Demystifying Cyber Security in Industrial Control Systems

Industrial control systems (ICSs) are changing by relying more on off-the-shelf information technology (IT), thereby exposing these systems to more IT risk. In the past, ICSs operated in isolated environments using custom-built technologies and were confined to risk within their own realms. However, with the advent of computer-integrated manufacturing (CIM), ICSs had to change and adapt to this new paradigm. ICSs are now connected to IT systems for logistics and management, but ICSs are unique, because they operate in a very different environment, in different conditions, where IT safeguards cannot be easily applied. An ICS, unlike IT, is highly dependent on its system being continuously available. Furthermore, it is designed for a longer operational life than IT. Applying security to an ICS is like going into battle with both hands tied behind one’s back. Security professionals need to get creative and find different ways to battle the attackers. These professionals must find work-arounds that can address peculiarities of ICSs and provide a robust security solution.

This article introduces the challenges in ICSs, lays out the differences between IT and ICS, and proposes a high-level framework that ICS security practitioners can use to develop a consistent, organized and standard security solution to protect ICSs.

Industrial Control Systems

ICSs are commonly found in industries such as oil and gas, water treatment plants, manufacturing, and energy. ICSs help to monitor and control industrial processes. Many of these processes are categorized as national critical infrastructure; therefore, ICS security is vital. These systems are designed to help operators and plants to manage the operation and make decisions based on the information that is collected from the process sensors. ICSs are plant automation and control focused. They are installed within the confines of a plant network and usually have no need to interface with anything outside of the plant. CIM plant systems changed the interface of ICSs to include systems outside of the plant network. CIM plant systems are integrated with IT systems to provide a seamless enterprise experience. Systems such as ordering systems and supply chain and financial systems are now integrated with plants to seamlessly fulfill orders and transport the goods to the end users quickly and efficiently.

Security Objective

Many critical US national infrastructures are controlled by ICS. The national economy, basic services and the well-being of individuals depend on the uninterrupted and continued operation of these processes. The stakes are high, and the importance of ICSs is evident. The main objective of ICS security is to ensure availability and, consequently, protect ICSs.
Tampering with this information can lead to safety issues and fatality, as in the events at the Australian sewage plant and the Iranian nuclear facility.

The key differentiator between ICS and IT security is in the primary objective of ensuring availability and safety. Ensuring continuous availability safely is a challenge. For example, patching systems in IT is assumed to be standard operating procedure. It is extremely challenging to patch a computer running a distributed control system (DCS) on Microsoft Windows. These computers cannot be recycled after applying the patch, due to the 24/7 availability requirement. A computer that cannot be shut down cannot be patched.

Security Challenges

The security professional in the ICS environment must be creative and think out of the box to address the numerous challenges of ICS security. ICSs rely heavily on vendor solutions and are very dependent on the vendor’s ability to support security solutions. The process industry relies on multiple vendors to build the control systems. Vendors provide the entire stack—hardware, software, network design and sensors, in some cases. These control systems are closed-loop systems and are built using various technologies that are based on the level in the ICS stack. For example, sensors and I/O modules can use vendor-specific technologies, and supervisory control and data acquisition (SCADA) or DCS systems can use systems built on Microsoft and Intel technology. Sensors can use vendor-specific communication protocol while the SCADA system can use Transmission Control Protocol (TCP)/IP protocol. Furthermore, vendors fine-tune the standard technologies to adapt them to their product. System administrators cannot directly patch these systems, although they might be standard IT technology, without the vendor’s approval. Vendors must apply the patch in a test environment and ensure that it does not interfere with the normal operation of the system before they can certify the patch. This is a lengthy process and needs to be

The importance of security in the industrial world is very high. A rogue ICS can have fatal consequences to life, the environment and the national economy. An example is the cyberattack on the Maroochy Water Services plant in Australia that released raw sewage into a local park and a local river, killing marine life. This attack had a catastrophic effect on the local environment and posed a health risk to local residents. Some IT systems have the same high level of security importance, e.g., equity trading platforms; however, this is generally an exception.

Integrity and confidentiality of information are also important concerns in ICSs, although they are of lesser importance. The Stuxnet worm malware was able to tamper with the feedback information from controllers and cause the centrifuges at the Natanz nuclear facility in Iran to spin uncontrollably and eventually seize up and crash. This security event compromised information integrity, causing process failure, which resulted in lack of availability, or, in IT terminology, denial of service (DoS). ICSs depend on the information feedback from input/output (I/O) devices to ensure proper monitoring and control.

A rogue ICS can have fatal consequences to life, the environment and the national economy.
In the past, ICSs were built on vendor proprietary infrastructure using specialized protocols, hardware and software. These systems were isolated with minimal risk of compromise. With the advent of the Internet and connectivity paradigm, ICS vendors began to adapt IT solutions and build the control stack using industry standard computers, hardware and protocols. This practice reduced the cost of development and maintenance, but exposed ICSs to cyberattacks, which are prevalent in the IT world. IT heavily relies on patching, antivirus software and other host-based solutions to mitigate some of the risk. These solutions, in many cases, are not applicable in ICSs. ICSs might be running on obsolete hardware that cannot provide the processing power needed by these solutions. Furthermore, these solutions can interfere with the normal functioning of products. In some cases, adding some of these controls adversely impacts the real-time performance and, therefore, is not recommended by the vendor due to the negative performance impact. The challenge is to protect ICSs from IT-based attacks, because parts of ICSs use standard IT technologies, and ICSs are connected to the IT enterprise network, but unable to have IT safeguards applied.

In the past, ICSs were built on vendor proprietary infrastructure using specialized protocols, hardware and software. These systems were isolated with minimal risk of compromise. With the advent of the Internet and connectivity paradigm, ICS vendors began to adapt IT solutions and build the control stack using industry standard computers, hardware and protocols. This practice reduced the cost of development and maintenance, but exposed ICSs to cyberattacks, which are prevalent in the IT world. IT heavily relies on patching, antivirus software and other host-based solutions to mitigate some of the risk. These solutions, in many cases, are not applicable in ICSs. ICSs might be running on obsolete hardware that cannot provide the processing power needed by these solutions. Furthermore, these solutions can interfere with the normal functioning of products. In some cases, adding some of these controls adversely impacts the real-time performance and, therefore, is not recommended by the vendor due to the negative performance impact. The challenge is to protect ICSs from IT-based attacks, because parts of ICSs use standard IT technologies, and ICSs are connected to the IT enterprise network, but unable to have IT safeguards applied.

A long operating life span and the inability to patch and update the systems quickly lead to obsolescence.

In the past, ICSs were built on vendor proprietary infrastructure using specialized protocols, hardware and software. These systems were isolated with minimal risk of compromise. With the advent of the Internet and connectivity paradigm, ICS vendors began to adapt IT solutions and build the control stack using industry standard computers, hardware and protocols. This practice reduced the cost of development and maintenance, but exposed ICSs to cyberattacks, which are prevalent in the IT world. IT heavily relies on patching, antivirus software and other host-based solutions to mitigate some of the risk. These solutions, in many cases, are not applicable in ICSs. ICSs might be running on obsolete hardware that cannot provide the processing power needed by these solutions. Furthermore, these solutions can interfere with the normal functioning of products. In some cases, adding some of these controls adversely impacts the real-time performance and, therefore, is not recommended by the vendor due to the negative performance impact. The challenge is to protect ICSs from IT-based attacks, because parts of ICSs use standard IT technologies, and ICSs are connected to the IT enterprise network, but unable to have IT safeguards applied.

Safety is of primary concern in process control. ICSs must quickly react to operational parameters that are drifting outside of the safe zone. In many cases, operators need immediate access to the control system to execute a manual override. For example, if an operator needs to log in quickly and this stress causes typing errors during multiple login attempts, the login account is locked out. The challenges are to find security controls that support emergencies and provide ways to bypass these
Security controls in a legitimate manner, i.e., provide an override, but protect it from misuse.

“The challenge is to convince executives that ICS cyber security is as important as IT security and should be adequately funded.”

Security takes a backseat in plants because of the culture. It is generally believed that the plant network is isolated, with no connection to the outside world. Decision makers believe that the control stacks are proprietary and too obscure for attackers to bother with them. Plants hesitate to invest in comprehensive cyber security programs. Instead of hiring dedicated system administrators who are skilled in security, plants rely on control engineers to manage their systems. This practice leads to unskilled personnel managing critical infrastructure. Furthermore, plants do not spend money on upgrading personnel skills, leaving these administrators woefully underprepared. The lack of a universal global security standard on which these administrators can rely exacerbates the security situation. Most enterprises have a comprehensive security program for IT, but they fall short for ICS security programs. The challenge is to convince executives that ICS cyber security is as important as IT security and should be adequately funded. Executive sponsorship is the key to ensure proper security posture in ICSs. Figure 2 shows the ICS security challenges.

Figure 2—ICS Security Challenges

Security Weakness

Challenges provide the context within which ICS security must be enabled and are constraints around which security professionals must work. On the opposite side, if challenges are not properly addressed, they create vulnerabilities. Vulnerabilities are specific weaknesses that can be exploited by attackers. Vulnerabilities generally exist because challenges, constraints or inadequacies are endemic in the system. Inadequate policies and procedures, improper hardware and software configurations, improper network implementation, or inadequate malware protection can lead to vulnerabilities. For example, one ICS challenge is to provide continuous availability while delivering robust security. Continuous availability leads to the inability to patch systems because systems cannot be rebooted after patching. The consequence is that systems remain unpatched and vulnerable to well-known and, sometimes, outdated attacks. Over time, these systems fall so far behind that no patches can be applied and systems become very fragile. System administrators lose confidence in these systems and refuse to do anything to them for the fear that these systems might not recover.

Vulnerability by itself is innocuous in the absence of a threat, i.e., if there are no agents that want to take advantage of the weakness, then the weakness by itself is harmless. Applying this concept to an ICS is important because it helps with understanding the risk and applying the appropriate mitigating controls.
Newer ICSs are built on IT-standard technologies that become obsolete faster than the ICSs. Support for the underlying IT systems disappears faster than the useful life of an ICS, therefore, rendering the ICS obsolete. Obsolete systems pose a huge risk to business continuity from security and operational perspectives. Obsolescence can be created by:

- Out-of-support underlying software or operating system
- Out-of-support hardware
- Inability to apply the patches that the vendor continues to provide
- Vendor that no longer exists
- Lack of staff expertise to keep up the environment
- Change in operating conditions that adapt systems so that they can be used for purposes for which they were not originally designed, therefore exposing them to unaddressed risk

Threats to ICS can be categorized mainly into two main buckets—internal and external. Internal threats are from threat agents who are inside the network (figure 3) and external threats are from threat agents who are outside of the ICS network. The internal and external threat source exploits the vulnerability using some type of tool. In figure 3, an internal threat agent (operator) exploits the open USB port vulnerability using a malware tool. This exploit can be a starter attack that leads to other exploits and eventually gets to the real objective.

ICSs are most vulnerable to attacks such as viruses, worms and Trojans, because they can be introduced by either an internal or an external agent. These attacks can employ techniques such as key logging, unauthorized access, and privilege escalation to execute attacks such as DoS, information stealing or information manipulation. An ICS is extremely sensitive to availability issues. An example scenario is an unsuspecting operator plugging in an infected universal serial bus (USB) stick to perform a task. The USB stick releases a malware that executes a synchronization (SYN) flooding attack on a SCADA server, depleting its resources and rendering it unresponsive. This type of attack can lead to a catastrophic situation such as an environmental disaster with potential loss of life.

“A framework is needed to address ICS security. Most of the time, the general principles that are used to tackle IT security can be applied to ICS security. However, ICSs have some specific and unique issues that are not present in IT.”
Some major vulnerabilities that can be found in ICSs are:

- Perimeter and network flaws
- Flaws from using antiquated protocols
- Patching issues
- Attacks on field devices
- Lack of proper cyber security controls

**Solution Framework**

A framework is needed to address ICS security. Most of the time, the general principles that are used to tackle IT security can be applied to ICS security. However, ICSs have some specific and unique issues that are not present in IT; therefore, ICSs need a context-specific solution.

Secure solutions must be procured and deployed. This works well when installing new equipment. A framework is needed that can be used to address assets that are already in use and, perhaps, obsolete or very close to obsolete.

Primarily, all solutions must work within the context of risk management, i.e., any solution must address the triad of threat (actor/motivation/capability), vulnerability and asset (figure 4).

All security must be addressed based on the risk profile, with more critical issues being addressed before least critical ones. The solution should address actors as much as vulnerability, if possible. For example, a motivated actor will simply move on to the next vulnerability when one vulnerability is plugged. In figure 3, the exploit was possible because the actor inserted an infected USB stick. The obvious response is to disable the USB port. If the actor is very motivated, he or she might find another weakness, perhaps a CD drive, with which to infect the system. In this example, one should ask the actor why he or she inserted a USB stick. The reason may be to copy files or to apply a patch. If so, determine if the patch management can be automated and offloaded to a patch server, and eliminate the necessity to insert a USB stick. If the actor inserted the USB stick because of ignorance, determine if well-structured training can help. In this example, disabling the USB is the right thing to do, but not the only solution.

The best way to solve the problem of ICSs that cannot be altered is to surround the system with multiple layers of controls. This approach is called defense in depth (figure 5).

The multiple layers of appropriate controls plug the vulnerabilities at multiple layers. This approach ensures that the attacker has to navigate around multiple compensatory controls and try very hard to
execute the attack. Figure 5 shows that the center is the core asset—the ICS. Surrounding it at the outermost layer are the constraints and challenges in which the ICS operates. These constraints and challenges create vulnerability, which is represented by the narrow tubes through which worms can be introduced. By using defense in depth, the ICS can be surrounded with multiple and different controls. If the attacker’s purpose is to deliver angry payload into the system, it must first encounter a segmented network. If it overcomes the isolation, then antivirus software protects the host. The host USB is disabled; therefore, this asset is protected from external and internal entry points. This diagram shows a simple illustration of defense in depth. A true defense in depth additionally addresses the possibility of the antivirus software missing the virus.

The best way to solve the problem of ICSs that cannot be altered is to surround the system with multiple layers of controls.

It is essential to understand that, by stacking controls around the ICS, layers of defense are being built, thus minimizing residual risk. The security risk is not being reduced by making direct changes to the asset itself, but by surrounding the asset with protection. Often, the systems are so old that antivirus software cannot be installed. In this condition, other compensatory controls should be added—perhaps, a process that ensures that the USB stick is first scanned on an offline computer before being inserted into an ICS. Defense in depth is a layered solution to a problem, and the solution is not always a technical control. Process controls and people controls can be layered to ensure that the ICS is safeguarded at different levels.

To determine the controls to apply, where to apply them, when to apply them, in which context controls are acceptable and when they are ineffective, a standard way to model ICSs is needed. This model should help to identify areas that need protection and guide security practitioners to the right kind of controls that are needed in those areas. A model of ICS components and a standard menu of applicable controls that can be applied as a standard are needed.

The Purdue Enterprise Reference Architecture (PERA) is one of the most common ICS reference architectures. PERA divides the process and automation stack into six levels and details the behavior of each level. The bottom four levels relate to ICS, and the top two levels relate to enterprise IT.

PERA divides the stack based on how the components are used in control systems and their degree of sophistication. The need for availability is the highest at level 0 and reduces relatively as one moves up the stack. The need only for availability diminishes relatively as one moves up the stack, but remains the prime concern in ICSs. Cryptography can be prescribed at level 3, but never at level 0, because it relies on high availability and short response time. PERA distinguishes between IT and ICS stacks. This model can be used to find appropriate controls at each level—for example, to prescribe isolation between level 3 and level 4 and to further segment the network between each level below level 3, based on degree of trust. Level 1 focuses on safety systems that require quick access and reaction. Using this knowledge, access management systems at level 1 can allow a common account for different operators, but level 2 systems should enforce unique accounts, because the focus at level 2 is on management and monitoring.

A comprehensive defense-in-depth strategy must be risk based and should be guided by a standard model. Controls should be picked based on their
relevance at each level and their ability to reduce residual risk at each level. A defense-in-depth strategy that is based on sound rationale and uses a structured approach that is based on a standard model improves security posture while deploying capital efficiently.

**Endnotes**


Conclusion

ICSs are being built using standard IT technologies, which exposes these systems to IT risk. Operating conditions in an ICS are very different from IT; therefore, the solutions from IT cannot be directly applied to ICSs. Because ICS security problems are unique, they need to be solved creatively. ICSs rely heavily on availability, and their operational lifespans are considerably longer than those of IT systems, making obsolescence endemic in ICSs. In most cases, ICS security must be enabled without making any direct changes to the system. The best way to accomplish this is to use the defense-in-depth strategy, layering appropriate controls to thwart attacks. Security practitioners should rely on architecture or a standard model to prescribe appropriate controls, which ensure minimized residual risk, and to eliminate wasteful ad hoc controls that do not contribute to risk reduction. It is worth examining defense in depth in detail and provide examples of how this strategy can be used to secure ICSs and tackle obsolescence.

“**A comprehensive defense-in-depth strategy must be risk based and should be guided by a standard model.**”