Belden on Industrial Security

Excerpts from the Belden Blog

Featuring: Heather MacKenzie & Oliver Kleineberg

Contents

ICS Security: 3 Ways to Get Started

By: Heather MacKenzie

If you're like me, when you don't know how to do something you avoid or delay doing it. Even though I love learning new things and tackling new adventures, in the context of work, there never seems to be enough time. That means taking on a new challenge or learning best practices about a new topic is often put on the back burner.

If cyber security is a new area for you, then this is an article you really want to read. It is short and it explains three important concepts that once you know, you can start putting into practice right away.

Think of it this way, cyber security is a topic of high concern at the top levels for all companies. Plus, the Industrial Internet of Things (IIoT) is connecting more devices and systems to the control network, increasing the likelihood of cyber incidents. It's more important now than ever before to understand the principles of cyber security. Let's get started….

One essential concept for ICS security is to protect your most important assets first. In the case of a water filtration plant that is likely the PLCs that control chlorine levels.(From the Belden Blog)

1. ICS Security Principle: Start with a Risk Assessment

Starting with a risk assessment is a best practice recommended not just by Belden, but by many security consulting firms and standards groups. You need to understand your network's level of risk and rate the state of cyber defenses at your facilities.

This might sound like a big project, or a costly consulting engagement. However, it is possible to do it internally and at no cost. While this may not be for everyone, it could be a viable option if a third-party assessment is not in your budget right now. It is also a heck of a lot better than doing nothing about improving the security of your Industrial Control System (ICS) network.

The steps for implementing a zero-cost industrial security risk assessment include the following:

- Determine who should help with the risk assessment (consider IT personnel, an executive and a person from each type of job in your company)
- Identify critical assets
- Prioritize and list the largest risks for each asset
- Prioritize the list of industrial security assets
- Determine and rate existing protection measures

Learning this process is important and it is not a one-time exercise. Good security requires monitoring, evaluating and improving your plans regularly in order to ensure current measures are working effectively. This will also help you to recognize new or developing risks to the network.

2. ICS Security Principle: Plan a "Defense in Depth" Strategy

After completing the risk assessment, you need to create a plan to secure your network. The approach you want to take is called Defense in Depth (DiD), which includes multiple layers of defense distributed throughout the control network.

A well-developed DiD strategy includes:

- Multiple layers of defense instead of relying on a single point of security
- Differentiated layers of defense, ensuring an attacker can't access all subsequent layers after getting past the first
- Context- and threat-specific layers of defense, meaning each layer is optimized to deal with a specific class of threats

If your network is protected by a DiD strategy, the impact of an accidental security incident or a malicious attack will be limited to the zone where the problem began. You want to set up your systems so that the right people or teams receive an alarm and the work to identify the issue begins in a timely fashion.

3. ICS Security Principle: Protect the Crown Jewels First

Lastly, you must prioritize the crown jewels. What are the crown jewels? Think of the systems that would cause a complete disaster for your network if they were shut down (either unintentionally or maliciously).

These might be the safety integrated system (SIS) in a refinery, the programmable logic controller (PLC) managing chlorine levels in a water filtration plant, or the remote terminal unit (RTU) in an electrical substation. Every control engineer knows what really matters to his or her particular operation. Aggressively protect this asset and the chance of a truly serious cyber incident is greatly reduced.

Control systems have become complex and difficult to protect at all times, so focus your resources on securing those assets that really matter to the survival of the company.

Don't let the complications brought on by the IIoT's increased connectivity or the high cost of formal risk assessments keep you from protecting your network effectively. By taking the right steps to understand your risks, choosing a layered approach to your ICS security, and prioritizing your most important assets, you can successfully protect your network in our increasingly connected world.

Written by Heather MacKenzie of the Belden Blog, August 19th, 2015. Find it here http://belden.com/blog/industrialsecurity/ICS-Security-3-Ways-to-Get-Started.cfm

A 1-2-3 Approach to Industrial Cybersecurity

By: Heather MacKenzie

One of the best parts of the Belden Industrial Ethernet Infrastructure Design Seminar, held last week in Chicago, was the lively presentation given by two of Belden and Tripwire's top experts on industrial cybersecurity:

- David Meltzer, Chief Research Officer of Tripwire
- Jeff Caldwell, Chief Architect-Security at Belden

If you are not familiar with Tripwire, the company provides advanced threat, security and compliance solutions for more than 9,000 organizations, including nine of the top 10 utilities in the U.S. Tripwire was acquired by Belden earlier this year and is an important part of our increased focus on network security solutions.

In their Design Seminar presentation David and Jeff spoke about the nature of cybersecurity incidents occurring in industrial networks today. They went on to discuss a 1-2-3 approach to securing industrial networks. Find out about this approach and how Belden and Tripwire products contribute to it.

David Meltzer of Tripwire (on the left) and Jeff Caldwell of Belden (on the right) discuss ICS Security at the 2015 Belden Design Seminar. (From the Belden Blog)

Most Industrial Cyber Incidents are Unintentional

The vast majority of cyber incidents on industrial networks are unintentional, resulting from:

- Human error, for example device configuration errors
- Software or device flaws, such as legacy equipment that fails when overloaded with multicast traffic
- The accidental introduction of malware, for example via a USB stick or a vendor laptop

An example of this type of incident was the manual shutdown of the Browns Ferry Nuclear Power Plant in 2006. Redundant drives controlling the recirculating water system failed due to "excessive traffic" on the control network. Network traffic between two different vendors' control products was the likely cause. The facility remained offline for 2 days, and $600K of revenue was lost.

While only about 20% of incidents are intentional, those from external hackers have become more and more sophisticated. ICS-CERT estimates that 55% of such ICS attacks come from Advanced Persistent Threats (APTs). APTs are carefully crafted attacks against a focused target that are designed to be effective over an extended period of time. Classic examples of such attacks on industrial systems are Stuxnet, Flame and the Dragonfly malware campaign.

Belden's 1-2-3 Approach to Industrial Cybersecurity

In order to protect availability, Belden has developed a 1-2-3 approach to industrial cybersecurity:

To protect against both unintentional and intentional threats to ICS security, Belden has developed a 1-2-3- approach. (From the Belden Blog)

At a high-level our portfolio of industrial networking solutions contributes to these three levels of protection as follows:

Industrial Cybersecurity Protection Areas			
	Industrial Network	**Industrial PCs**	**Industrial Controls**
Belden / Tripwire Products	Tofino L2 firewalls for network segmentation and zoning, including Deep Packet Inspection of industrial protocols	Industrial HiVision for asset inventory	Tripwire Log Center for detecting attacks and unauthorized changes
	Hirschmann EAGLE L3 firewalls for multipurpose protection of data availability	Tripwire Security and Configuration and Compliance Manager	Tripwire Vulnerability Management for identifying exploitable controls
	GarrettCom & Hirschmann routers for physical and VLAN network segmentation	Tripwire Log Center for insights on suspicious events	
	Industrial HiVision for network monitoring, accurate configuration and security lockdown of devices	Tripwire Vulnerability Management	
	Hirschmann OpenBAT products for secure wireless		
	Hirschmann switches for device-level security and zero-failover redundancy		

(From the Belden Blog)

All together Belden and Tripwire's solutions are being engineered to work together to deliver the "Belden Safe Network Architecture."

David and Jeff's talk also hinted at new Belden/Tripwire cybersecurity solutions to come – and I for one am really looking forward to learning about them. Stay tuned…..

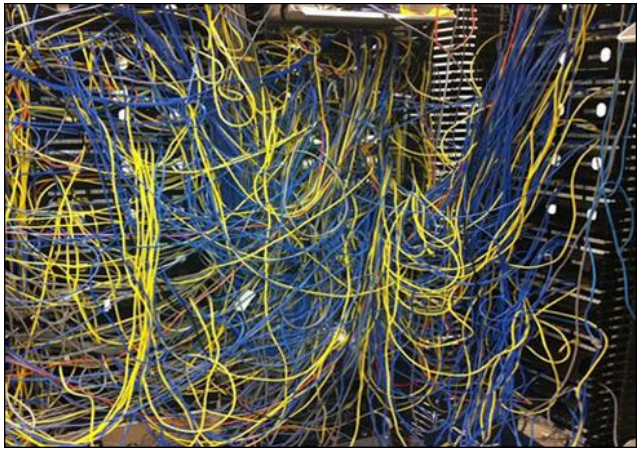
Written by Heather MacKenzie of the Belden Blog, October 28th, 2015. Find it here http://belden.com/blog/industrialsecurity/A-1-2-3-Approach-to-Industrial-Cybersecurity.cfm

ICS Security Depends on Good Network Design

By: Heather MacKenzie

A proper network design can be the difference between a secure, rugged process that keeps running smoothly or a nightmare that is not reliable. In a manufacturing enterprise the industrial network is often unnoticed or unappreciated. Yet a poorly designed network can take away from the bottom line.

“Ethernet today is not the same as it was when it was invented 40 years ago,” said Jim Laurita, technical service manager in Belden’s Industrial IT group. His talk “Industrial Ethernet Infrastructure (IEI): Design Best Practices” opened the Belden Design Seminar, held last month near Chicago, IL. “There have been steady improvements.”



Poor organization and design of an industrial network leads to downtime and cybersecurity incidents.(From the Belden Blog)

The Evolution of Industrial Ethernet Infrastructure

Among the improvements have been increased bandwidth, full duplex communication, bi-directional communication, no collisions, switching, prioritization and segmentation via a VLAN, Laurita said.

The beauty of Ethernet is that it keeps developing with greater robustness. Bandwidth speed is increasing, there is a lower cost, it is an open technology and it is a non-proprietary solution.

The beauty is the manufacturing sector can learn from how IT handled and used the technology.

“Automation is lagging behind IT by many years. It has taken longer for Ethernet to gain wider acceptance,” Laurita said. “Control and automation systems and applications are migrating from proprietary to open standards to enable seamless connectivity.”

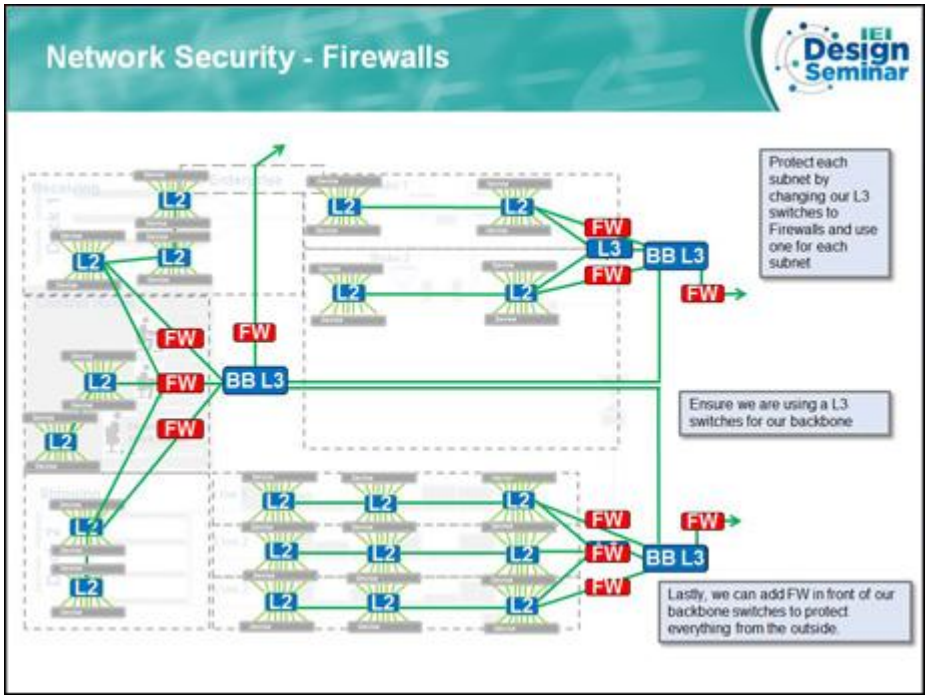
What Laurita wanted to stress is that open and viable Ethernet is here to stay and, knowing that, people need to understand good basic design principals necessary for a secure and viable network.

“There is a common misconception about networking that ‘I have installed this at home, how hard can it be?’” Laurita said. “The home network is not plug-and- play, it is more like plug-and-pray. The practice of just installing industrial Ethernet equipment randomly for connectivity is no longer practical.”

Key Components of Good Industrial Network Design

Laurita showed a basic manufacturing network and went over the various key components to assess:

- Consultation
- Physical side of the network
- Equipment selection
- Logical design
- Multicast control
- Redundancy
- Network security
- Wireless
- Other key aspects like Power over Ethernet (PoE), time synchronization, user interface, and ease of troubleshooting
- Network management



A properly segmented network utilizes subnets and industrial firewalls to ensure network security. (From the Belden Blog)

"Industrial Ethernet is more than just a physical ruggedization of IT equipment or block diagrams with lines," Laurita said. "Users need to determine the applications now and in the future and focus on total lifecycle and cost of ownership.

"In addition, designing an industrial network requires knowledge and cross-collaboration from many disciplines. There is not one person who knows all the answers."

In short, a secure network design works and ensures a smoothly running process.

"A well designed network will result in the highest level of availability and scalability for the future and enhance the total lifecycle manageability of the asset."

Written by Heather MacKenzie of the Belden Blog, November 11th, 2015. Find it here http://belden.com/blog/industrialsecurity/ICS-Security-Depends-on-Good-Network-Design.cfm

3 Ways to Use Industrial Firewalls for Defense in Depth

By: Oliver Kleineberg

An important best practice for industrial security is to implement a Defense in Depth strategy. With this approach, multiple layers of defense are implemented, in contrast to just one defense mechanism, such as a single firewall.

A complementary best practice used as part of a Defense is Depth strategy is Zones and Conduits, as defined in the ISA IEC 62443 standard. This involves segmenting the network into zones of devices with similar security requirements and using conduits to restrict the communication between zones.

Using Zones and Conduits as part of a Defense in Depth strategy is not a new concept. If you look at castle construction for any culture, you will see that layers of security were built into the castle design –moats, multiple walls, turrets. Individual zones of the castle are separated from each other by controlled conduits - gates, drawbridges and iron bars – to contain attackers and make their movements more difficult. Industrial firewalls play an important role in implementing both Defense in Depth and Zones and Conduits. Let's look at 3 examples of how they do it.

Industrial Firewalls Establish Network or Zone Boundaries

Firewalls are devices that protect networks or network devices, such as industrial PCs, control systems and other devices from unauthorized access by preventing traffic to or from these systems.

Using multiple layers of security (Defense in Depth) and containing attackers to a particular area (Zones and Conduits) are not new protection strategies -- they have been used for centuries in castle design. (Image is of Cité de Carcassonne, a medieval citadel in France. From the Belden Blog)

The fundamental technical function of any network firewall is to filter packets. The firewall inspects each packet it receives to determine whether the packet corresponds to a desired template for traffic patterns. The firewall then filters (drops or discards) or forwards packets that match these templates.

These templates are modeled in the form of rules. A firewall at the boundary of a network can, for example, include rules in the form of "A communication link within the network can only take place with a specified server" or "Only the PCs for remote maintenance can be reached outside the network, not any other devices."

There are many types of firewalls built for different use cases. They differ not only in their form factors, certifications, and physical specifications but also in the type of filtering they provide. For example,

a firewall designed to protect an operational zone of a plant floor with a sophisticated Deep Packet Inspection filtering capability might contain rules for industrial protocols, e.g. Modbus/TCP, such as:

"Write-commands for the Modbus/TCP protocol, coil 56, are permitted only from the maintenance terminal."

A detailed discussion of 3 different types of filtering done by industrial switches, routers and firewalls is available in a previous article.

But where are these firewalls used in today's security models?

Using Firewalls for Industrial Security

Firewalls play various roles in partitioning networks. Here are three common examples:

1. Boundary Firewalls

These firewalls are generally placed in the data center and typically work in tandem with industrial hardened firewalls such as the EAGLE 20/30 in the production area to isolate the critical control networks and the more exposed enterprise networks from one another.

Industrial firewalls with router functions are also perfect for smaller external sites. Because such a firewall represents the border between the company's own network (the external site) and an external network (a provider network or the Internet), the firewall must possess full capabilities for packet filtering and filtering traffic between various networks. Such a firewall is called an IP firewall since it processes Internet Protocol (IP) traffic.

These firewalls are often installed very near the actual facility, requiring industrial hardening of the firewall device. For example, the ability to function at high or low temperature ranges and/or approval for use in special areas (e.g. energy supply, hazardous location or transportation) may be critical.

2. Firewall in a WLAN

Wireless networks represent another network border, and communication from wireless to wired networks should also be protected by firewalls. If a client is connected to a WLAN, it is possible, in principle, to communicate directly with all other devices in the same network. Thus, a successful attack on a WLAN client could be extended to any other device on the Ethernet network.

Special firewalls that can also filter the direct traffic between wireless clients are required for this task. Normal edge firewalls are not up to this task. This problem can be solved by restricting the forwarding of messages between WLAN clients with a firewall at the WLAN access point. For example, the communication of a tablet that is connected to a device via a WLAN can be limited so that it only accesses data through the user interface but not additional subsystems or other devices connected to it.

This is the reason why Belden industrial wireless LAN access points, for example the OpenBAT products from Hirschmann, are all equipped with firewall functionality. Devices designed for industrial environments are important here as well.

3. Firewalls at the Field Level

A key tenet of Defense in Depth is that the protection of external network boundaries against attackers is insufficient security. Multiple layers of protection are required to provide safety against external threats. In addition, many cyber incidents actually originate inside a network. Industry studies have shown that most cyber incidents are not

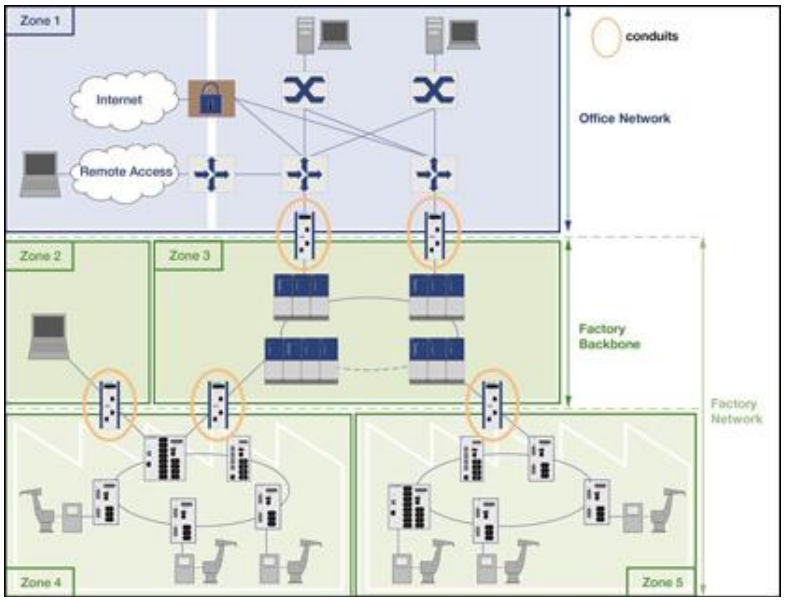
due to intentional external attacks but from software or device failures and human error.

In a networked control system, errors and mistakes can quickly propagate within the system unless proper design steps are undertaken to isolate and contain failures. Thus, an effective cybersecurity strategy is not just about security but is also an important component of ensuring the safety, resiliency and reliability of your system. This is exactly what ISA IEC 62443 and Zones and Conduits are targeted to address.

Firewalls can be used as the tool to implement the conduits that police the communication conduits. They contribute to the overall resiliency against unintentional errors by limiting communication between different zones of the local network.
This requires a firewall that is tailored to fit a particular use case. If communication from outside the facility is only supposed to be possible with a single device, the firewall should specifically permit this connection while it prevents other attempts at communication. To ensure only proper messages flow between zones and to critical assets, these firewalls must understand the origin and destination of the messages.

In addition, particularly for critical control systems, the firewall should also support detailed analysis of industrial protocol traffic (Deep Packet Inspection) so it can ensure the content of the messages is valid and reasonable. An example is the Tofino Xenon security appliance.

A word of caution about deploying firewalls: while effective in preventing unauthorized communication traffic on the network, these devices can also add latency or delays. Where rapid filtering must take place, high-quality network switches using hardware accelerated access control lists, can be an effective means to achieving both security and effective communications flow.



Simplified network diagram showing the use of firewalls to contribute to Defense in Depth by acting as conduits between the zones of a well segmented network. (Click here for larger image, from the Belden Blog)

Why Industrial Firewalls are Important

Firewalls are important components in today's security strategies. Different types of firewalls are used in various locations within the network to provide different types of protection as part of both the Defense in Depth and Zones and Conduits best practices.

Written by Oliver Kleinberg of the Belden Blog, June 1st 2016. Find it here http://belden.com/blog/industrialsecurity/3-Ways-to-Use-Industrial-Firewalls-for-Defense-in-Depth.cfm