Revealing network threats, fears

How to use ANSI/ISA-99 standards to improve control system security

By Eric Byres

Anyone integrating automation technologies these days is well aware of the pressure on the operators of industrial plants to increase productivity, reduce costs, and share information in real time across multiple industrial and enterprise systems. Adding to these business pressures is the growing fear of cyber attack as the world has become aware that the Stuxnet worm was specifically designed to disrupt an industrial process. Operators and engineers are under pressure to isolate automation systems at the same time as management is asking for greater interconnectedness.

This article explains how the ANSI/ISA-99 security standards provide a framework for helping deal with network security threats that arise from the "push for productivity" and the fear of the next "Son-of-Stuxnet" worm.

1. Why the "push for productivity" has degraded control network security

As corporate networks have converged with industrial networks, there have been many integration projects where proprietary networks or equipment were replaced with TCP/IP networks

and commercial-off-the-shelf equipment. This shift in technology has greatly increased the complexity and "interconnectedness" of control systems. As a result, they now have many of the same vulnerabilities that have plagued enterprise networks. In addition, the controllers in these networks are now subjected to new threat sources that they were never designed to handle.

The result has been a significant increase in the number of plant disruptions and shutdowns due to cybersecurity issues in the control networks at industrial facilities.

The Repository for Industrial Security Incidents (RISI—www.securityincidents.org) is the world's largest database of security incidents in control and SCADA systems. An analysis of the data from 1982 to 2009 found the type of incidents breaks down as follows:

- 76% of incidents were accidental in nature
- 24% of incidents were due to malware

In our study of the incidents in the RISI database, we see problems arising from three common sources:

a. Proliferation of "soft" targets: Control systems devices were designed with a primary focus on high-performance real-time I/O, not robust networking. Many devices will crash if they receive malformed network traffic or even high loads of correctly formed data. Also, Windows PCs in these networks often run for months at a time without security patches or antivirus updates and are susceptible to even outdated malware.

b. Multiple points of entry: Even without a direct connection to the Internet, control systems are accessed by numerous means, including:
   - Remote maintenance/diagnostics connections
   - Shared historian and Manufacturing Execution Systems (MES) servers
   - Serial connections
   - Wireless systems
   - Mobile laptops
   - USB devices

   These pathways can be exploited by malware and other disruptive elements.

c. Poor network segmentation: Control networks are now more complex than ever before, consisting of hundreds or even thousands of individual devices. Unfortunately, the design of many of these networks has remained "flat" with virtually no segmentation. As a result, problems that originate in one part of the network can quickly spread to other areas.

Mitigations

There is limited opportunity for control system engineers to address the first source in the short term. Most plant operators are dependent on their equipment vendors to secure the controllers and software that they use. With the competitive pressure that most companies face to improve productivity and access to the systems and data in their plants, it is unlikely they will be able to significantly reduce the number of internal and external pathways into their plants. However, operators can implement good network segmentation, and we address this topic in this article.

2. The fear of "Stuxnet 2" and its impact on industrial control project priorities

2010 was a watershed year for industrial cybersecurity because of the identification of the Stuxnet worm and the wake-up call it has created for operators of all industrial facilities. Stuxnet has given a clear warning: Secure your control and automation systems, or the reliability and safety of your entire operation is at risk.

For those of you who have not closely followed the Stuxnet story:

- The Stuxnet worm was discovered in June 2010 by a Belarus-based company doing business in Iran.
- It is a very advanced computer worm that took many man-years to create. It was designed to jump from computer to computer using human and network pathways until it found the specific, well-protected control system it was designed to destroy (most likely Iran's nuclear enrichment program).
- Once it penetrated the facilities in Iran, Stuxnet targeted Siemens programmable logic controllers (PLCs) and human machine interfaces (HMIs). From there, it modified commands and data going to the frequency converters that regulate the speed at which centrifuges spin to enrich nuclear fuel. The worm made the centrifuges turn very quickly so they were damaged, but not destroyed. The worm also masked the changes in speed or PLC logic from being discovered at the operator's control panel.
- At its height, Stuxnet infected an estimated 100,000 computers and 50 to 60 industrial control systems around the world.

Most facilities will not be subject to an attack as sophisticated as Stuxnet. However, the worm's existence has paved the way for future industrial control system attacks

FAST FORWARD

- RISI data shows security problems arise from three common sources: proliferation of "soft" targets, multiple points of entry, and poor network segmentation.
- ISA-99 introduces the concepts of "zones" and "conduits" as a way to segment and isolate the various sub-systems in a control system.
- "Defense in depth" is multiple layers of defense distributed throughout the control network.

and abolished the concept that "security by obscurity" protects automation systems. As well, the detailed and public analysis of Stuxnet's design has become an "instruction manual" for future worm developers, showing them how to attack other industrial systems.

3. ISA-99 standards and solutions that work on the plant floor

To reduce cybersecurity issues in control networks, either due to technology convergence or for "Son-of-Stuxnet" protection, well-designed network segmentation is critical. This topic is addressed as part of the ANSI/ISA-99 Standards: Security for Industrial Automation and Control Systems.

ANSI/ISA-99 is a complete security life-cycle program, with best practices for developing and deploying policy and technology solutions to address security issues in control systems. In this article, however, we will focus on one aspect of the standard—containing communication in control sub-systems to avoid having security issues in one area migrate to another area.

ISA-99 introduces the concepts of "zones" and "conduits" as a way to segment and isolate the various subsystems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors such as criticality and consequence. Equipment in a zone has a security level capability. If that capability level is not equal to or higher than the requirement level, then extra security measures, such as implementing additional technology or policies, must be taken.

Any communications between zones must be via a defined conduit. Conduits control access to zones, resist Denial of Service attacks or the transfer of malware, shield other network systems, and protect the integrity and confidentiality of network traffic. Typically, the controls on a conduit are intended to mitigate the difference between a zone's security level capability and its security requirements. Focusing on conduit mitigations is typically far more cost effective than having to upgrade every device or computer in a zone to meet a requirement.

Sub-section number and description	Requirement
4.3.2.3.1: Develop the network segmentation architecture	A network segmentation countermeasure strategy employing security zones shall be developed for Industrial Automation and Control Systems (IACS) devices based upon the risk level of the IACS.
4.3.2.3.2: Employ isolation or segmentation on high-risk IACS	Any high-risk IACS zone shall be either isolated from or employ a barrier device to separate it from other zones with different security policies, levels, or risks. The barrier device shall be selected commensurate to the risk reduction required.
4.3.2.3.3: Block non-essential communications with barrier devices	Barrier devices shall block all non-essential communications in and out of the security zone containing critical control equipment.

Figure 1: Key recommendations from ANSI/ISA-99.02.01

Zone and conduit design starts with the facility being analyzed to identify groups of devices that have common functionality and common security requirements; these groups are the "zones" of equipment that require protection. For example, a facility might first be divided into operational areas, such as materials storage, processing, finishing, etc. Then within these areas, it could be further divided into functional layers, such as MES, Supervisory Systems (i.e., operator HMIs), primary control systems (i.e., PLCs), and safety systems. Often, the models from other standards such as ANSI/ISA-95.00.01-2000 or the Purdue manufacturing model are used as a basis for this division.

The next step is to discover the pathways in the network through which data is passed between these zones; these are the network "conduits." Industrial firewalls can be installed in these conduits and configured to pass only the minimum traffic that is required for correct plant operation, blocking all other unnecessary traffic.

Good network design would also suggest the firewalls should implement some kind of alarm reporting mechanism to alert operations or security personnel any time that abnormal behavior (i.e., blocked traffic) is observed in the network.

This approach implements a strategy of "defense in depth"—multiple layers of defense distributed throughout the control network—which has been proven in the IT community to be a strategy that works well.

Consider how a network protected in this manner would respond to threats such as a traffic storm created by a device failure or a "Son-of-Stuxnet" virus. The impact would be limited by the firewalls to the specific zone in which the problem occurred, and the alarm messages from the firewalls would pinpoint the zone and even the source device where the problem originated.

A real-world example

An example from a real customer application shows how an ISA-99 "zones and conduits" analysis was performed in a refinery to analyze the potential threat sources and develop a plan to protect the plant. A high-level network diagram of the refinery is shown in Figure 2.

For simplicity, only two refinery operations areas (Op #1 and Op #2) are shown, but in real life, there were multiple operations. Each operation has its own basic control, safety, and HMI/supervisory systems. These systems connect to a common Process Information Network, where Historian and MES servers are accessible from the Enterprise and control networks. In addition, wireless sensors are being deployed throughout Op #2, and a Remote Access gateway is provided to permit remote maintenance on plant systems by the control system engineers.

The first step was to identify the "zones" of devices with common functionality and common security requirements. The next step was to identify all the conduits that exist in the plant network. The result of this analysis is

shown in Figure 3.

Following this analysis, the potential threat sources and consequences of an attack were identified and reviewed with the plant engineers. Through this analysis, it was evident the safety integrated system in each operational unit should be located in its own zone. To ensure continued safe plant operation, it was vital that the safety system could not be compromised from the plant control network. These were the first zones to be protected with "plug and protect" security appliances.

4. Implementing ISA-99 zones and conduits with industrial security appliances

Some industrial security appliances are engineered specifically to support a "defense in depth" strategy in control networks. These are the ideal platform on which to base an ANSI/ISA-99 zones and conduits deployment.

On start-up, any industrial security appliance should be "plug and protect" ready. That is, as shipped from the factory, it transparently bridges all traffic between its Ethernet ports, so it can be installed in the control network without any changes to the design or IP addressing of the network. Some industrial security appliances can be fine-tuned for a particular purpose by installing firmware modules that implement security features, such as firewall, asset management, VPN, and content inspection of particular protocols, such as Modbus or OPC.

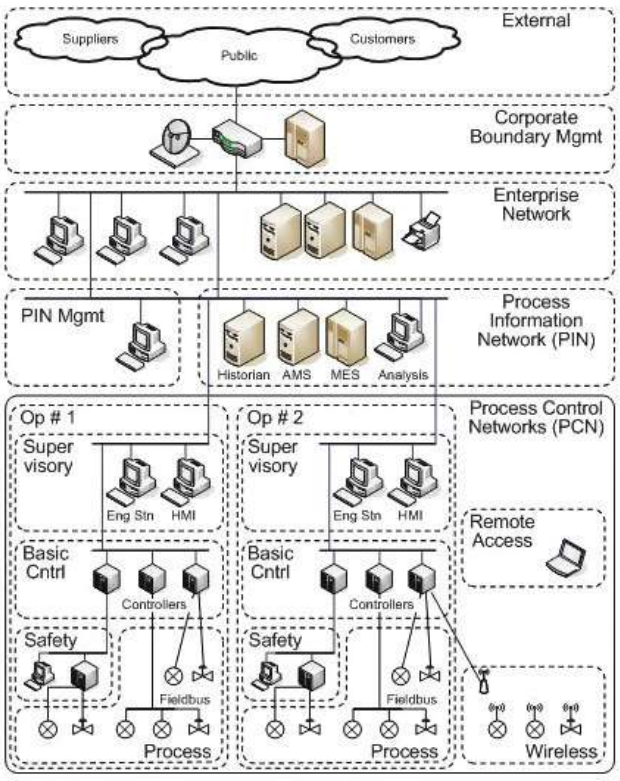
In an ANSI/ISA-99 zones and conduits deployment, industrial security appliances would be installed in each conduit that was identified in the network. Once this is done, a firewall module can be activated in each appliance to provide the capability to filter all traffic passing through that conduit. The firewall makes it simple to build intrinsically secure networks because it automatically blocks and reports any traffic for which there is no "allow" rule. The control system engineer need only configure firewall rules that specify which devices in the network will be allowed to communicate through the conduit and what protocols they may use, and the industrial security appliance will block any other traffic not matching these rules.

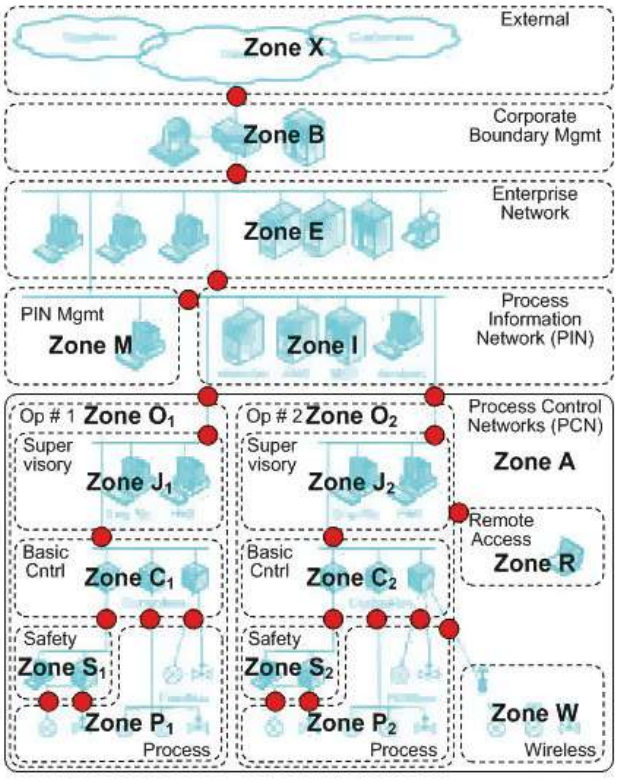
Testing the system

Ideally, the industrial security appliance's configuration tools are designed specifically to match the needs and capabilities of the control engineer. Such tools make it very easy not only to configure firewall rules, but also to test them before they are actually implemented.

For example, there should be a "Test" mode that transparently bridges all traffic through the device, but reports any traffic that would have been blocked if the firewall rules had been active. This permits the control engineer to interactively edit and test the rules in the network using real network traffic, but with no risk of accidentally shutting down the plant. When no more "blocked traffic" alarms are generated by the device, the engineer can have a high level of confidence that the firewall rules are correct and complete, and that it will be safe to switch the security appliance to "Operational" mode where the firewall rules will be enforced.

Typical control networks will have multiple conduits distributed over many locations in a plant. Preferably





the multiple industrial security appliances can be managed from a single management console application.

Summary

New network and PC-based technologies introduced into control systems have provided tremendous improvements in plant performance and productivity. In 2010, the Stuxnet malware showed us sophisticated viruses targeted at industrial processes exist and are likely to be more common in the future. The impact of these two trends will be to increase the urgency and thus project priorities for cybersecurity initiatives that improve control network security and reliability.

The ANSI/ISA-99 standards provide a framework for companies to achieve and maintain security improvements through a life cycle that integrates design, implementation, monitoring, and continuous improvement. System integrators and control engineers who become proficient with segmenting control networks for zones and conduits, and who gain expertise with appropriate industrial security solutions, will be able to mitigate cybersecurity threats that arise from the "push for productivity" and "Son-of-Stuxnet" malware.

ABOUT THE AUTHOR

Eric Byres, ISA Fellow, is a security expert and CTO of Byres Security. His e-mail is eric@byressecurity.com. Byres is heading an ISA committee that will conduct a gap analysis of the current ANSI/ISA-99 standards to see if companies following this standard would have been protected from Stuxnet.

View the online version at www.isa.org/intech/20110204.

RESOURCES

Stuxnet
www.tofinosecurity.com/stuxnet-central

ANSI/ISA-99.02.01
www.isa.org/link/ISA99_09

Building Intrinsically Secure Control and Safety Systems
www.isa.org/link/Build_secure