Session 14:

Functional Security in a Process Environment

Kurt Forster
Industrial IT Solutions Specialist, Autopro Automation Consultants

Abstract

In an ideal industrial production security scenario, the Process Control Network (PCN), Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) would not need to communicate with external devices, networks or the internet. Air-gaps could be created which would provide excellent security. With air-gaps between the networks costs would be mitigated for connectivity and security solutions. However, in the real world patch management and monitoring of the networks as well as data sharing with external systems is fast becoming a business necessity. This paper will provide some generic guidelines not just for securing the connectivity between the PCN, DCS and SIS networks to external sources but for a full functional secure environment for all assets.

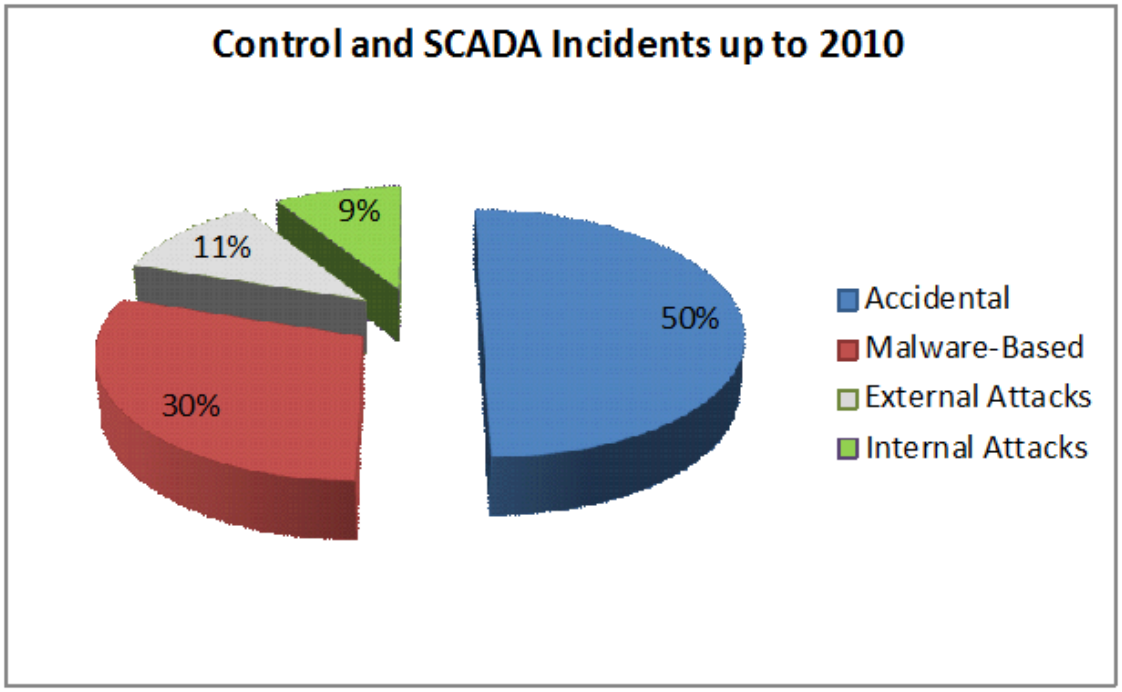
Introduction

The DCS, PCN/Scada, and SIS networks in todays process environment can no longer be standalone components of an industrial solution for companies due to access and management requirements. These networks are only a fraction of the network systems you have in an industrial environment. Other Industrial networks like DVM (Digital Video Monitoring), Wireless transmitters/Backbone (ISA100.11a, WirelessHART, Zigbee etc.), Point of entry, VOIP, SAN, Virtual Infrastructure and even Cloud can also found in an industrial infrastructure today. Each of these environments all require updates and maintenance to keep them healthy and secure.

Industrial Cyber Security (ICS) is part of the larger Functional Security group of functions in the Industrial IT Solutions team. This team's role is to protect, maintain and develop new methods, standards and procedures to protect industrial infrastructure.

Combining the use of ISA95, ISA99 and the new and upcoming ISA106 standards with other specialized standards for parts of the process environment like ISA84/IEC 61511 for SIS (Process) systems we are able to secure the process control environment.

The Repository for Industrial Security Incidents (RISI) is the largest database of security incidents in control and SCADA systems in the world. An analysis of the data up to 2010 found that the type of incidents affecting control systems breaks down as follows:



RISI Incidents up to 2010

Industrial Environments

An industrial environment is where the manifold of its activities are connected with production and services to produce goods which are then sold via a financial business environment.

The modern industrial environment is no longer a separate standalone environment which is catered for by small teams of people that required minimal knowledge of the infrastructure to keep it running. It is also not entirely true to say that large vendors can dictated how it should be run in its entirety. Large vendors do not have the knowledge or capability to develop a complete vendor neutral end to end solution that is flexible to what their customer requires.

Every part of the modern industrial environment that has an interface that transmits and receives data is susceptible to be attacked and this is why we need to protect it. Some of the larger vendors have been able to protect and emphasis that their process control environment like Honeywells FTE community, EMERSON's Delta V Environment can be secured if you follow their rules and guidelines. These Process Control communities normally reside from Level 1 and level 2 of the ISA95 architecture, but we still have Levels -0, 0, 3 and 3.5 to protect. Most vendors have done a great job to protect their process control community networks with rules and best practices but his is not enough to protect the whole of the network environment.

Process environment components

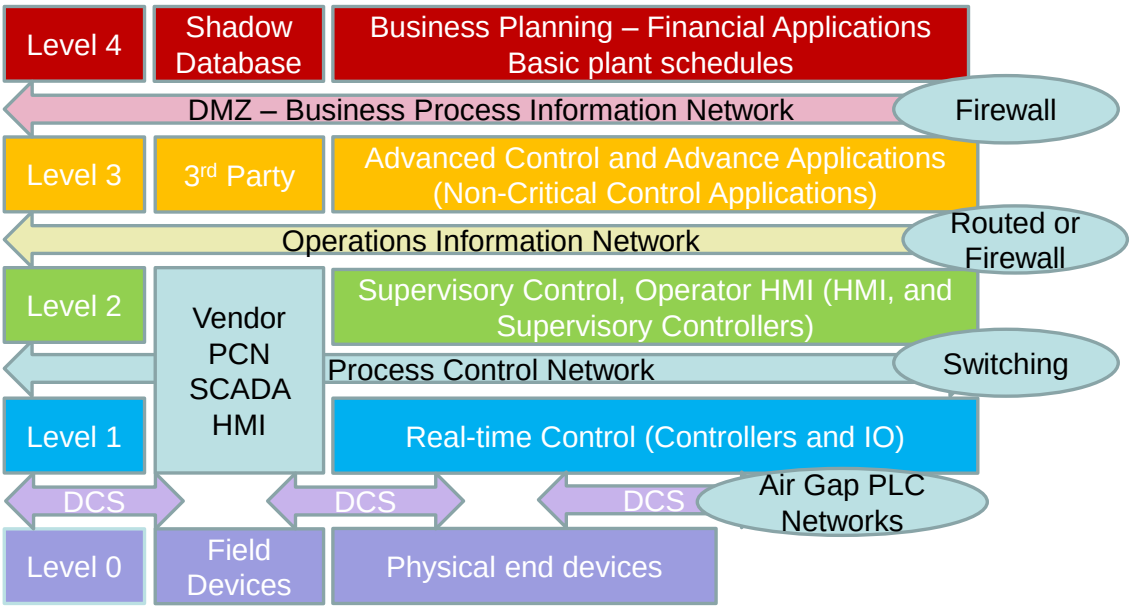
The operating system which is in most cases windows workgroup or widows server domain, networking hardware and the PCN/SCADA, DCS, SIS networks

are to name but a few. All of the above are components of a process environment.

The PCN/SCADA, DCS, SIS networks can run on a mixture of serial, TCP/IP or wireless networks. Each device that runs on a TCP/IP or wireless network requires to be updated at some point. These updates are mainly driven by policies, application compliance or security vulnerabilities.

Working with the ISA95 perdu levels the

- Level 0 DCS is the backside of the controllers and IO's that can be hardwired, serial and/or standalone TCP/IP control networks, would reside at level 0 communicating to end devices.
- Level 1 Realtime Control (Controllers and IO) which are TCP/IP controllers, PLC,s and any other control network devices
- Level 2 Supervisory Control, Operator HMI (HMI, and Supervisory Controllers) the PCN/Scada workgroup/domain operating systems and applications are at this level
- Level 3. Advanced Control and Advance Applications (Non-Critical Control Applications) Workgroup and the forest root domain with shadow databases would reside at this level. This level is also where other 3rd party networks would join to the PCN
- Level 4 The Business LAN or Enterprise network is the working environment for every day finical business. The data that comes from the PCN is used here to sell the goods produced. No direct connection between the industrial networks and business LANs should be performed.



ISA95 Perdue Levels

The way to look at the process infrastructure could be the following:

- Industrial Site = A refinery or site that may contain several Process Control Networks.
- Process Control Network = ISA95 L0 - 3.5 is a single process control network may contain a single process community or several

communities depending on the amount of process required to produce the product.

- Process Control Community = ISA95 L1 & 2 may be a single process or a single process in a multi process PCN. This community is normally a group of nodes that run on a fault tolerant network infrastructure and is normally built on a single broadcast domain. Communication between PCC's is normally done via a router or Firewall placed at level 3

Connecting the networks together

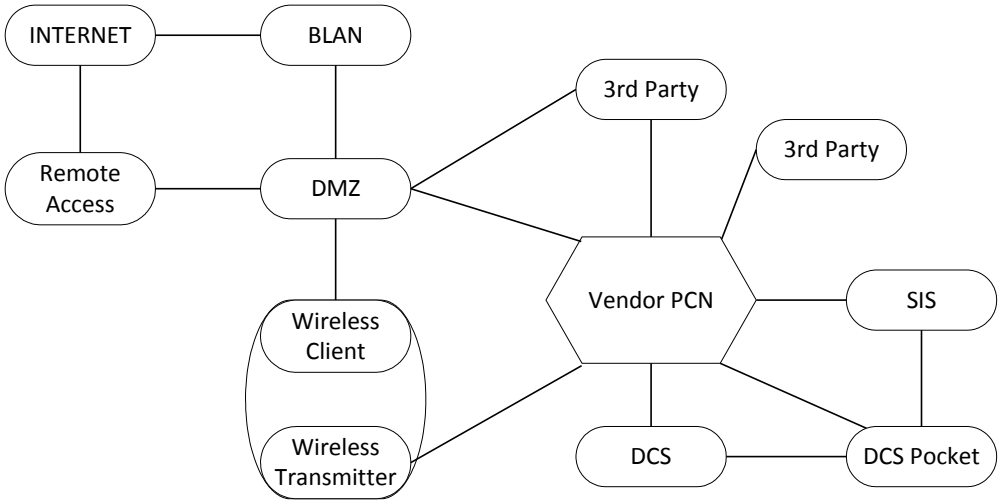
Connecting the different network segments together is where the biggest amount of controversy comes today when introducing multiple vendor systems together. The basic rule of thumb when designing Greenfield sites or upgrading brownfield sites is this:

Which vendor controls the main process? If it's Honeywell, EMERSON, Yokogawa, ABB or one of the many other large vendors then it is advisable to work with their best practices. However this is mainly ISA95 L1 and L2 only. As a company you need to have a defining set of policies and procedures on how and where these devices will connect.

Working with the ISA-95 standard is arguably one of the most important for manufacturing companies; ISA-95 Control to Enterprise Integration standard is a multi-part International standard. It defines the boundary conditions between a manufacturing and a business system, the touch points between them and which data elements should be transferred. Part 3 of the standard provides a model for a manufacturing organization and defines the interactions between information systems inside the organization.

Using the ANSI/ISA-99 / IEC 62443 introduces the concepts of 'zones' and 'conduits' as a way to segment and isolate the various sub-systems in a control system. A zone is defined as a grouping of logical or physical assets that share common security requirements based on factors including criticality and consequence. Any communications between zones must be via a defined conduit. Conduits control access to zones, resist DoS attacks or the transfer of malware, shield other network systems and protect network traffic integrity and confidentiality. 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.

If you use the ISA95 Perdue model then your primary vendor network resides at Level 1, 2 and possibly level 3. All other networks are classed as 3rd party networks and should connect at level 3.



Identification of zones and conduits

NOTE: Definition of a 3rd party vendor network is a self sustained environment that may consists of at least 1 or multiple switch(s) with nodes or devices that no requirement for communication outside of that environment for standard working conditions.

Individual 3rd party nodes that are not dual homed with other process networks may connect to just the primary vendors Level 2 network if they comply with policies and procedures for that network segment. It is important to understand that depending on the vendor, the node may or may not be accepted on the switched process community network or comply with workgroup/domain policies.

Data transfer and access around the network

Process control networks are mainly built in a modular format. Infrastructures normally have a core infrastructure that is from 1 of the large vendors and other vendors connecting in to delver a specific service to the infrastructure. These 3rd party segments normally transfer data back to the core to be processed then displayed to operators or sent other areas of the infrastructure.

The PCN also has the need for remote access, monitoring, patch management and other non process related actions. All this process and non process related data requires to be transferred around infrastructure without delay in the shortest secured route possible. This requires a sound understanding of

- Vendors process control networking knowledge
- Enterprise support applications.
- ANSI/ISA/IEC Standards

Where the ISA95 Perdue levels are week is data transfer at the level 0. Not all data is transferred around the PCN network infrastructure but is transferred via pockets of DCS control networks at level 0. These pockets may include standalone TCP/IP devices. These devices also require to be updated which now causes a dilemma. These pockets now require a duel connected network. Process data going out to a L1 controller or PLC to control the process, and the

TCP/IP devices being updated from level 3, this is not supported in the ISA95 standards. There will always be exceptions in a network but a risk analysis needs to be made at this point.

	Process control	Supervisory Control	Advanced Control	DMZ	BIN/BLAN
ISA95 Level	1	2	3	3.5	4.
1	FF	LF	NC	NC	NC
2	LF	FF	LF	VL	NC
3	NC	LF	FF	VL	NC
3.5	NC	VL	VL	LF	VL
4	NC	NC	NC	VL	FF

Key	
FF	Free Flow of information
LF	Limited Flow of information
VL	Very Limited Flow of information
NC	No Communication

Data flow and permitted access

Who architects the secure network?

To combine a DCS and PCN network design into a secure and workable design is mandatory for correct conduits and zoning. This task may be hard to accomplish as DCS engineers and Industrial IT solution architects design systems differently due to knowledge gaps between both of these roles. DCS engineers are trained to work and design DCS systems but the average DCS engineer do no not hold the Industrial IT skills required to design IIT networks. Modern Industrial IT networks are relatively new and would not have been on the training syllable during their schooling. The average Industrial IT specialists do not have the in-depth knowledge of DCS systems but know more about PCN/SCADA, and Enterprise applications and security hardware systems.

Problems arise with the decision, at what stage are the two disciplines introduced to each other?

Securing the process environment

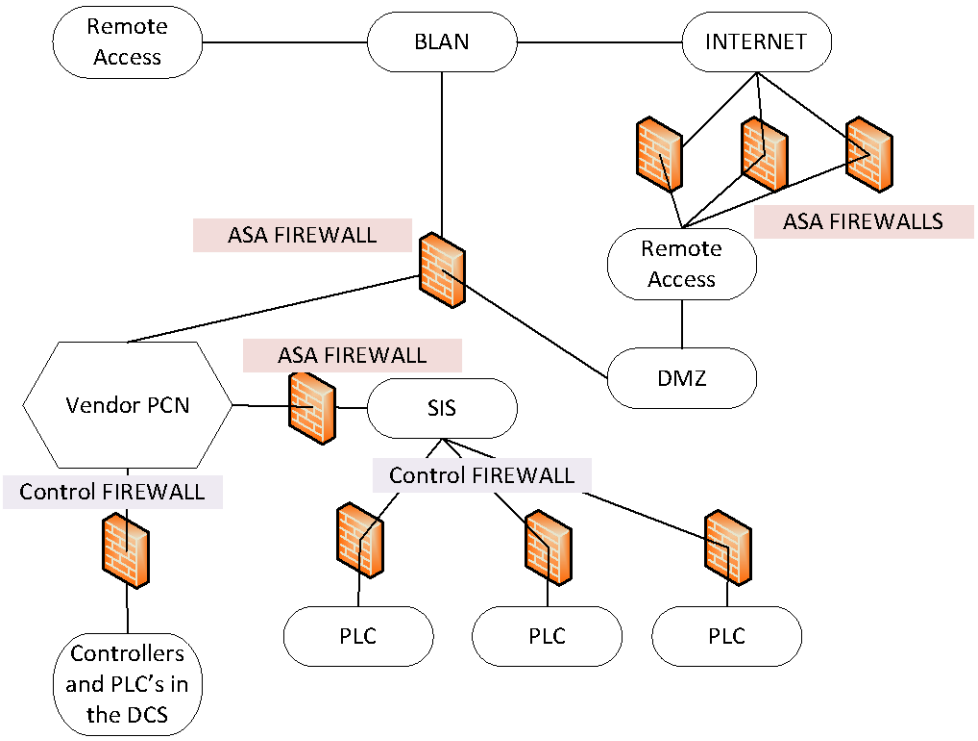
Securing the process environment from the inside is about working with zones and conduits. By identifying the zones in the network infrastructure it is possible to keep data transfer within these zones or transfer limited data between zones via the conduits.

In the industrial network infrastructure the zones we would be looking at would be

- DMZ
- Individual PCN's
- The DCS Pockets
- SIS networks
- Other 3rd party networks
- Wireless
- PLC's and Controllers

Once the zones have been identified then the protection can be put into place. Fully managed Firewalls like the cisco ASA series can be used for boundary or perimeter protection.

Tofino control firewalls are ideal devices that can be used to protect PLC's, Controllers, and any mission critical device that connects onto the Process infrastructure.



Securing the Environment

Conduits would be used within a zone or to connect zones together. These conduits would be methods like Access control lists, or VLANs. These methods are not security boundary's and should not be used as a security boundary. Conduits in this environment would be VLANS and ACL's. However; VLAN truncking and ACL's take up lots of resources in the hardware devices.

Conduits are not to be used inside the Vendors PCN environment e.g. ISA95 L1 and L2 as strict rules dictate from most vendors that multiple VLANS, and VLAN trunking is not to be used.

White or Black listing is a method that could be used but care should be taken when using this type of security. White listing is the most common used protection.

IPSec or 802.1x are very good security protocols used in enterprise networking where modern applications are developed to work with these securities. In the process control world these protocols are still not built into the vendors applications. There are vendors who are developing systems around these but be aware the other 3rd party vendors may not be able to work in the same environment.

Remote access should never come into the PCN directly. These services should terminate in the L3.5 DMZ and proceed downwards into the PCN from there. This may result in multiple remote desktop sessions.

The DMZ is a security buffer zone that normally separates L3 and L4 also known as L3.5. This is where access and data transference should always be a one way direction and not bi directional. No services should ever transfer from L4 to L3 and beyond without first stopping at L3.5

Cyber Security

Cyber security is not new and it's a poor choice of words as the wording of Cyber security makes people dream up images of spotty university kids hacking into your system to change websites and steal data. Cyber security is more about how is your system maintained and secured against all aspects of security.

Access to your grounds, buildings, rooms, cabinets and what access you give to your personnel is all included into cyber security. Other aspects are Antivirus, transferal of data, access by system engineers and patching of PCN, SIS and DCS device and applications. By securing all of this in a process environment and knowing how to do it with the process vendors rules is the largest part of cyber security.

SIS systems and Cyber security

SIS networks are the last line of defence against major disasters in most cases. So this means that it should have the least amount of access to the outside world. However in todays modern environments updates and remote access is required.

SIS network security is all about zones and who or what may enter these zones. By using Microsoft Active Directory group policies in a domain infrastructure this will limit the use and actions of local and remote accounts on a PC in the SIS network. Network Firewalls and Control Firewalls will protect against Dos attacks and harmful malware and virus outbreaks on the outside of the network.

Adhering and policing Policies & Procedures is the most effective manor of protecting against 89% of all the threats. Protecting against the last 11% is having a proactive Industrial IT team who keeps up to date with the latest

threats and testing the solutions in labs before they are rolled out into the process control environment. This will almost take up 99% of their man hours.

In Summary

It is not just the protection of the SIS network which is going to protect against attacks to the system. It is the development of sound Industrial environment architecture. This includes identifying the industrial IT staff, Policies and procedures, what is not included in the vendor's installations and filling the gaps to make it secure, zoning the infrastructure, training and evaluation of staff and infrastructure as technologies evolve.

Making one compartment on the titanic water tight would not have saved the ship from sinking.

References

Industrial defender white paper[Cyber security best practices]

Honeywell White paper Cyber security Best practices

Emerson Delta V Best practices User Guide

Yokogawa Cyber security forum and technical conference

ISA95, ISA99, ISA88 ISA website

The Repository for Industrial Security Incidents

Industrial Ethernet Book [http://www.iebmedia.com]