SIEMENS

White Paper

Securing Industrial Control Systems:

The Challenge and Common-sense

Industrial control systems (ICSs) across numerous industry verticals are increasingly migrating from serial communications to Internet Protocol (IP)-based communications as Operational Technology (OT) networks are integrated with Information Technology (IT) networks for enhanced performance, reliability, efficiencies and other operational advantages.

The convergence of OT and IT networks, however, has introduced new challenges and threats to ICSs. Because ICSs monitor and control physical processes in the real world, they have more stringent response requirements for determinism and real-time data transfer.

Determinism describes a known, measurable parameter for the speed and reliability of signals in the network and ICSs require low to zero latency in response time and low to zero variance in that response time (aka, "jitter"). As a result, OT networks have different Quality of Service (QoS) considerations than IT networks, depending on the specific industry vertical employing the ICS.

Traditionally, ICSs were isolated systems and, thus, secure from network-based threats. The trend from serial-based networks to IP-based networks has introduced potential vulnerabilities and threats common to ICSs in manufacturing or critical infrastructure sectors such as power and energy, transit, and advanced traffic control.

ICSs in these branches are increasingly vulnerable to cybersecurity attacks with potentially devastating impacts to brands, businesses, and public safety.

A significant proportion of industrial plants and ICSs in operation today were designed and implemented prior to the need for various security measures common to IT networks. Inter alia, these measures include access policies and controls to enforce them, authorization and authentication procedures or policies to facilitate change management, and activity or audit logs that support forensic investigations into security breaches.

Potential impacts

A breach of a company's IT network can have adverse impacts on day-to-day business operations. Examples of this include cyber theft of intellectual property or customer information, or the disabling of a business's public-facing website. In contrast, a breach of an ICS that serves OT can interrupt production, damage physical assets, and even result in injury or death to employees and public alike. These potential impacts are magnified when the target is critical infrastructure.

Cyber-attacks increasing

A 2016 study by Booz Allen Hamilton, "Industrial Cybersecurity Threats are on the Rise," found that cyberattacks on ICSs are increasing and likely to expand.

The Booz Allen Hamilton study cited publicly available data for 314 organizations worldwide in which 34 percent of ICS operators reported more than two breaches of their systems over the preceding 12 months. Forty-four percent could not identify the source.

In a 2016 article by U.S. News & World Report that focused on a specific industry vertical, "Cyberattacks Surge on Energy Companies, Electric Grid," 150 energy companies and electric utilities reported a successful breach of their networks in the prior 12 months, nearly half reported that such attacks had recently increased, and more than 80 percent expected that physical harm to facilities would result in the ensuing year. "Intruders were able to breach one or more firewalls, antivirus programs or other protections," the magazine reported.

A SecurityWeek analyst recently identified "The Top 3 Threats to Industrial Control Systems": external threats by nation states, terrorists or hacktivists, internal threats from disgruntled employees or contractors, and simple human error – perhaps the most pervasive and potentially damaging threat of all.

What this means to your business

Cyber threats to ICSs have become a fact of life. Many subject matter experts argue that these threats must be addressed with common sense and known methodologies – whether cyberattacks affect your business is a matter of when, not if.

According to the Infosecurity Group, which studies ICS risks, an attacker or malware spent an estimated 243 days on a business' network before being discovered, it took an average of 32 days to resolve such an attack and 63 percent of affected businesses had to be notified of a breach by an outside organization such as the Department of Justice, Homeland Security or National Security Agency.

Clearly, eliminating all threats may not be feasible, given that human error can be a major factor and that malicious attacks are becoming more sophisticated and frequent. However, effective strategies, backed by proven security measures, can prevent most human error, detect, isolate and mitigate malicious attacks and their impacts, and provide resiliency to ICSs.

Common concerns

Executives and managers with responsibility for ICSs often say that their biggest frustration is a lack of precise knowledge of what resides on their networks. They express similar concerns about accidental or intentional breaches of their network, as well as complying with regulatory bodies and practicing overall responsibility for ICS security.

Fortunately, well-established strategies, proven technologies, and a trusted advisor with deep experience in building, operating and protecting ICSs can address these and other concerns.

Defense in depth

On a conceptual level, subject matter experts point to the significant difference between compliance and security. Compliance with regulations may be defined as conforming to a set of rules or standards, subject to an audit based on inquiry and inspection by a third party or authority.
In contrast, security is defined as the implementation of technical, physical and administrative measures and controls to provide confidentiality, integrity and availability. In this context the administrative measures can also address accountability and assurance aspects.

Stated simply, compliance does not equal security. Compliance is merely a snapshot of how your security program meets a specific set of security requirements established by regulators at a given moment in time. Security is a much broader concept and requires going beyond compliance and its checklist of actions and measures to a more comprehensive approach.

The concept of "Defense in Depth" is an industry best practice involving multiple layers of protection that detect, prevent and mitigate human error or malicious intrusions. Defense in depth for protecting ICSs relies on the tendency of an attack to lose momentum over time; it can protect against common attacks or human misbehavior but it can also delay targeted and sophisticated attacks to buy time for mitigating the threat.

A useful analogy is the multiple measures most people use to protect their homes. Locking the doors is a first step, but that single, mechanical approach often proves insufficient to stop a burglar. Home security is enhanced by multiple layers of protection that slow an intrusion long enough to detect it and stop it. Motion sensing lights, a dog barking, and a house alarm system that alerts authorities to a breach all contribute to addressing various threats and mitigating risk

In an ICS, a defense-in-depth approach requires Plant security (e.g. physical access protection, processes and guidelines, holistic security monitoring), Network security (e.g. cell protection, perimeter network protection, firewalls, VPNs), and System integrity (e.g. system hardening, patch management, detection of attacks, authentication and access protection) to address the multiple attack vectors of that system. Though most companies implement measures against one or more of these vectors, too few adequately address all of them in a holistic strategy. In other words, individual measures such as passwords or firewalls alone cannot meet today's cybersecurity threats. Instead, by employing established procedures and technologies at each of these levels, defense in depth can minimize downtime or potential harm from cyberattacks.

The role of a trusted advisor

Few enterprises go it alone on cybersecurity, due to the breadth of experience with all security measures of defense in depth that is required. A trusted advisor should begin by listening and assessing a company's existing approaches to cybersecurity before addressing potential solutions to remaining gaps in those approaches.

Designing and implementing solutions at each layer of a defense in depth approach typically requires a trusted advisor with long standing experience in the industrial controls domain and expertise in operational technologies, ICS and the industry verticals in question. That domain experience and expertise should be complemented by good security know how, robust software solutions and reliable, industrial-strength hardware to support them.

A list of industry verticals that must address cyber threats to ICSs underscores the importance of selecting a trusted advisor with the breadth of experience, the depth of expertise and the portfolio of solutions to implement defense in depth in ICSs. That list includes manufacturing, food and beverage, pharma, water & waste water, electric power generation, transmission and distribution, renewable energy facilities, oil and gas wells, pipelines and refineries, railroads and intelligent transportation systems for urban traffic control.

In a crowded marketplace brimming with "solutions," it isn't enough to turn to information technology (IT)-savvy vendors who are just learning about the operational technologies at stake in protecting ICS networks. Additionally, simply purchasing and plugging in hardware without a holistic cybersecurity strategy and software solutions to run on that hardware would be ill-advised.

Instead, a proven solution provider and partner in cybersecurity should have a long track record in manufacturing, implementing, trouble-shooting, and safeguarding operational technologies that run on ICSs in the pertinent industry verticals of power, energy, and transportation.

Figure 1

Three layers and solutions

Figure 1 illustrates the three layers of a holistic, defense in depth strategy. No single layer is more important than the others; all layers play a role in defense in depth. But it is helpful to use Figure 1 to envision how the layers relate to each other and to a holistic strategy.

The devices and data to be protected sit at the core, where access controls ensure that only the right person with proper authorization can interact with this layer in the right place and time. Solutions must be proven, scalable, and intuitive for end users, while meeting national and global cyber-security requirements and standards, including those for encryption.

Plant security

Plant security goes hand-in-hand with cybersecurity and starts with conventional building access and extends to securing of sensitive areas by means of key cards, locks, and security cameras. Plant security includes processes and guidelines for comprehensive plant protection. These range from risk analysis and the implementation and monitoring of suitable measures to regular updates.

Network security

The network layer must be protected by firewalls, virtual private networks (VPNs) and network intrusion detection capabilities that work in concert with other elements of a defense in depth strategy to thwart cyberattacks. Firewalls provide monitoring and control of network traffic according to security rules. VPNs encrypt data traffic between central and peripheral computing units on a network.

System integrity

To both protect existing knowledge and prevent unauthorized access to your automation processes protecting the integrity of your ICS is imperative. Protection of application firmware and system/host software is a key part of maintaining system integrity. This can be done by system hardening, regular patch management, and other integrity protection methods.

Perhaps most importantly, the human element involved with the implementation, maintenance, and operation of these systems is crucial to defense in depth. By raising awareness of proper cybersecurity policies and procedures through proper training, the workforce can be prepared to meet cyber threats.

Siemens' deep expertise in ICS cybersecurity

Siemens' heritage is predominantly based in operational technologies and, thus, in ICSs, with deep knowledge of cybersecurity and related industry verticals. Its suite of proven cybersecurity solutions and services can address each of the layers in a defense in depth strategy. Our professional services teams can assess ICS vulnerabilities and design solutions to build defense in depth and follow through with implementation.

Siemens' unique value proposition is its deep experience in protecting ICS networks and supporting its software-based solutions with hardware engineered for industrial environments, which sets it apart from recent market entrants and their IT-based offerings.

For instance, Siemens' asset inventory and management tools provide a solution to ICS managers concerned that they don't know what devices are on their network. Siemens can also assist if the goal is end-to-end cybersecurity and act as an advisor to help comply with regulatory mandates. If the ever-present possibility of human error – or malicious attacks – drives cybersecurity concerns, Siemens' authentication, password management, and intrusion detection solutions address these vulnerabilities.

Let's talk

Your approach to cybersecurity and ICSs may already rely on Siemens' expertise and experience and its approach to defense in depth and our proven strategies, software and industrial hardware platforms. Or you may be focusing on ICS cybersecurity for the first time. In either case, maintaining a dialogue with a trusted advisor on your ongoing industrial cybersecurity needs should be on your to-do list.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

PDF
WhitePaper
BR 0318 / 5 En
Produced in Germany