SecureICS White Paper: August 2014

Vulnerabilities in Process Control Networks: *Identifying Frequently Overlooked Threats*

Dr. Alex Tarter, Ph.D., Technical Director

ABSTRACT

Cyber security as it relates to critical infrastructure is a growing concern to governments and large enterprises. The risks are increasing due to a rise in published vulnerabilities, wider connectivity, and the adoption of open standards that can expose networks and critical edge devices, or end points, to serious exploits. Yet the methods and technologies available to mitigate or eliminate these risks often are ignored, inadequate or inconsistent.

The wide range of industrial control implementations, architectures, and impacts have led the industrial cyber security market to advocate a risk-based management approach. However, technology advances and versatile attackers often leap ahead of security systems built on the all-too-common "protect against the last attack" approach. If a method of attack is new, or is paradigm shifting (as was Stuxnet), industry often is slow to respond. For example, Stuxnet overcame an “air-gapped” network, yet the majority of protection advice still calls for better perimeter security. How does this security approach address network perimeter breaches or insider attacks? Can such attacks even be protected against, or identified?

Good perimeter security and computer end-point protection are sound security recommendations. Even so, questions remain whether they are sufficient, and are designed to defeat future threats.

Cyber security often is presented as complicated, full of technical jargon, difficult to grasp, and often at odds relative to priority status with safety. In fact, the concepts of cyber security are straightforward. It is the implementation that is difficult, and security should complement safety rather than oppose it, as will be seen. When the cyber risk cannot be adequately explained, or understood, then any mitigation solution cannot be validated for effectiveness, and managers cannot say they have controlled it. Security, like safety, is an inherent foundation for any industrial automation facility, and so must be appreciated and integrated throughout the system lifecycle.

This paper will outline some of the emerging trends and vulnerabilities in the attack space, and what it means for the current approach to industrial cyber security. It will present fundamental questions every industrial control owner should ask of their security solution. An industrial control or automation system is not the same as an enterprise IT system, as the risks and the impacts are different. Security solutions must fit within the operational constraints of the system and within the risk appetite of the client organization. Otherwise the fix can cause a greater undesirable impact overall than an attack.

Vulnerabilities in Process Control Networks: *Identifying Frequently Overlooked Threats*

OVERVIEW: INCREASING SECURTIY RISKS

Daily headlines warn of hostile governments and criminals working to hack their way into domestic power stations. The ICS-CERT website continuously updates newly discovered vulnerabilities disclosed by security researchers on almost every industrial control vendor's products. Still, many more are found by those who are less responsible, but tenaciously persistent. These products, computers and software have been found to have serious vulnerabilities or backdoors that allow unauthorized remote access, with credentialed users none the wiser. Critical infrastructure is an attractive target for cyber-attacks by criminals, activists, and even governments, yet many industrial control systems (ICSs) are thinly protected by firewalls, anti-virus software and gateways that can be bypassed, and by passwords that can be cracked.

The industrial control industry finds itself at the confluence of a number of factors that have contributed to a dramatic increase in risk. These factors include the wider network connectivity of systems, the increased reliance on computer control, the adoption of open standards, the interest of the security community to find vulnerabilities, and the wide availability of sophisticated hacker tools that a layman can use. The required ability to attack an industrial control facility has therefore become much easier just as the means to do so have become available to anyone.

Although headline grabbing cyber-attacks on Target, Twitter and major U.S. banks have received disproportionate attention, ICSs have increasingly become a target-of-choice for attackers who have specifically sought to disrupt and damage industrial control systems and their integrated networks.

According to Gartner, the worldwide security market may grow to more than $86 billion in 2016.[i] A U.S. Department of Homeland Security (DHS) report released in January 2013 revealed that ICSs were hit with 198 "documented" cyber-attacks in 2012 and that many of these attacks were deemed serious. Forty percent of those attacks were on energy firms, according to ISC-CERT, which reviewed every incident. Water utilities came in second, with 15 percent of the attacks focused on them.[ii]

The meteoric rise in successful cyber-attacks demonstrates that attackers can not only disrupt communication networks but also the automation and control systems that are linked to them. Former U.S. Defense Secretary Leon Panetta pointed to cyber-attacks in a well-covered policy announcement, noting that they mark "a significant escalation" in cyber warfare.[iii] However, many of these threats can be effectively counteracted by private industry through the use of certified security processes and COTS (commercial off the shelf) products in their industrial control systems.

ICS SECURITY CHALLENGES

Despite the attention given to it, security is just one aspect of a successful operational control system. Security controls cannot impact safety, and the cost of mitigations must be balanced against the likelihood of attack. Every business must manage risks, and balance competing concerns such as cost so that the chosen security-system design is appropriate to the operating environment. Every business must evaluate security end-to-end. This means assessing risk from the outer-most networked PC in the office domain to the lowest PLC (programmable logic controller) in the operational domain.

A computer need not be a PC to be attacked by a hacker or malware. Embedded devices such as controllers and sensors are just as vulnerable; sometimes more so. Likewise, a cyber security control need not be technological; vulnerability might as effectively be mitigated with a procedural or managerial control as with a new product.

The facility manager's mission is total operational effectiveness and reliability. It is necessary for this reason to design, build and deploy solutions that combine technology, policies and procedures to align risk with valid, and often turnkey, solutions that maximize systems spending while eliminating downtime due to breaches.

Implementers	Industries
✓ Plant Operators ✓ Facilities Managers ✓ Main Automation Contractors ✓ Industrial Equipment Vendors ✓ Embedded Device Manufacturers	✓ Critical Utilities (e.g. Power Generation, Water, Waste) ✓ Distribution (e.g. Electricity, Gas, Oil) ✓ Industrial Facilities ✓ Healthcare ✓ Telecommunications ✓ Building Automation
Desires	**Concerns**
✓ Efficiency savings through automation ✓ Optimization of plant operations and processes ✓ Safe and reliable operation ✓ Share information between stakeholders ✓ Connect equipment over an IP network ✓ Utilize open and common protocols	✓ Unauthorized external access to networks and systems ✓ Loss of command and control or data integrity ✓ Loss or degradation of system availability ✓ Malware infection manipulating operations ✓ Cyber-attack causing physical impact ✓ Intentional misuse of systems or control causing physical impacts ✓ Reputation loss due to publicized vulnerabilities or attacks ✓ Cyber security attacks impacting normal operations

WHAT IS PROTECTED TODAY

The good news is that almost every industry sector has taken notice of the threats. Decision makers are pursuing standards and best practices for improved and assured systems safeguards. The bad news is that these standards and practices often adhere to familiar methodologies: define a critical system's perimeter, erect perimeter defenses, control what comes in and out.

This methodology has resulted in a preponderance of so-called "secure systems" through the use of data-diodes or gateways, which are barely more than networks of segregated enclaves with restricted access between themselves, and from public networks. This is a good first step, and can be used to protect against the legacy and standard methods of attack. However, it is only a thin barrier against a determined attacker who is highly motivated to penetrate the network. The real issue is that it is a matter of time before the perimeter is breached, and once inside the perimeter (or enclave) there are no protections preventing attackers from doing whatever they like.

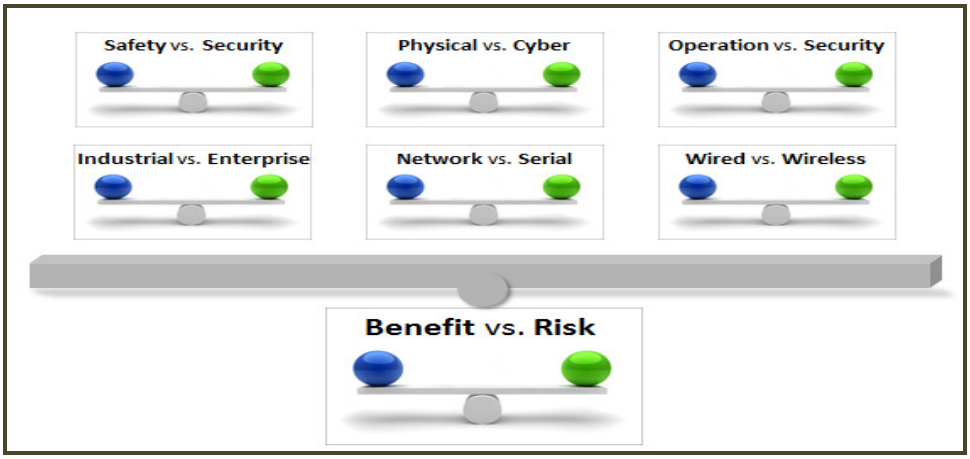
This security approach, while it will stop a cursory attempt, will not stop a dedicated or targeted assault. Technology and attackers often elude the assumptions made in the risk assessment, leading to a "protect against the last attack" approach. At that point, as evidenced with Stuxnet, the damage has been done. Along the same lines, if an attack is paradigm-shifting, industry typically is slow to respond, further exacerbating the impact. With the increasing numbers of high-profile insider attacks in the news, industry principals should consider whether the security controls in place would prevent an insider from successfully attacking the system.

With each security control and architecture design, industry insiders should ask whether this system or feature prevents vulnerability from exploitation, or merely prevents an attack vector. The reality is that, in most industrial control facilities, the weakest and most vulnerable devices are the end-devices such as the PLCs or similar non-PC embedded computers. When operated correctly, a PLC is one of the most reliable devices in operation. If told to do something unexpected or non-standard, it more often than not fails or malfunctions. Therefore if an attacker wanted to cause physical damage or impact a facility's operations, the goal is to interfere with PLC-related communications. The best-practice defense, however, is firmly focused on protecting the supporting PCs. Firewalls, proxy-servers, anti-virus, and data-diodes are being used to protect PC-to-PC communication in hopes that doing so will protect the machine-to-machine (M2M) communication of the controllers. When one of these has been compromised, the critical control network and attached devices (e.g. PLCs, RTUs) are left defenseless and vulnerable to attack.

MITIGATING VULNERABILTY RISKS

It is important to understand the difference between a vulnerability and an attack vector. The essence of any security risk-management activity is mitigating vulnerabilities rather than attack-vectors. Every PC is vulnerable to malware, and anti-virus protections seek to identify all known pieces of malware (attack-vectors). However, with new types and forms of malware coming online daily, trying to keep up with the anti-virus signatures is an endless pursuit leaving the user potentially vulnerable to an as yet undetected attack-vector. To apply an analogy: Humans are mortally vulnerable to polio, plague and measles. We can attempt to barricade the various avenues through which the disease can reach us, as was tried during outbreaks of Black Death. In the end, our vulnerability remains until a vaccine comes to the fore.

For many critical systems, when choosing a security solution or risk mitigation, the assessment should always establish whether the solution mitigates the vulnerability or solely the most likely attack-vector. Do vulnerabilities remain if the attacker tries a different approach that bypasses that mitigation?



UNCOVERING VULNERABILITES

To reduce an attack surface, organizations must understand their specific weaknesses. Once identified, a system may be designed that pinpoints vulnerabilities down to the device level, rather than the network level to ensure complete end-to-end integrity and source validation.

Unauthorized Device Connections	Stop individuals from unplugging a legitimate device and plugging in their own to access a protected area (typically performed from a less secure area) from equipment maintenance terminals, for example, that provide access to the entire business network.

Eavesdropping/ Network Interception	Someone intercepting communications and downloading or manipulating them.
Unauthorized Access	A device on a network is compromised, affording the attacker access to every machine on the network; for example, a PC in the corporate office is infected by malware giving the attacker access to the power generation system.
Sophisticated Malware	A piece of targeted malware (e.g. Stuxnet) created by a sophisticated attacker, perhaps state sponsored, tests for vulnerabilities to cause physical damage or disruption through an industrial control system.
Insider Attack	An insider (possibly the operator him or herself) instructs the control system to perform a dangerous or malicious action.
Complexity	Effective solutions are be easy to deploy, manage and maintain, and do not interfere with standard operations.
Expanding Networks & Legacy Networks	Connecting multiple devices and processes for maximum convenience and efficiency has also created the greatest degree of vulnerability than has existed before.

IMPLEMENTING "GOOD" SECURITY

Today, most general-purpose operational systems incorporate ISA-adopted security concepts. However, there is no guarantee that a supplier selling COTS products has implemented security correctly. The industry requires independent safety validation and testing before a product can be deployed, but there are no such requirements for security. A vendor can claim to have implemented security correctly and the customer can only accept the claim on faith. With continued vulnerability reports and security patch releases, is this wise? To overcome lingering security concerns about the use of networks in critical industrial operations, facility managers are increasingly looking for guidance on deploying secure networks more effectively. For example, government agencies require a minimum level of assurance that a product's stated security claim for protecting sensitive data is valid. Today, the U.S. government develops and implements networks using proven security standards with independently-tested and compliance-certified solutions to assure that industrial applications and critical data are sufficiently protected.

In the industrial automation and control sector, insufficiently secured devices, maintenance access and unguarded user stations can seriously compromise networks. Hackers specifically target unprotected devices using specialized tools to break encryption and authentication. Because most networks connect back to a central network at some point, hackers can use any unsecure station as a launch pad to remotely breach a network.

Today, many plant operation systems have voluntarily adopted the ISA99 security approach (also known as IEC 62443).[iv] Unfortunately, as many industry watchers have found, there is denial in certain quarters responsible for critical infrastructure regarding the potential severity of cyber threats that can damage and disrupt industrial control systems. The first step in embracing the ISA99/IEC62443 approach is simple

recognition that cyber security is not an irrelevance or distraction. It must become an integral component of planning and acquisition from the outset.

ISA99/IEC62443 provides a good baseline approach for system-level architecture. However, there remains a need to validate the security of the components that comprise the system. A barrier wall can be only as strong as the materials supporting it. Industry cannot afford to rely on vendor assurances of security absent independent validation and testing to standards equivalent to those applied for safety. Strong and secure components are necessary for ISA99/IEC62443-complient implementations.

ISA99/IEC62443 provides sound direction for improving the confidential status, integrity, and availability of components or systems used for industrial automation and control, and for criteria in procuring and implementing secure control systems. The guidance seeks to improve system security and help identify vulnerabilities in order to address them. The intent is to reduce the risk of compromised confidential information, and of degraded the equipment or process under control.

Confidentiality, integrity, and availability, collectively, form the basis of businesses IT security. For enterprise systems, the first priority is confidentiality. Logically, for real-time operational systems used in industrial settings, the priorities are reversed, with availability shifted to top priority. The control system must operate 24 hours a day without interruption for extended periods. Systems are designed to operate at multiple levels, with redundant control computers backed up by local controllers that are, in turn, backed up by safety shutdown systems.

TRUSTING "SECURITY-BY-DESIGN"

A critical step toward adopting good security involves method of implementation. Many protocols employ basic "security-by-design," a concept that incorporates security into all aspects of network design, construction, and operations. A successful security-by-design methodology results in a more robust security infrastructure that minimizes insider access to materials, as well as opportunities for risks associated with malicious acts (sabotage, diversion, etc.), while providing flexibility to respond to a changing threat environment.

To illustrate, wireless networks created under the ISA100.11a standard feature authentication and encryption controlled by a flexible security policy that can be varied under ISA100.11a's two-layer security approach. First, "link layer" security applies hop-to-hop authentication and encryption. ISA100.11a wireless subnets feature multi-hop, mesh-enabled subnets with packets of data routing over multiple devices to the subnet extraction point. Each router used in this structure authenticates and encrypts-decrypts the packet that it routes.

The security associated with the second layer, or "transport layer," provides end-to-end authentication and encryption of data messages. Here, the originating device authenticates and encrypts the packet at the transport layer, and only the destination authenticates and decrypts the packet. This is accomplished through sessions that are established between pairs of devices that communicate at the transport layer.

Various levels of authentication and encryption can be enabled for both layers of security, and these levels are inherited from the security policies supported by IEEE 802.15.4 -- the underlying wireless technology on which ISA100.11a is based.

Although ISA100 has security built in by design within the standard, it must still be implemented correctly. Improperly implemented security is equivalent to no security at all. Many vendors claim product functionality and offer security without any validation or oversight. Federal official assessments and daily updates from ICS-CERT published online[v] establish that the number of product vulnerabilities found in the industrial control sector continues to rise.

Independently validated and robust security products represent sound investments. Applying these standards result in security solutions that extend critical-infrastructure protection from the enterprise edge to the PLC, embedded controller, and other devices.

THE MULTILAYERED SECURITY APPROACH

A multilayered approach to security allows requirements for function and security to be met at the same time. The vulnerability created to enable more efficient operation can be mitigated with a different layer of security. Combining these layers afford protection greater than that provided by any single layer.

Industry -- including product developers, systems integrators and plant operators -- must plan, design for and implement multilayered security when fielding products and systems. By utilizing layers of defense, and recognizing that the internal network might be (or become) infected, systems can be connected across trusted or un-trusted networks without compromising security. Only the systems designed to communicate with each other should be able to do so; they must, in effect, be isolated from other network communications and devices.

Air gapping	Separate one network from another: Considered robust, but not difficult to inject a problem, even if accidentally.
Firewalls and demilitarized zones (DMZ)	Used on the business perimeter, and on internal perimeters. This allows access needed to obtain a report from a server, as well as access for data logging to a historian; however, routing directly across the two devices is not possible.
Programmable switching	Route traffic from one device to another without broadcasting across the network. This reduces communications traffic and can limit access to other networked resources.
Virtual private networking (VPN)	VPNs are often used to create a tunnel between a device such as a laptop and the corporate network over an unsecure network, often the Internet. They can also be used to connect remote systems.
Unidirectional devices or data diodes	Unidirectional gateways allow traffic in one direction only. This effectively prevents data and other transmission to one way, similar to an air gap. Unauthorized interception is prevented -- transmission is encrypted and cannot be intercepted or deciphered.
Deep packet inspection	Inspect and manage traffic at the edge, not just at the firewall, using deep packet inspection, logging, reporting and control.
Device-level authentication	Ensure integrity and source validation -- devices cannot communicate with other devices without authorization.
Physical security layer	Physical security with intrusion detection and prevention.

CONCLUSIONS

Cyber security often is presented as complicated, full of technical jargon, difficult to grasp, and often at odds with safety. In reality, the concepts of cyber security are straightforward. It is the implementation that is difficult, and security should complement safety. When the cyber risk cannot be adequately explained, or understood, then any mitigation solution cannot be validated for effectiveness. Managers cannot say they have controlled it. Security, like safety, is an inherent foundation for any industrial automation facility, and so must be appreciated and integrated throughout the system lifecycle.

Two fundamental questions should be asked by every industrial control owner relative to security: 1) What is actually being protected and, 2) Will it reduce the risk of attack. An industrial control or automation system is not the same as an enterprise IT system for the simple reason that the risks and the impacts are different. Security solutions must fit within the operational constraints of the system, and within the risk appetite of the client organization. Otherwise, the fix can cause a greater impact overall than an attack.

ABOUT THE AUTHOR

Dr. Alex Tarter, Technical Director, Cyber security Group, Ultra Electronics, 3eTI
The author, Alex Tarter is an expert and thought leader on new technologies and solutions for industrial and commercial applications for the protection of critical infrastructure. In addition to the work he does developing security solutions, Alex performs vulnerability and cyber security work for military and industrial applications, having prepared more than 50 reports on various aspects of security and situational awareness for industry, UK MoD, and US DoD. He holds a PhD from Lancaster University, and a Master's of Engineering from Imperial College London. He serves as a civilian advisory expert to NATO on Cyber Defense for the Industrial Resources and Communications Services Group.

KEYWORDS:
Cyber security, industrial control systems, encryption, embedded OEM encryption, secure energy management, intrusion detection, access control systems, layer 2, layer 3 security, process control network security, Machine-to-Machine (M2M), risk mitigation, risk management

---

[i] Gartner, June 11, 2013: "Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013." Read more.

[ii] Homeland Security News Wire, January 14, 2013: "DHS: Industrial control systems subject to 200 attacks in 2012." Read more.

[iii] New York Times, October 11, 2012: "Panetta Warns of Dire Threat of Cyberattack on U.S." Read more.

[iv] ISA99 is the Industrial Automation and Control System Security Committee of the International Society for Automation (ISA). The purpose of the ISA99 Committee is to develop and establish standards, recommended practices, technical reports and related information to define procedures for implementing electronically secure industrial automation and control systems, and security practices.

[v] ICS-CERT Vulnerability Disclosure Policy: http://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy.