Tofino Security

White Paper

Version 1.2
Published May 2014

Using ISA/IEC 62443 Standards to Improve Control System Security

Contents

Author

Eric Byres, P. Eng., ISA Fellow
Chief Technology Officer
Tofino Security, a Belden Brand
Belden Inc.

eric.byres@Belden.com
www.tofinosecurity.com
www.tofinosecurity.com/blog

1. Executive Summary

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.

How can you help your company or clients deal with the conflicting requirements of more integration and more isolation? This white paper explains how the "zone and conduit" model included in the ISA/IEC 62443 (formerly known as ANSI/ISA-99) security standards provides a framework for helping deal with network security threats that arise from both the "push for productivity" and the fear of the next "Son-of-Stuxnet" worm.

2. What's New in this Version

In 2010, the standards were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards. This revision reflects those changes.

3. Why the "Push for Productivity" has degraded Control Network Security

As corporate networks have converged with Industrial Control System (ICS) networks, there have been many integration projects where proprietary networks were replaced with commercial-off-the-shelf equipment using Ethernet-TCP/IP technology.

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 shut-downs due to cyber security issues in the control networks.

The Repository for Industrial Security Incidents (RISI[1]) is the world's largest database of security incidents in control and SCADA systems. An analysis of the data from 1982 to 2010 found that the type of incidents affecting control systems breaks down as follows:

- 50% of incidents were accidental in nature
- 30% of incidents were due to malware
- 11% of incidents were due to external attackers
- 9% of incidents were due to internal attackers

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

i. Proliferation of "Soft" Targets

Supervisory Control and Data Acquisition (SCADA) and ICS devices such as PLCs, DCS controllers, IEDs, and RTUs were designed with a focus on reliability and real-time I/O, not robust and secure networking. Many ICS 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 even susceptible to outdated malware.

[1]www.securityincidents.org

ii. Multiple Points of Entry

Even without a direct connection to the Internet, modern control systems are accessed by numerous external sources. All of them a potential source of infection or attack. These include:

- remote maintenance and diagnostics connections
- historian and Manufacturing Execution Systems (MES) servers shared with business users
- remote access modems
- serial connections
- wireless systems
- mobile laptops
- USB devices
- data files (such as PDF documents or PLC project files)

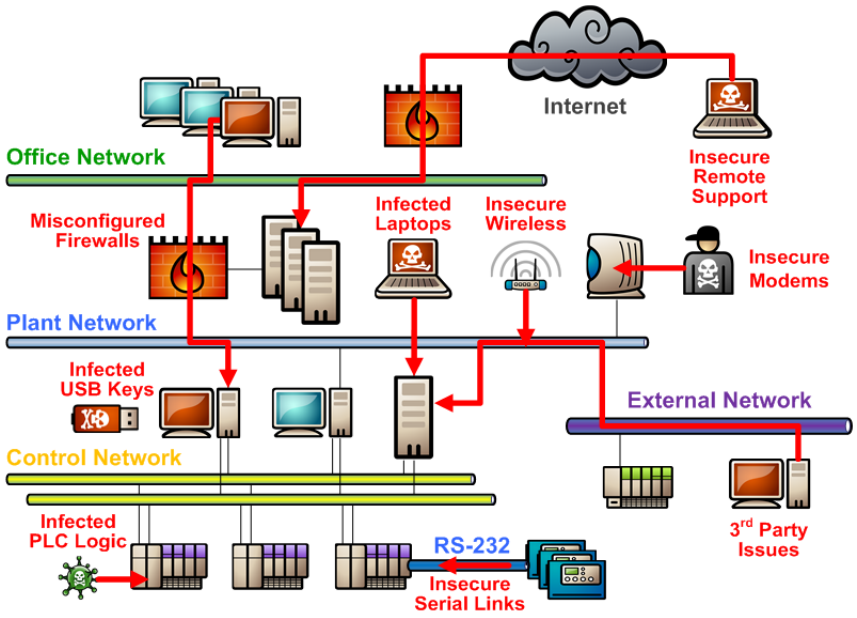

Figure 1: Possible Pathways into the Control System

These pathways are underestimated and poorly documented by the owners and operators of industrial systems. In testimony by Mr. Sean McGurk, the Director of National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security noted:

> *"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."*[2]

As the Stuxnet worm showed us in 2010, these pathways can be readily exploited by malware and other disruptive elements. Stuxnet used at least eight different propagation mechanisms, including USB drives, PLC project files and print servers to work its way into the victim's control system.

[2] The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing. 58:30 -- 59:00

iii. Poor Internal 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.

4. The ISA/IEC 62443 Zone and Conduit Security Model

Given the above concerns, what can the control or SCADA engineer do to secure his or her system? With the competitive pressure that most companies face to improve productivity and access to the data in their plants, it is unlikely that engineers will be able to significantly reduce the number of internal and external pathways into their facilities. Furthermore, the use of modern IT technologies now requires a steady stream of electronic data onto the plant floor as well. These often take the form of upgrades, patches, process recipes and remote support connections, all of which pose a security risk.

There is also limited opportunity for plant engineers to address the proliferation of soft targets in the short term. Aggressive patching strategies do help reduce the risk of exposed operating system vulnerabilities, but most plant operators are dependent on their ICS/SCADA equipment vendors to secure the actual controllers and ICS software products. Unfortunately, this has met with limited success. As of December 2011, the US ICS-CERT had published 137 advisories on control system products[3] with known security vulnerabilities. Less than 50% of these had patches available at the close of the year.

The good news is that engineers can address the third cause by implementing good network architectures in their control systems. This white paper explains how to do this using the strategies outlined in the *ISA/IEC 62443 Standards: Security for Industrial Automation and Control Systems*.

ISA/IEC 62443 is a complete security life-cycle program for industrial automation and control systems. It consists of 11 standards and technical reports on the subject, a number of which have been publicly released as American National Standards Institute (ANSI) documents. Work products from the ISA99 committee are also submitted to International Electrotechnical Commission (IEC) as standards and specifications in the IEC 62443 series.

ISA/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 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.

[3] https://www.us-cert.gov/control_systems/ics-cert/archive.html

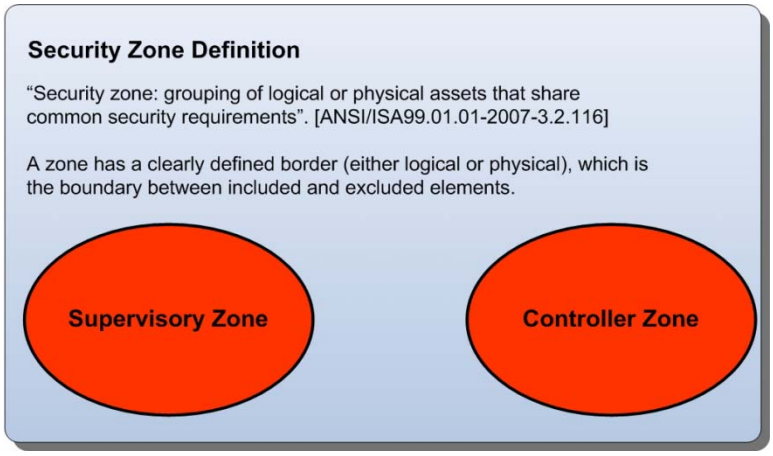

Figure 2: Security Zone Definition

Any communications between zones must be via a defined conduit. Conduits control access to zones, resist Denial of Service (DoS) 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.

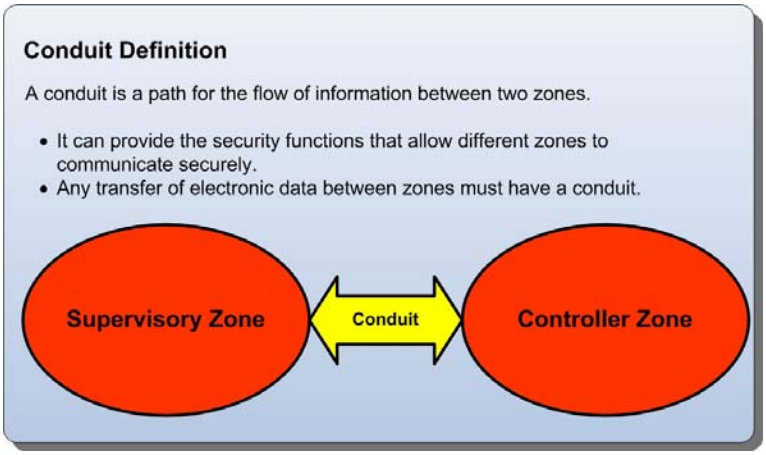

Figure 3: Conduit Definition

It is important to understand that ISA/IEC 62443 standards do not specify exactly how a company should define its zones or conduits. Instead, the standard provides requirements based on a company's assessment of its risk from cyber attack. Since risk is a function of not only the possibility of a cyber incident, but also the consequences of such an incident, the zones and conduits and the protection needed for each will vary for each facility. Figure 4 lists some of the sub-sections in the document ANSI/ISA-62443-2-1 (99.02.01)-2009 that address network segmentation using zones and conduits.

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 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 4: Key Zone and Conduit Requirements from ISA/IEC 62443-2-1

5. Defining the Security Zones

Zone and conduit design starts with the facility or operation being analyzed to identify groups of devices that have common functionality and common security requirements. These groups are the zones 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 Manufacturing Execution Systems (MES), Supervisory Systems (i.e. operator HMIs), primary control systems (e.g. DCS Controllers, RTUs and PLCs) and safety systems. Often 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. Vendor design documents can also be helpful.

Each zone can then be defined by a number of zone characteristics (attributes). The following are some recommended characteristics:

1) Zone Description
    i) Zone Name
    ii) Definition
    iii) Zone Function
2) Zone Boundaries
3) Typical Assets (or if possible, Asset Inventory)
4) Inheritance from Other Zones
5) Zone Risk Assessment
    i) Security Capabilities of Zone Assets
    ii) Threats and Vulnerabilities
    iii) Consequences of a Security Breach
    iv) Business Criticality
6) Security Objectives
7) Security Strategy
8) Acceptable Use Policy
9) Inter-zone connections (i.e. Access Requirements)
10) Change Management Process

Examples are provided later in this white paper to help clarify these attributes.

Notice that each zone is defined with not only its boundaries, assets and risk analysis, but also its security capabilities. In other words, the security capabilities of a zone full of Windows 2008 servers is very different than of a zone of Windows NT servers or a zone with PLCs. This security capability, along with the security risk faced by the zone, drives the security function requirements for conduits that connect the zone to other zones. The soon to be published *ISA-62443.03.03 (99.03.03): Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels* helps the user define these security capabilities and requirements.

Zones can also be defined according to a control asset's inherent security capabilities. For example, older PLCs that have very weak password controls (i.e. authentication) could be grouped into a zone that provides them with additional defenses.

6. Defining the Security Conduits

The next step is to discover the pathways in the system through which data is passed between these zones; these are the network "conduits". Each conduit should be defined in terms of the zones it connects, the technologies it utilizes, the protocols it transports and any security features it needs to offer its connected zones.

Typically, determining the information transfer requirements between zones over the network is straight forward. Tools like traffic flow analyzers or even simple protocol analyzers can show which systems are exchanging data and the services they are using.

It is also wise to look beyond the network, to determine the hidden traffic flows. For example, are files ever moved via USB drive between the lab and the primary control systems? Do people remotely connect to the RTUs using a dialup modem? These flows are easy to miss, but can result in serious security issues if not managed carefully.

Data flow diagrams are an excellent tool to summarize the conduits and the traffic flows they contain. Each zone can be represented by a node and each flow can be represented by a vector.

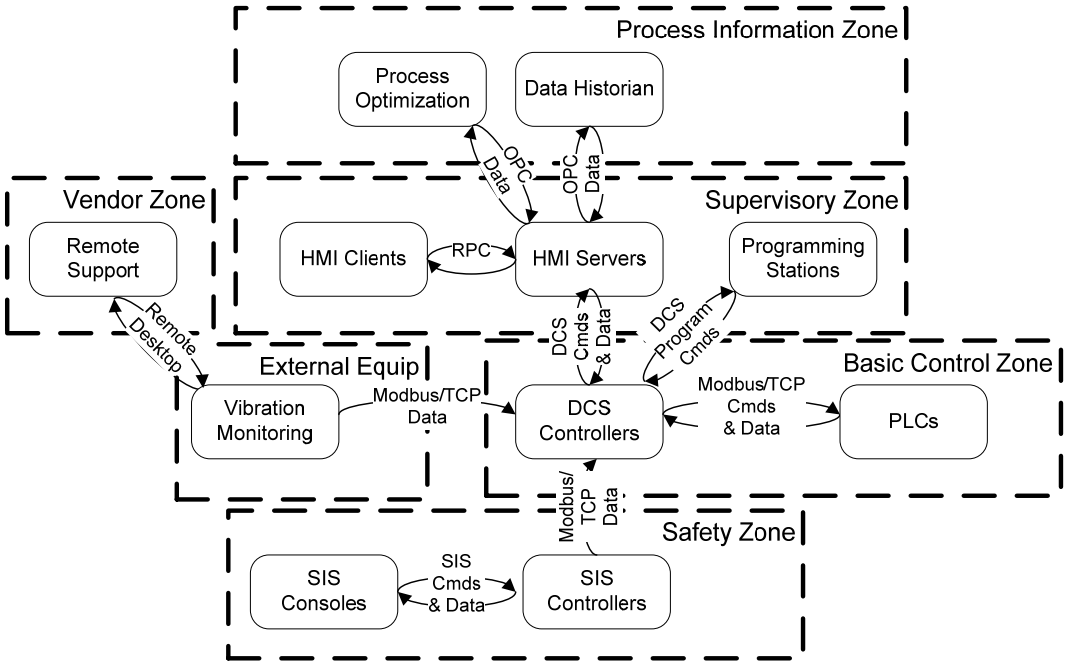

Figure 5: Example Data Flow Diagram

7. Securing the Conduits

Once the conduits and their security requirements are defined, the final phase is to implement the appropriate security technologies. There are two popular options for this stage:

- **Firewalls:** These devices control and monitor traffic to and from a zone. They compare the traffic passing through to a predefined security policy, discarding messages that do not meet the policy's requirements. Typically they will be configured to pass only the minimum traffic that is required for correct system operation, blocking all other unnecessary traffic. They can also filter out high risk traffic, such as programming commands or malformed messages that might be used by hackers to exploit a security hole in a product. Industrial firewalls are designed to be very engineer-friendly and are capable of detailed inspection of SCADA protocols such as DNP-3, Ethernet/IP and Modbus/TCP.
- **VPNs (Virtual Private Networks):** These are networks that are layered onto a more general network using encryption technology to ensure "private" transmission of data and commands. VPN sessions tunnel across a transport network in an encapsulated format, making them "invisible" to devices that don't have the have access to the VPN members' secret "keys" or "certificates".

The whole zone and conduit approach implements a strategy of "defence in depth" – multiple layers of defence distributed throughout the control network – which has been proven in the IT community to be a strategy that works well.

8. A Real-World Oil Refinery Example

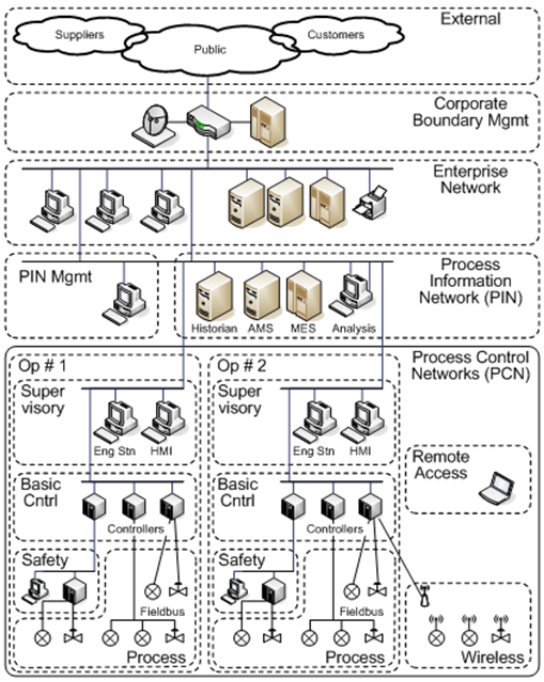

Figure 6: Core Refinery Operations

An example from the oil industry site shows how the ISA/IEC 62443 zones and conduits design techniques were used by a large refinery to create a security architecture and protect its operations.

This company owns a large industrial refinery process facility. Inside the facility there are multiple operations such as Distillation, Hydrotreating, Catalytic Reformers and Utilities.

The company also follows the concepts of ANSI/ISA-95.00.01-2000 and ANSI/ISA-62443-1-1 (99.01.01)-2007, dividing its process operations into Levels 0 through 4. Because of the nature of its operations, many (but not all) of its operations require safety integrated systems (SIS). It also has several control areas that are beginning to use wireless technology. Finally, suppliers (such as control system vendors) and downstream customers (for custody transfer) must interface with its control systems.

A high-level network diagram of the refinery is shown in Figure 6**.** For simplicity, only two refinery operations areas (Op #1 and Op #2) are shown in this diagram, 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 both the Enterprise and control networks. In addition, wireless sensors are being

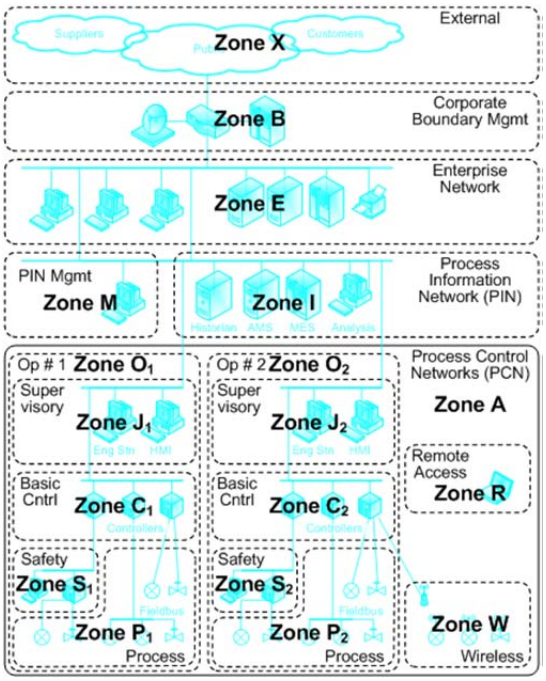

Figure 7: Refinery Zone Diagram

deployed throughout Op #2, and a Remote Access gateway is provided to permit remote maintenance on plant systems by the control system engineers.

The company then began to divide its systems into zones based on operational function, process level, security requirements and security capabilities as shown in Figure 7. All control functions belong to an overall Process Control Zone (A) and within that there are Operational Zones (O1, O2... On) for each major operational unit. This way security requirements for a particular operation could be adjusted for its potential for risk (e.g. security for a low consequence unit like waste water could be relaxed, as compared to a hydrocracker unit). Finally, the Operational Zones could be divided into subzones based on the ISA-95 level they operate at.

Once the zones were defined, they needed to be described with the zone attributes as noted earlier. Figure 8 shows an example zone definition for one of the safety area zones. It is worth mentioning that the zone definition procedure is an iterative process. It is likely that zone boundaries need to be redefined and new zones created as the description stage is conducted.

ZONE S_1

Zone Name: Unit 1 Hydrocracker Safety System

Definition of this Zone: This zone includes all safety integrity systems for the Unit 1 Hydrocracker.

Controlling Agency: Process Automation Department, SIS Team.

Zone Function: The systems in this zone provide safety functions to the Unit 1 Hydrocracker.

Zone Boundaries: The Safety Integrated System as defined by the Unit 1 Hydrocracker HAZOP.

Typical Assets: The Safety Integrated System controller, engineering station and communications hardware

Inheritance: This zone inherits attributes from Zone C_1 (Unit 1 Hydrocracker Basic Control System)

Zone Risk Assessment: This is a low to moderately secure zone with extreme consequences if breached.

a) **Security Capabilities of Zone Assets:** All assets are assumed to be incapable of withstanding low level attacks (i.e. those launched by unsophisticated attackers or malware) on their availability or confidentiality. This is a result of the protocols in use and system design. Assets are assumed to be capable of withstanding medium level attacks (i.e. those launched by moderately sophisticated attackers or malware) on their integrity.

b) **Threats and Vulnerabilities**: The vulnerabilities of this zone are assumed to be typical of legacy industrial control devices using MODBUS for communications. The principal threats are:
   a. Network-based Denial of Service to SIS communications.
   b. Internal or External unauthorized access to the SIS engineering station.
   c. Spoofing of MODBUS/TCP control commands.
   d. Spoofing of MODBUS/TCP responses to the process system.
   e. Reprogramming of safety functions.

c) **Consequences of a Security Breach**:
   a. Loss of production >6 hrs from false trip of emergency shutdown system.
   b. Loss of production <6 hrs due to loss of visibility to safety system.
   c. Disabling/manipulation of emergency shutdown resulting in fatality or major community incident.

d) **Business Criticality:** Extreme

Security Objective: To protect the integrity and availability of the Unit 1 Hydrocracker Safety System.

Acceptable Use Policy: I/O and Fieldbus communications is allowed to Zone P_1 (Unit 1 Hydrocracker Process). Read access to published data is allowed to approved systems in the Zone C_1 (Unit 1 Hydrocracker Basic Control System). All Write access to this zone is forbidden. All system management and programming functions shall be internal to this zone.

Inter-zone Connections: Conduits to this zone may be established from Zone C_1 (Unit 1 Hydrocracker Basic Control System) and from Zone P_1 (Unit 1 Hydrocracker Process).

Security Strategy: All connections to this zone must be controlled using type S conduits. Access to these systems must be approved by the Controlling Agency.

Change Management Process: All changes to this zone or any of its connecting conduits must follow the approved change management process of its corresponding Controlling Agency (see above). This includes, but is not limited to, the installation or replacement of equipment, modification of security policy, and exceptions to security policy or existing practices.

Figure 8: Example Zone Definition Document for the Safety Zone

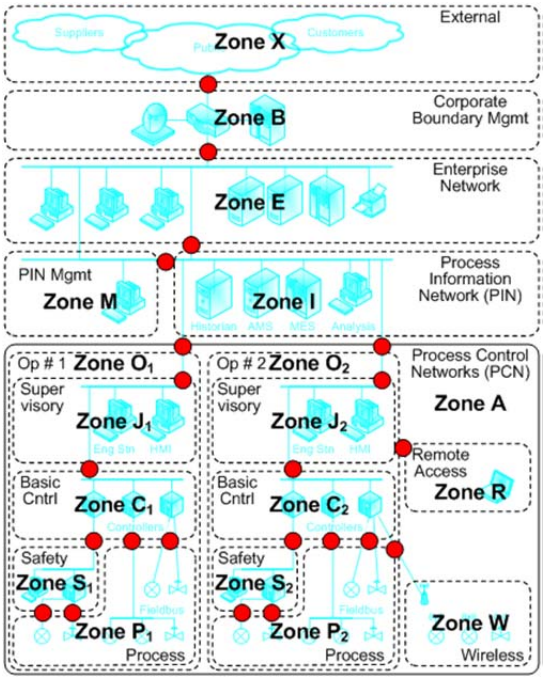

Figure 9: Defined Conduits in Refinery

This facility was no exception. Following the initial analysis, the potential threat sources and consequences of an attack were identified and reviewed with the plant engineers. Through this analysis, it was evident that the safety integrated system (SIS) in each operational unit should be located in its own zone (initially they were part of the basic control zone). To ensure continued safe plant operation, it was vital that the safety system could not be compromised from the plant control network. Later in the process, these were the first zones to be protected with security appliances on the conduits.

With the zones defined, the next stage was the conduit definitions. For all connections between two zones, a "conduit" was defined. This is a record of approved connections and data flows (called channels in ISA/IEC 62443) between zones. Figure 9 shows a simplified diagram of the network conduits. Non-network conduits should also be documented, such as information transfers by USB drives between zones, or the use of dial up modems.

9. Implementing Zones and Conduits with Industrial Security Appliances

The final stage of the zone and conduit security process is to select technologies to secure the conduits and zones. Some industrial security appliances are engineered specifically to support this "defence in depth" strategy in control networks. These are the ideal platform on which to base an ISA/IEC 62443 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 ISA/IEC 62443 zones and conduits deployment, industrial security appliances can be installed in each conduit 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

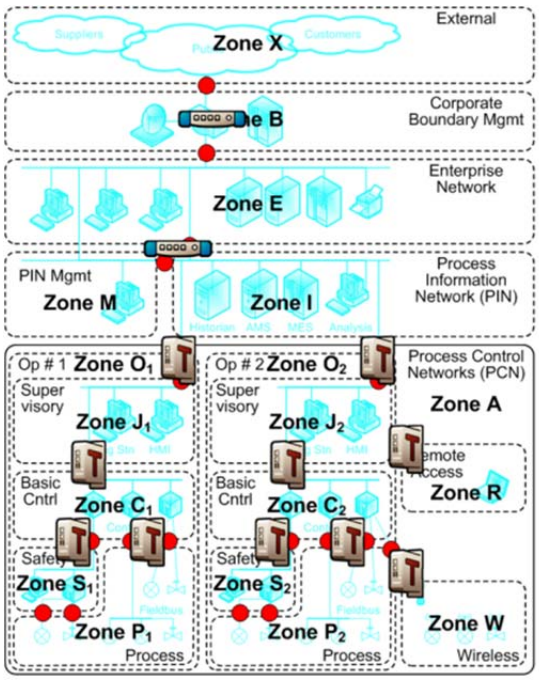

Figure 10: Securing the Conduits and Zones with Firewalls and VPNs

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.

10. Testing and Managing the Security Solution

The next stage in the process is to test the architecture and implementation. This includes not only making sure the deployment blocks attack, but also ensuring that the operation of the industrial process is not negatively affected by the security deployment.

Ideally, the industrial firewall's configuration tools should be designed specifically to match the needs of the control engineer responsible for configuration and testing. Good security tools make it very easy not only to configure firewall rules, but also to test them before they are actually implemented. This is essential for safe deployment of a firewall or VPN in control networks – it is not acceptable to accidently block "good" network traffic that is required for correct plant operation.

One solution is a "Test" mode that transparently bridges all traffic through the firewall, 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 accidently 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. It is then safe to switch the security appliance to "Operational" mode where the firewall rules will be enforced.

The final stage is to manage the system on an ongoing basis. Typical control networks will have multiple conduits distributed over many locations in a plant. Ideally, the multiple industrial security appliances should be managed from a single management console application. We will discuss this in more detail in future white papers.

11. Summary

New network and PC-based technologies introduced into control systems have provided tremendous improvements in plant performance and productivity. In 2010 the Stuxnet worm showed us that sophisticated malware 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 cyber security initiatives that improve control network security and reliability.

The ISA/IEC 62443 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 cyber security threats that arise from both the "push for productivity" and "Son-of-Stuxnet" malware.

12. Resources

White Paper on the penetration of control systems by Stuxnet:
http://www.tofinosecurity.com/how-stuxnet-spreads

ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models: https://www.isa.org/store/products/product-detail/?productId=116720

ANSI/ISA-62443-2-1 (99.02.01)-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program:
https://www.isa.org/store/products/product-detail/?productId=116731