INL/CON-07-12804
PREPRINT

Control Systems Cyber Security: Defense-in-Depth Strategies

2007 ISA Expo

Mark Fabro
Trent Nelson

October 2007

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Control Systems Cyber Security: Defense-in-Depth Strategies

Prepared by
Idaho National Laboratory under contract with U.S. Department of Homeland Security, Control Systems Security Program, Principal Authors Mark Fabro and Trent Nelson

Keywords

Defense in depth, industrial control system, SCADA, PCS, cyber security, mitigation, firewall, IDS, intrusion detection, encryption, DMZ

INTRODUCTION

Information infrastructures across many public and private domains share several common attributes regarding information technology (IT) deployments and data communications. This is particularly true in the control systems domain. A majority of the systems use robust architectures to enhance business and reduce costs by increasing the integration of external, business, and control system networks. However, multi-network integration strategies often lead to vulnerabilities that greatly reduce the security of an organization and can expose mission-critical control systems to cyber threats.

This document provides guidance and direction for developing "defense-in-depth" strategies for organizations that use control system networks while maintaining a multi-tier information architecture that requires the following:

- Maintenance of various field devices, telemetry collection, and/or industrial-level process systems
- Access to facilities via remote data link or modem
- Public-facing services for customer or corporate operations
- A robust business environment that requires connections among the control system domain, the external Internet, and other peer organizations.

BACKGROUND

The critical infrastructure systems that support major industries, such as manufacturing, transportation, and energy, are highly dependent on information systems for their command and control. While there is still a high dependence on legacy control systems, critical infrastructure/key resource (CI/KR)

systems are migrating to new communication technologies. As a result, the diverse and disparate proprietary mechanics of control systems are being replaced with common communications protocols and open architecture standards, which can have both positive and negative impacts.

The new protocols and communication standards that are providing increased interoperability and control in the control system community are the same technologies that have been exploited and compromised in the Internet and networking domains. Figure 1 illustrates the traditional separation of corporate architectures and control domains. This architecture provided means for data sharing, data acquisition, peer-to-peer data exchange, and other business operations. However, the security of any given system was based on the fact that few, if any, understood the intricate architecture or the operational mechanics of the resources on the controls system local area network (LAN). This "security by obscurity" works well for environments that have no external communication connections and allows an organization to focus primarily on physical security.

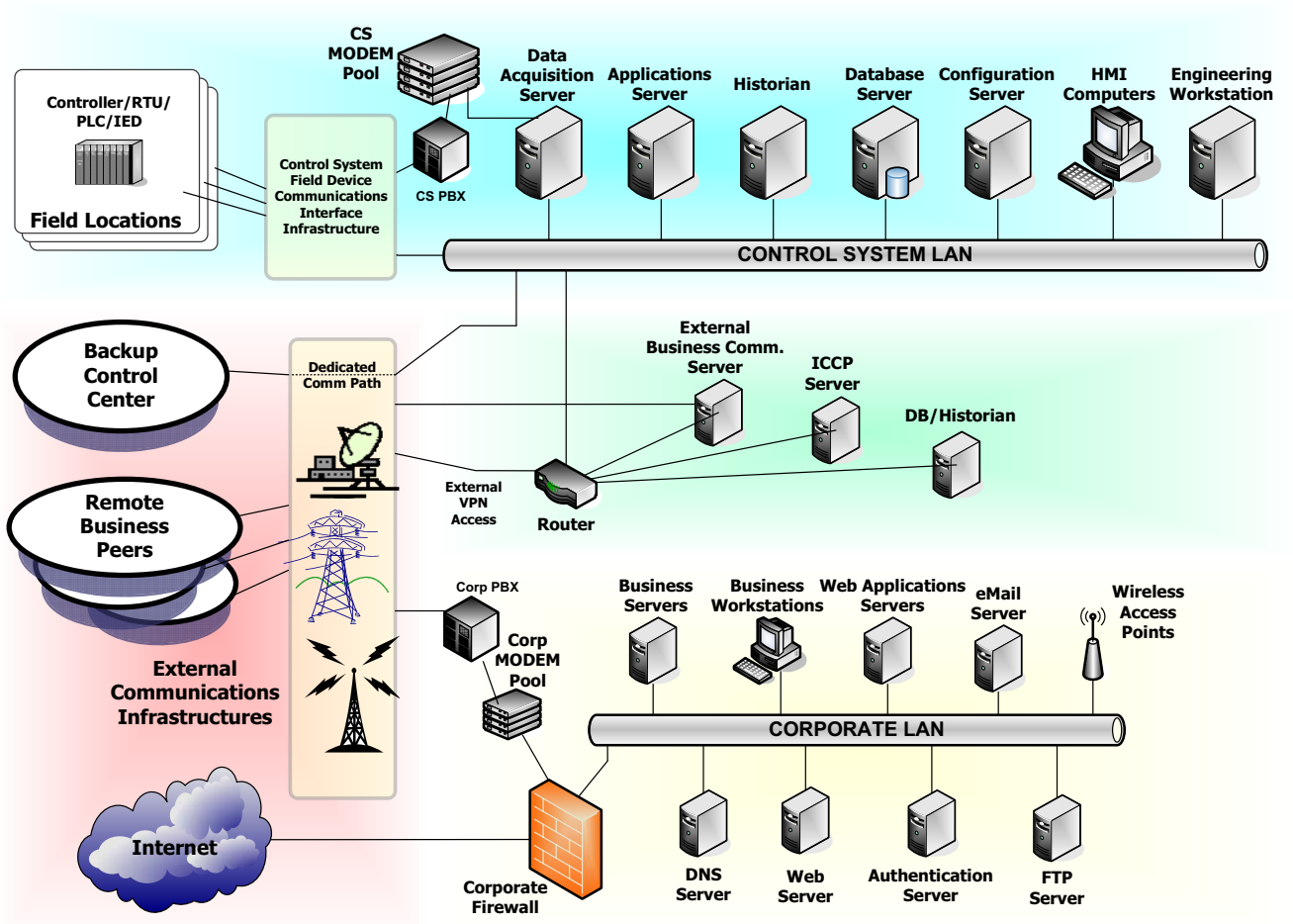

Figure 1. Traditional isolation of corporate and control domains.

OVERVIEW OF CONTEMPORARY CONTROL SYSTEMS ARCHITECTURES

In today's competitive markets, isolated control system networks are being interconnected. In connecting these networks, and introducing IT components into the control system domain, security problems arise due to the following:

- Increasing dependency on automation and control systems
- Insecure connectivity to external networks
- Usage of technologies with known vulnerabilities
- Control system technologies have limited security
- Control system communications protocols are absent of security functionality
- Considerable amount of open source information is available regarding control system configuration and operations.

Control system operational security has historically been defined by industry as the level of reliability of the system to operate. The total isolation from the external (and untrusted) network allowed the organization to reduce the level of communications security; threats to operations resided with physical access to a facility or plant floor. Thus, most data communications in the information infrastructure required limited authorization or security oversight.

Obviously, this arrangement is very different from effective network and IT cyber security systems. Figure 1 shows an integrated architecture, and it is clear that such architectures, if compromised, could provide an attacker with various avenues for accessing critical systems. The very nature of such architectures demands the exchange of data from disparate information sources, a factor that could clearly be taken advantage of by an attacker.[1]

SECURITY CHALLENGES IN CONTROL SYSTEMS

Historically, security issues have been the responsibility of the corporate IT security organization, usually governed by security policies and operating plans that protect vital information assets. Contemporary network-based communications have security issues that must be addressed in the control system domain, because unique vendor-specific protocols and assumed legacy system security are not adequate to protect mission-critical systems.

Examples of threats in open systems architectures that can (and most likely will) migrate to control system domains include hostile mobile code (if applicable to the system), escalations of privileges through code manipulation, network reconnaissance and data gathering, covert-traffic analysis, and unauthorized intrusions into networks, either through or around perimeter defenses. To fully translate

---

[1] This type of architecture, and the back-end control system, is vulnerable to both external attackers and internal attackers. Insider attacks have always been a major threat to IT systems, but architectures like the one shown in Figure 2 exacerbate the issue by providing access to a large, highly connected, and unprotected trusted information infrastructure. The insider has historically been a threat to control systems, but new connectivity creates opportunity for the external attacker as well.

information security and information assurance into the control system realm, one must understand the key differences between traditional IT architectures and control systems technology.

From a mitigation perspective, simply deploying IT security technologies into a control system may not be a viable solution. Although modern control systems use the same underlying protocols that are used in IT and business networks, the very nature of control system functionality may make even proven security technologies inappropriate. Much work has been done regarding some of the more common security elements an organization could leverage and how they are addressed in IT domains, as opposed to architectures that run control systems.[2]

SECURITY PROFILES AND ATTACK METHODOLOGIES

Control networks have evolved from stand-alone islands to interconnected networks that co-exist with corporate IT environments, introducing security threats. For example, mobile code, in the form of viruses, worms, and parasitic code, can manifest itself in network-enabled control system environments just as easily as in non-control system domains. For devices with embedded firmware, such as controllers and relays, hostile mobile code cannot generally have an impact through network propagation. However, should the compiled code these devices download on a regular basis be corrupted with hostile malware, the effects could be very damaging.[3]

Critical cyber security issues that need to be addressed include those related to the following:

- Backdoors and holes in network perimeter
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and “man-in-the-middle” attacks.

Understanding attack vectors is essential to building effective security mitigation strategies, and effective security depends on how well the community of control system operators and vendors understand the ways that architectures can be compromised.[4] For this document, a discussion of various attack vectors may provide some insight into how a defense-in-depth strategy can be effective.

BACKDOOR ATTACKS VIA NETWORK PERIMETER[5]

---

[2] NIST SP 800-82 has a concise section discussing these differences.

[3] Although the occurrence of this type of compromise is currently unlikely, such attack vectors should not be ignored when considering future attack scenarios.

[4] The technical mechanics of attacks are beyond the scope of this paper.

[5] http://www.us-cert.gov/control_systems/pdf/backdoors_holes0805.pdf

As is the case in common networking environments, control system domains are subject to myriad vulnerabilities and holes that can provide an attacker a "backdoor" to gain unauthorized access. Adversaries (threats) often do not require physical access to a domain to gain access to it and will use any and all discovered access functionality. Modern networks, especially those in the control-system arena, often have inherent capabilities that are deployed without sufficient security analysis and can provide access to attackers once they are discovered. These "backdoors" can be accidentally created in various places on the network, but it is the network perimeter that is of greatest concern. These technologies often include firewalls, public-facing services, and wireless access.

ATTACKS USING COMMON PROTOCOLS (OPC/DCOM ATTACKS)[6]

The impact of modern operating systems on control systems has been significant. Over the last several years, more and more organizations have started to use underlying services in these environments, including the Object Link and Embedding (OLE) for Process Control (OPC). The convergence of traditionally isolated control networks with business environments, and the associated protocols, provides a new environment for attackers to exploit. What makes this very interesting, and also a concern, is that the traditional mitigation strategies for common networks are not always effective or practical in control systems architectures. In a simple example, SP2 for Microsoft XP, a platform commonly used in control systems, mitigates the security issues associated with some mobile code attacks by disabling DCOM (Distributed Common Object Model). If this patch is deployed in a production environment where OPC is used for interoperability, OPC over DCOM will not work. There have been several reports of this patch bringing production facilities to a complete stop or creating unexpected and irrational behavior in the control systems.

With the convergence of control systems and modern networking technologies comes some inherited security vulnerabilities. Even though many of these vulnerabilities have solutions and available workarounds, the deployment of these mitigations in control systems architectures is not always feasible.

ATTACKS INTO CONTROL SYSTEMS VIA FIELD DEVICES

Control systems architectures usually have a capability for remote access to terminal end points and telemetry devices. In some cases, the field equipment itself has the capability to be accessed a number of ways, including by telephonic or dedicated means. To provide for the collection of operational and maintenance data, some modern equipment has embedded file servers and web servers to facilitate robust communications.

However, as has been previously discussed, these devices are part of an internal and trusted domain, and, thus, access into these devices can provide an attacker with an unauthorized vector into the control system architecture. Recognizing that field devices, such as Remote Terminal Units (RTUs), are extensions of the control system domain, attackers can add these field devices to their list of viable

---

[6] See US-CERT "Security Implications of OPC, OLE, DCOM, and RPC in Control Systems."

targets to be investigated during reconnaissance and scanning phases of the attack. If the attacker decides to scan back into the control network, which is probable considering the assumed trust between resources, it may be possible to do so by using the communications protocols for the entire control system domain. This is of particular advantage to the attacker, as it is likely that the connections are not monitored for malicious or suspect traffic.[7]

DATABASE AND SQL DATA INJECTION ATTACKS [8]

Database applications have become core application components of control systems and their associated record keeping utilities. Traditional security models attempt to secure systems by isolating core control system components and concentrating security efforts against threats specific to those computers or software components. Database security within control systems follows these models by using generally independent systems that rely on one another for proper functionality. The high level of reliance between the two systems creates an expanded threat surface. The information contained in databases makes them high-value targets for any attacker, and the cascading effect of corrupted database content can impact data acquisition servers, historians, and even the operator HMI console. Moreover, compromise of key trusted assets, such as a database, creates additional resources the attacker can use for both reconnaissance and code execution.

MAN-IN-THE-MIDDLE ATTACKS[9]

Control system environments have traditionally been (or been intended to be) protected from non-authorized persons by air gapping, and communications are trusted because the security is designed to prevent access to the control network. Three of the key security issues that arise from assumed trust are the ability of an attacker to (1) re-route data that is in transit on a network, (2) capture and analyze open critical traffic that is in plaintext format, and (3) reverse engineer any unique protocols to gain command over control communications. By combining all of these, an attacker can assume exceptionally high control over the data flowing in a network and, ultimately, direct both real and "spoofed" traffic to network resources in support of the desired outcome.

Assuming an attacker has gained access onto the controls systems network, perhaps using any of the aforementioned attacks, he will use network reconnaissance to determine resources that are available on that network. Because the attack is on the control domain, this plaintext traffic can be harvested (sniffed) and taken offline for analysis and review. This allows the attacker to review and re-engineer packet and payload content, modify the instruction set to accommodate the goal of the attack, and re-inject the new (and perhaps malicious) packet into the network.

---

[7] Some Intrusion Detection Systems (IDS) can be updated with control systems signatures to help defend control domains. Usually, these systems are signature-based and will trigger upon recognition of malicious traffic. In lieu of a viable signature, IDS can be deployed to trigger upon recognition of non-specific traffic, or traffic that is not expected or unusual. See below for the discussion on IDS.

[8] See US-CERT "Attack Methodology Analysis: SQL Injection Attacks."

[9] http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf

ISOLATING AND PROTECTING ASSETS: DEFENSE-IN-DEPTH STRATEGIES

Modern IT architectures that involve both business and control network components share many common characteristics, regardless of how diversified their applications may be. In general, there are four main zones (see Figure 2) that provide the following:

- External connectivity to the Internet, peer locations, and back-up facilities (Zone 1)
- External connectivity for corporate communications (Zone 2)
- Control systems communications from external services (Zone 3)
- Control systems operations, be they process based or SCADA (Zone 4).

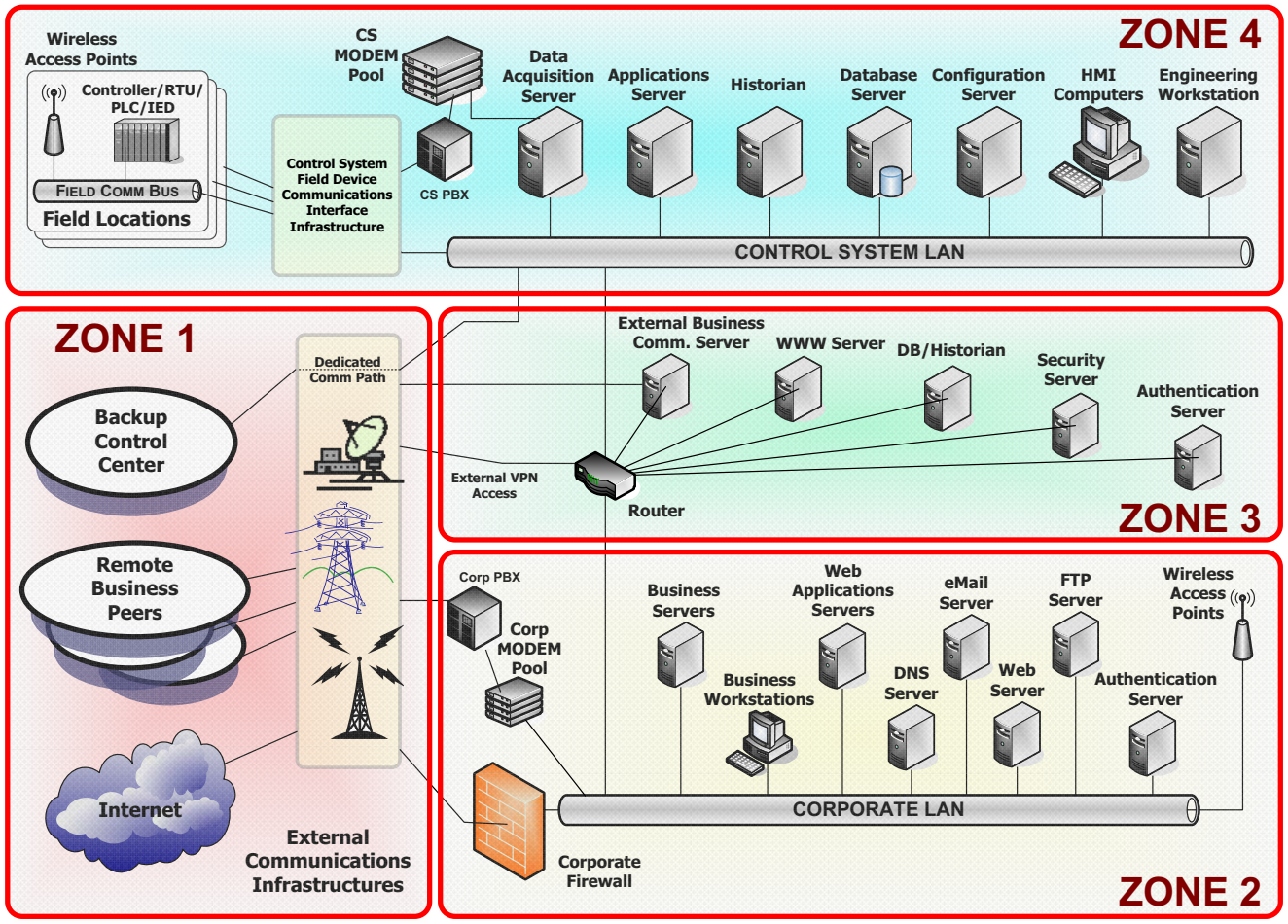

Figure 2. Common architecture zones.

Each of these zones requires a unique security focus. A “peel-the-onion” analysis shows that an attacker trying to affect a critical-infrastructure system would most likely be after the core control

domain.[10] In this paper, and in the suggested supporting documentation provided by DHS through US-CERT, numerous categories of attacks and outcomes have been discussed. In each of the scenarios discussed in these documents, the intrusion begins at some point outside the control zone and the attacker pries deeper and deeper into the architecture. Thus, defensive strategies that secure each of the core zones can create a defensive strategy with depth, offering the administrators more opportunities for information and resources control and introducing cascading countermeasures that will not necessarily impede business functionality.

FIREWALLS

There are many types of firewalls, and some research is required to ascertain what type of firewall is right for a given control architecture. The concept of security zones provides some insight as to how an organization can determine what risk and consequence is associated with a particular zone. This analysis can be used to select the type of firewall and attributes that are best suited for protecting the assets. In general, there are four main types of firewalls: packet filter, circuit level gateways, proxy gateways, and stateful inspection. Considerable work has been done regarding analysis of firewalls for use in the industrial control domain.[11]

PACKET FILTER FIREWALLS

Although usually flexible in assigning rules, the packet filter firewall is well suited for environments where quick connections are required and rules can be developed based on device addresses. It is effective for environments, such as control systems, that need security based on unique applications and protocols.

PROXY GATEWAY FIREWALLS

Proxy gateway firewalls are good for analyzing data inside the application (POST, GET, etc.) and collecting data about user activities (logon, administration, etc.). They are gateways that require users to direct their connection to the firewall. In control systems environments, this type of firewall is well suited to separating the business and control LANs and providing protection to a demilitarized zone (DMZ) and other assets that require application-specific defenses.

STATEFUL INSPECTION FIREWALLS

Stateful inspection firewalls include characteristics of all the other types of firewalls but tend to use algorithms to process data rather than run proxies. These firewalls execute a considerable amount of inspection of packets that are arriving on the interfaces, are capable of keeping track of valid sessions, and may make a good choice for protecting key assets in the control domain.

---

[10] This of course depends on the overall objective of the attacker. In general it is believed that complete control over core services and operational capability of the control system has high value.
[11] www.**niscc**.gov.uk/**niscc**/docs/re-20050223-00157.pdf

CREATING DEMILITARIZED ZONES

Network segmentation has traditionally been accomplished by using multiple routers. Firewalls should be used to create DMZs to protect the control system network. Figure 3 shows a robust architecture with multiple DMZ deployments to accommodate several types of services.

.

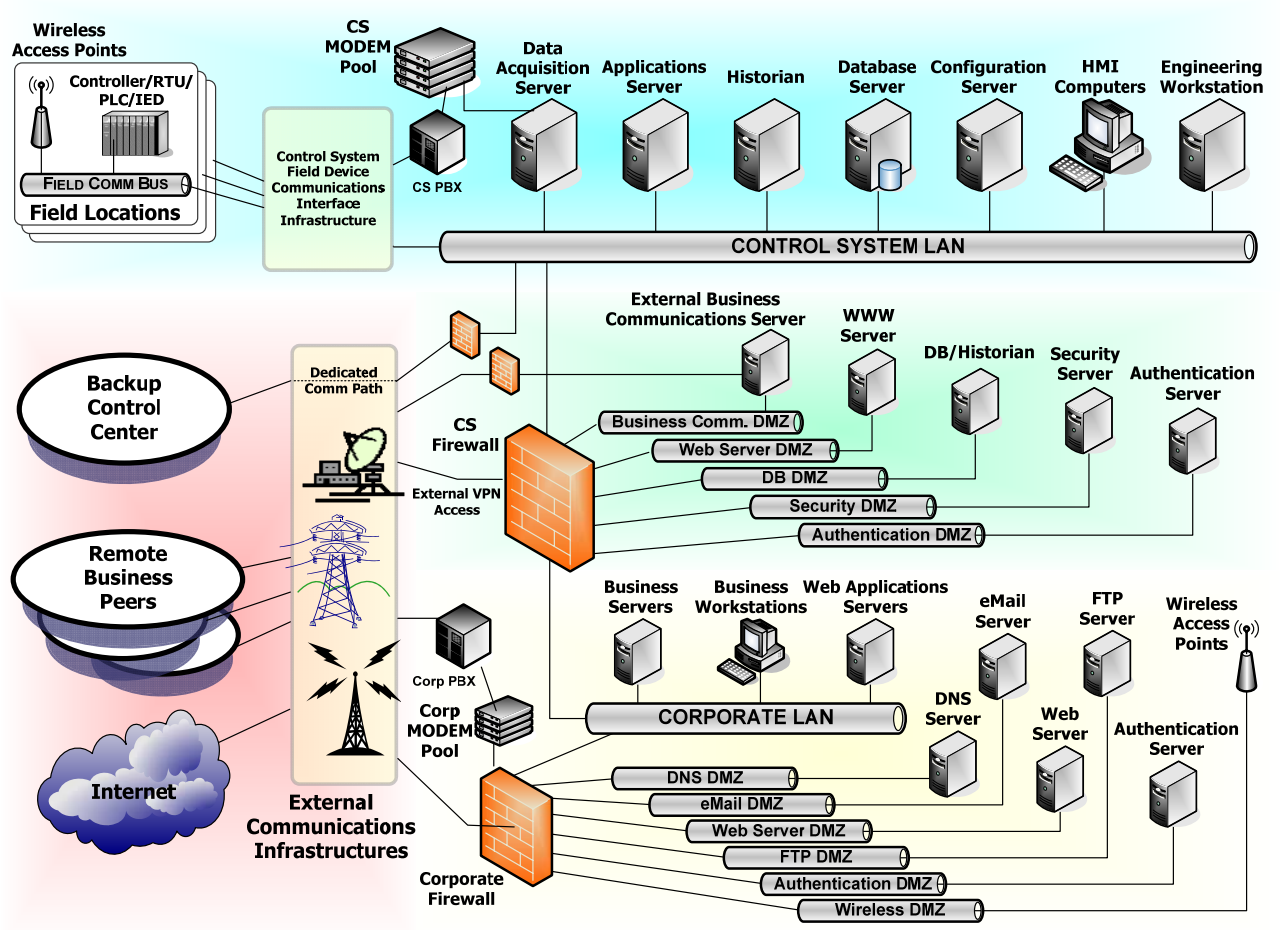

Figure 3. Architecture with DMZ deployments.

Multiple DMZs have proved to be very effective in protecting large architectures comprised of networks with different operational mandates. An example of this kind of architecture is illustrated in Figure 3, which shows the conjoined networks for control systems and business. In this example, the secure flow of data into and out of the different environments is critical to operations. Having multiple DMZs protects the information resources from attacks using Virtual-LAN (VLAN) hopping and trust exploitation and is a very good way to enhance the security posture and add another layer to the defense-in-depth strategy.

INTRUSION DETECTION SYSTEMS

Most intrusion detection systems (IDSs) are signature based, and even though many contemporary IDS signatures files are very robust and can detect a wide range of attacks, the signatures required to monitor for malicious traffic in control networks are not adequate. When looking at the unique communications protocols used in control systems, such as Modbus or DNP3, specific payload and port numbers have traditionally not been a part of the signatures seen in contemporary IDSs. When deploying IDSs in a control system, the ability to add unique signatures must be used. It is also commonplace to remove some of the default signatures and response capability, as it may have no relevance to a control system network. However, analysis must be made to ensure that some of the inherent capability of the IDS is leveraged, with some of the capability refined and augmented. It is imperative, when deploying IDSs on control system networks, that rules sets and signatures unique to that domain be used. It has been shown that developing security signatures and rules in a cooperative relationship with the control system vendor is very advantageous.

THE SECURITY POLICY

Effective security policies and procedures are the first step to a secure control systems network. Many of the same policies used for information technology (IT) security for corporate systems can be applied directly to control system networks. The SANS Institute provides free templates for many types of security policies and can be a valuable resource for control system network administrators in developing their own policies. Control system-specific requirements can then be added to it, such as the North American Electric Reliability Corporation (NERC) cyber security requirements for electric systems.[12]

To make the security policy effective, it must be practical and enforceable, and it must be possible to comply with the policy. The policy must not significantly impact productivity, be cost prohibitive, or lack support. This is best accomplished by including both management and system administrator personnel in policy development.

SECURITY TRAINING

Security training and robust security awareness programs that are specific to the controls systems domain are critical to the security of the control systems and the safety of those involved with any automated processes. Like the security awareness programs that are developed for the corporate domains, the programs that will support control-systems domains have key components that can help drive a continuous and measurable security posture. Within common security awareness programs, such as those listed in NIST SP800-50 “Building an Information Technology Security Awareness and Training Program”[13], organizations can create applicable security awareness and training curricula.

---

[12] http://www.nerc.com/~filez/standards/Cyber_Sec_Renewal.html

[13] http://www.csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

INCIDENT RESPONSE

To fully support a defense-in-depth strategy, a robust incident response capability is required. In the event that there is a security-related incident in the control system domain, activities to recognize, respond, mitigate, and resume need to be established. An incident response procedure will instruct employees on the steps to take if a computer on the network has been compromised. All employees should be trained on and have access to the procedure before an incident occurs. Examples of questions to be answered in the incident response procedure include the following:

- What are the indications that an incident has occurred or is currently in progress?
- What immediate actions should be taken (e.g., should the computer be unplugged from the network)?
- Who should be notified and in what order? Should law enforcement be consulted?
- How should forensic evidence be preserved (e.g., should the computer be left on to preserve the evidence in memory)?
- How can the affected computers be restored?

The National Institute of Standards and Technology (NIST) developed a Computer Security Incident Handling Guide, SP 800-53, which provides guidance to security personnel in developing an incident response procedure. In addition, US-CERT has extensive information and reporting capabilities available for any control system security incident. This reporting can be done at http://www.us-cert.gov/control_systems/.

SPECIFIC RECOMMENDATIONS AND COUNTERMEASURES

When protecting any information infrastructure, good security starts with a proactive security model. This iterative model is comprised of several key security strategies that are illustrated in Figure 4.

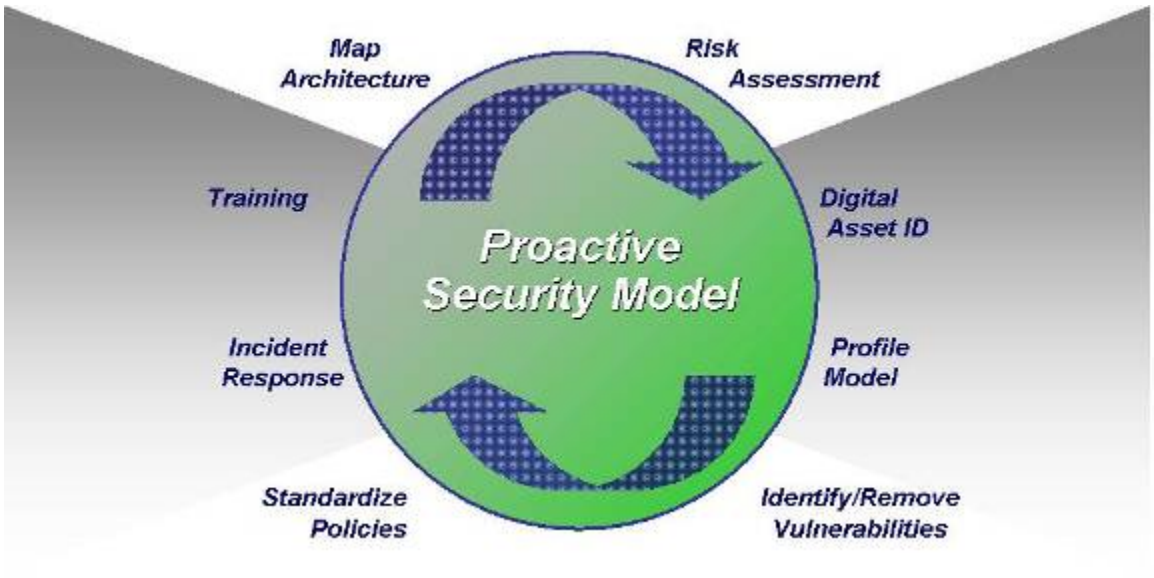

Figure 4. Proactive security model.

Traditionally, development of a defense-in-depth strategy starts with mapping the control systems architecture. Having an accurate and well-documented architecture can enable an organization to be very security-conscious, deploy effective security countermeasures, and be equipped to understand security incidents more readily. Having an understanding of the architecture will allow the administrators to know what it is they want to protect.

A robust understanding of architecture also allows for effective risk assessments, as the development of the assessment parameters and processes can be easily aligned to the existing (and known) information assets in the control system environment.