operational performance of the end device. Encryption at OSI layer 2 should be considered, rather than at layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.

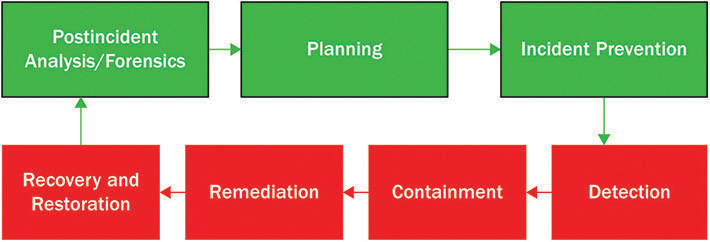
• Wireless devices, if being utilized in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain.

• Wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network prior to installation. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas.

• Wireless users’ access should utilize IEEE 802.1x authentication using a secure authentication protocol (such as Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via a user certificate or a Remote Authentication Dial In User Service (RADIUS) server.

**Continuous Monitoring, Incident Response, and Forensics**

The organization’s information assurance team should operate an incident response function that includes continuous monitoring and incident reporting. The incident response team should be trained in the specific ICS the organization uses and should understand the types of data and mission the ICS serves. The incident response team should coordinate with ICS-specific cyber emergency response teams such as the US ICS-CERT. ICS-CERT provides control systems–related security incident and mitigation information. [Figure 28-4](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch28.html#ch28fig4) provides an overview of a continuous monitoring and incident approach as proposed by the US ICS-CERT.



**Figure 28-4** Continuous monitoring key elements (Source: ICS-CERT)

As part of the continuous monitoring process, organizations should gain an understanding of normal operations. In doing so, they can understand abnormal behavior. The U.S. National Institute of Standards and Technology Special Publication 800-82 advises organizations to be on the lookout for the following:

• An account in use when the user is not at work

• Antivirus or IDS alerts

• Attempted or actual use of administrator-level accounts

• Cleared log files

• Creation of new user accounts

• Disabled antivirus software and other security controls

• Full log files with unusually large number of events

• Locked-out accounts

• Machines connecting to outside IP addresses

• Out of disk space or significantly reduced free disk space

• Requests for information about the system (social engineering attempts)

• Unexpected changes in configuration settings

• Unexpected patch changes

• Unexpected system shutdown

• Unusually heavy network traffic

• Unusually high CPU usage

**Business Continuity and Backups**

Because ICSs are typically focused on integrity and availability, organizations need to consider the strength and resilience of their network infrastructure. This can conflict with the need to keep an ICS segmented and protected because redundant or load-balanced sites can rapidly direct traffic from one location to another to ensure performance metrics are met. Organizations should ensure networking technologies are properly scoped through a business impact analysis to determine the recovery time objective and recovery point objective for the ICS.

Redundant power systems on separate suppliers, power generation from solar, wind, or thermal, and routine testing should be designed to ensure the ICS can operate in adverse conditions such as natural disasters and possible human-caused outages as well. The networking infrastructure must also be taken into consideration, and in critical applications, diverse connectivity paths should be considered; for example, one path may be via fiber to a local telecommunications company, while a backup link is provided by another company’s cellular network or satellite telecom.

**Further Reading**

• Assante, M.J. Testimony on Securing Critical Infrastructure in the Age of Stuxnet. National Board of Information Security Examiners, November 17, 2010.

• Christensen, Sharon, et al. “An Achilles Heel: Denial of Service Attacks on Australian Critical Information Infrastructures.” *Information & Communications Technology Law.* 19, no. 1 (2010): 61–85.

• Fabro, M., and V. Maio. Using Operational Security (OpSec) to Support a Cyber Security Culture in Control System Environment, 2007. <http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf>.

• Falliere N., L.O. Murchu, and E. Chien. W32.Stuxnet Dossier. Symantex, February 2011. [www.wired.com/images\_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf](http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf).

• IBM Internet Security Systems. A Strategic Approach to Protecting SCADA and Process Control Systems. [www.iss.net/documents/whitepapers/SCADA.pdf](http://www.iss.net/documents/whitepapers/SCADA.pdf).

• Interim Report to the Department of Homeland Security. Development of a Baseline Set of Technical Metrics, January 2007.

• Jansen, W. Directions in Security Metrics Research. NIST special publications, April 2009.

• Jelen. G. SSE-CMM Security Metrics, The National Institute of Standards and Technology (NIST) and Computer System Security and Privacy Advisory Board (CSSPAB) Workshop. Washington, D.C., June 13–14, 2000.

• Linden E.V. Focus on Terrorism, Volume 9. Nova Science Publishing, 2007.

• Manadhata, P.K., et al. An Approach to Measuring a System’s Attack Surface, CMU-CS-07-146. Carnegie Mellon University, August 2007. http://reports archive.adm.cs.cmu.edu/anon/2007/CMU-CS-07-146.pdf.

• Morris, Thomas H., et al. “Engineering Future Cyber-physical Energy Systems: Challenges, Research Needs, and Roadmap.” North American Power Symposium (NAPS). pp. 1–6. IEEE, 2009.

• Morris, Thomas, R. Vaughn, and Y.S. Dandass. “A Testbed for SCADA Control System Cybersecurity Research and Pedagogy.” Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research., p. 27. ACM, 2011.

• National Cyber Security Research and Development Challenges Related to Economics. Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective. The Institute for Information Infrastructure Protection (I3P), 2009.

• Payne, S.C. A Guide to Security Metrics. SANS Security Essentials GSEC Practical Assignment, Version 1.2e. June 19, 2006. [www.sans.org/reading\_room/whitepapers/auditing/55.php](http://www.sans.org/reading_room/whitepapers/auditing/55.php).

• Savola, Reijo M. Towards a Taxonomy for Information Security Metrics. International Conference on Software Engineering Advances (ICSEA 2007). Cap Esterel, France, August 2007.

• Report to the Department of Homeland Security. INL/EXT-06-12016, Cyber Security Metrics, December 2006.

• Slay, J., and M. Miller. *The Maroochy Water SCADA Breach: Implications of Lessons Learned for Research in Advances for Critical Infrastructure Protection*. Springer, 2007.

• Slay, J., et al. “Process Control System Security and Forensics: A Risk Management Simulation.” Proceedings of SIMTECT 09. Adelaide, June 15–19, 2009.

• Swanson, M., et al. *Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55*, July 2003.

• The CIS Security Metrics Service. The Center for Internet Security (CIS), July 1, 2008. <http://securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner%20handout.pdf>.

• The First National Security Statement to the Australian Parliament. The Prime Minister of Australia the Hon. Kevin Rudd MP, December 4, 2008. <http://pmrudd.archive.dpmc.gov.au/sites/default/files/file/documents/20081204_national_security_statement.pdf>.

• Vaughn, Rayford, Jr., R. Henning, and A. Siraj. Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy. 30th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 7–10, 2002.

**Critical Thinking Exercises**

1. The accountants at an energy company have been to a technology presentation about the cloud and Infrastructure as a Service (IaaS). They come into the CIO’s office and tell him he can cut his costs by significant margins if they use only IaaSX (the cloud offering from the provider). The CIO is responsible for maintaining a large number of natural gas pipeline control networks in addition to the ICS operating several large refineries. Should he agree with the accountants? Is there another answer he should provide?

2. A heating, ventilation, and air-conditioning company has just installed a state-of-the-art environmental system for an organization. As part of the purchase, the organization is going to receive one year of monitoring and efficiency reporting for free. The vendor requests to have the new equipment connected to the network and be given a domain admin account. The vendor says it needs the admin account so it can access the environmental control servers any time and perform repairs or maintenance. The CISO is discussing the request with the facilities manager. What response should she provide?