PNNL-20776

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Secure Data Transfer Guidance for Industrial Control and SCADA Systems

RE Mahan
JD Fluckiger
SL Clements
C Tews
JR Burnette
CA Goranson
H Kirkham

September 2011

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

PNNL-20776

Secure Data Transfer Guidance for Industrial Control and SCADA Systems

RE Mahan
JD Fluckiger
SL Clements
C Tews
JR Burnette
CA Goranson
H Kirkham

September 2011

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PNNL-20776

Pacific Northwest National Laboratory
Richland, Washington 99352

Table of Contents

Introduction

This document was developed to provide guidance for the implementation of secure data transfer in a complex computational infrastructure representative of the electric power an and natural gas enterprises and the control systems they implement.

For the past 20 years the cyber security community has focused on preventative measure intended to keep systems secure by providing a hard outer shell that is difficult to penetra Over time, the hard exterior, soft interior focus changed to focus on defense-in-depth add multiple layers of protection, introducing intrusion detection systems, more effective incid response and cleanup, and many other security measures. Despite much larger expenditu and more layers of defense, successful attacks have only increased in number and severit

Consequently, it is time to re-focus the conventional approach to cyber security. While it is important to implement measures to keep intruders out, a new protection paradigm is warranted that is aimed at discovering attempted or real compromises as early as possibl

Put simply, organizations should take as fact that they have been, are now, or will be compromised. These compromises may be intended to steal information for financial gain the theft of intellectual property or credentials that lead to the theft of financial resources to lie silent until instructed to cause physical or electronic damage and/or denial of service This change in outlook has been recently confirmed by the National Security Agency [19].

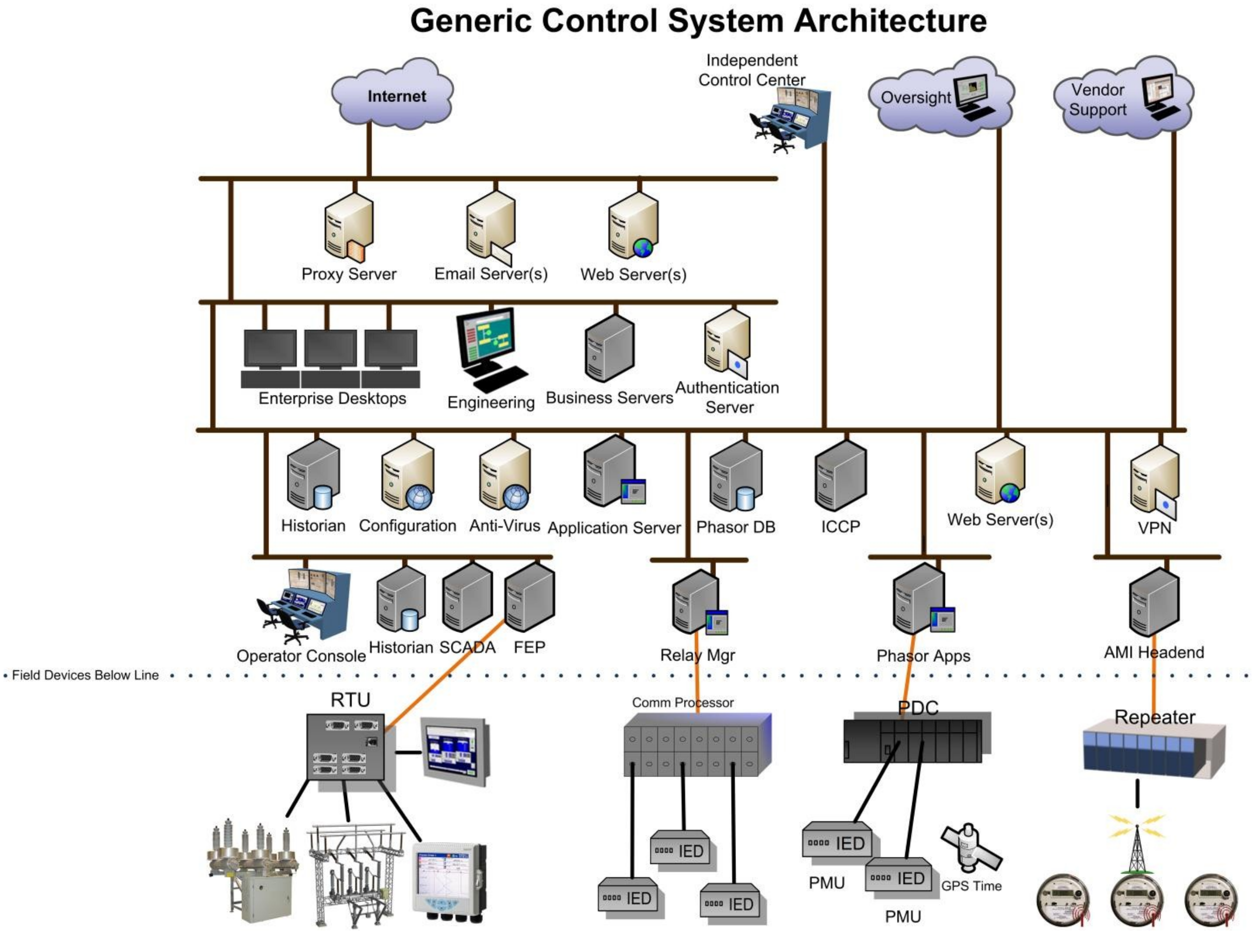
The discovery of attempted and actual compromises requires an increased focus on monit events by manual and/or automated log monitoring, detecting unauthorized changes to a system's hardware and/or software, detecting intrusions, and/or discovering the exfiltratio sensitive information and/or attempts to send inappropriate commands to ICS/SCADA (Industrial Control System/Supervisory Control And Data Acquisition) systems.

Secure Data Transfer

Current Architecture

A generic Industrial Control System/SCADA architecture was documented as shown in Figu to indicate the general functionality typical of existing systems (although actual implementations are highly variable). In addition, 6 use cases are documented at the inte shown by the red dots (1-6) in Figure 2 to indicate locations requiring protection. These us cases are shown in greater detail in Appendix 1.

Figure 1. Generic ICS/SCADA Architecture



RTU: Remote Terminal Unit
IED: Intelligent Electronic Device
PLC: Programmable Logic Controller
PDC: Phasor data Consolidator
PMU: Phasor Measurement Unit
SCADA: Supervisory Control and Data Acquisition

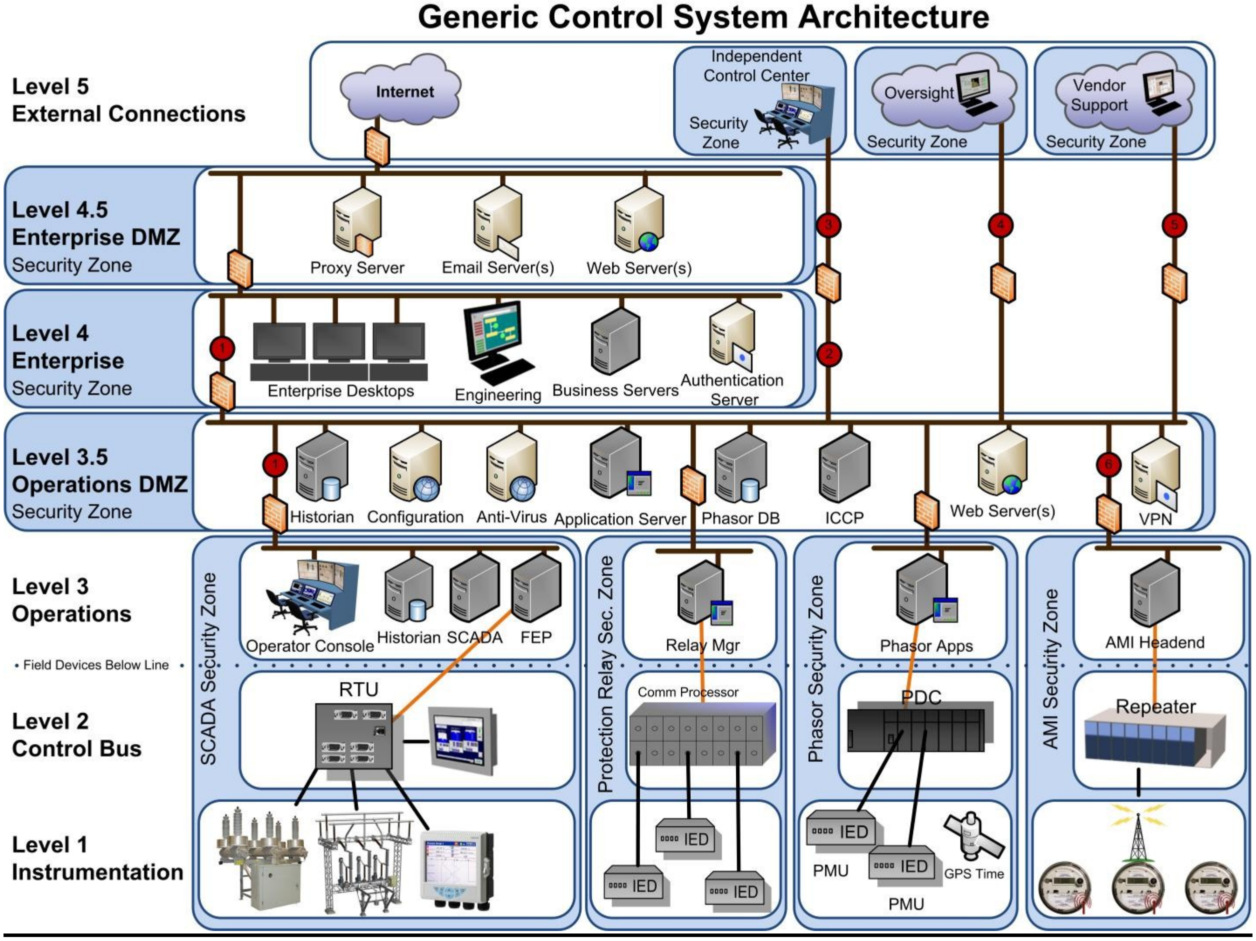
Proposed Architecture

The proposed architecture shown in Figure 2 presents the arrangement of Figure 1 with th addition of the security recommendations made in this document including: 1) improved security for the corporate/enterprise network connection to the Internet; 2) a recommend security zone architecture intended to isolate critical networks; and 3) the addition of mul screened subnets/Demilitarized Zones (DMZ) with no transit traffic.

It is important 1) that the implementation of the proposed architecture should allow no connections between security zones that are not firewall protected; 2) that an inventory o remote access paths that enter the Generic architecture be completed to ensure there are

connections that bypass the firewall infrastructure; and 3) that remote access be through
connection with strong access controls (i.e., at least 2 factor authentication).

Figure 2. Proposed SCADA Architecture



The red circles on the diagrams indicate use cases that were considered while authoring t
guide. Six specific use cases were considered and are presented in greater detail in Apper
Use case 1 is the connection between the Enterprise network and the Operations network
case 2 is the connection between control centers that share phasor data. Use case 3 is the
connection between control centers. Use case 4 is the connection that supports regulatory
reporting (e.g., to NERC). Use case 5 is any connection established to support vendor acti
(e.g., monitoring and maintenance). Use case 6 is the connection that supports data colle
from smart meters. Each one of these connections needs to be protected since each of th
paths represents a potential channel for compromising one, or more, systems that reside
architecture. Not shown is a general enterprise wireless network. If one is present it must
protected from intrusion and compromise.

The Engineering workstations might logically reside inside the enterprise network, in its o
dedicated security zone, or as a part of the operations network. In any case, since enginee

often has a requirement for direct access to control center systems or systems at remotes (e.g., generation, distribution, etc.) these systems must be well protected.

The remainder of this document describes the recommended implementation of the propo architecture.

SECURITY ZONES

Definition

A security zone is a collection of information systems connected by one, or more, internal networks under the control of a single authority and one security policy. The systems may structured by physical proximity or by function, and may be independent of location [1]. F example, engineering and business operations may be located in the same building or dis facilities, but share common functions like e-mail and general web services. Consequently often decided to locate them in the enterprise security zone.

Control centers perform significantly different functions, have some common requirement (e.g., e-mail), and support active communications and control with local and/or remote sit The need for common services delivered to all locations across the entire enterprise argue a single enterprise network, while the need to protect critical resources argues against a common network. The most effective solution to this situation is to segregate the enterpri network into security zones such that necessary services can be supported, but critical resources can be protected.

The most important characteristic of a security zone-based architecture is that all systems residing within a specific zone are protected under the same policy (i.e., all systems must implement at least the minimum level of protection specified for the zone). Conversely, it acceptable for the protection of individual systems within a zone to exceed minimum spec requirements depending on the criticality of the system.

A security zone must have a well-specified boundary, and communication between zones be filtered in accordance with policy. Services, protocols, and applications that are not ess within a zone should be disabled within the zone. Any boundary-crossing traffic carrying th services, protocols, or applications should be blocked at the boundary. For example, ICS/S protocols such as Modbus TCP or DNP3 are required components for controlling process devices. Whenever possible, these protocols should be disallowed outside the Operations security zone. If that is not possible, then compensating measures need to be taken to pro them from attack and/or misuse from sources outside the process control network.

Recommendations

A zone-based architecture is recommended to strengthen the capability to perform secure transfers across the generic SCADA architecture.

Segment the architecture into at least 5 security zones (External Connections, Enterprise Enterprise, Operations DMZ, and Operations).

Issues/Clarification

In some of the literature, security zones are referred to as enclaves. This term is most pre in IT security practices.

Our model loosely follows the zone model described in the Purdue Reference Model (PRM) Computer Integrated Manufacturing of IEC Standard 62254-1 and reference model IEC Standard 622443-1 that suggests a model with 6 zones [2].

Zone 1: Automation: Process (equipment under control), Safety & protection, Basic control/Local control),
Zone 2: Operation Control: Supervisory control,
Zone 3: Operation support: Operation management,
Zone 4: Business support: Business planning and logistics,
Zone 5: Corporate IT: Enterprise IT & common services, and
Zone 6: External Integration: Connections and information transfer to third parties.

ANSI/ISA exhibits a 4 zone model [3].

Enterprise Zone: Corporate systems
Control Center Zone: Primary and Backup Control Centers.
Demilitarized Zone: Historian and Remote Operator Console.
Site Control Zone: Local Operator and Engineering workstations, servers, and ICS/DCS/SC devices.

SCREENED SUBNET (DEMILITARIZED ZONE (DMZ))

Definition

A screened subnet (or DMZ) is a perimeter network segment that is logically between two networks. Its purpose is to enforce the internal network’s Information Assurance (IA) polic external information exchange and to provide external, untrusted, sources with restricted access to information that needs to be released outside the protected network while shiel the internal network from outside attack [4].

The most common DMZ architecture uses a firewall with three network interfaces betwee networks. Interface 1 connects to the external network (e.g., the Internet). Interface 2 connects to the protected DMZ (e.g., the public web servers hosted by the organization) a interface 3 connects to an internal network (e.g., the enterprise network).

Recommendations

Implement an external DMZ to provide public access to external (e.g., Internet) facing ser (e.g., enterprise web services) as provided by corporate policy. No transit traffic is allowe across servers located in the DMZ. Data is pushed to the servers located in the DMZ from enterprise network and accessed by the public.

Add an internal DMZ between the enterprise network and the operations network(s). An Internal DMZ provides enterprise access to operations information, typically the Historian holds data from the ICS/SCADA network and remote stations. No transit traffic is allowed a servers located in the internal DMZ. As a corollary, the historian should not be located on enterprise network or the ICS/SCADA network but should reside in the DMZ, though some secure implementations utilize mirrored historians in the operational network and in the internal DMZ. Similarly, any server (e.g., a data server or patch management server) that jointly accessed from the enterprise network and the ICS/SCADA network should be locate the DMZ and transit traffic blocked. In addition, special attention should be paid to locking down DMZ servers (e.g., removing all unnecessary services, whitelisting IP/MAC addresses limit access to only those workstations approved by policy) In addition, traffic should be subjected to port filtering disallowing unnecessary services between security zones. The c devices that should exist in the DMZ are devices that store data that needs to be shared between networks (e.g., Historian).

Multiple segregated DMZs at either Level 3.5 or 4.5 may be necessary if the architecture requires. In Figure 2 it is likely that the ICCP server would be in its own DMZ separate from other systems at that same level in the hierarchical model.

Issues/Clarification

In most of the literature, a DMZ means a protected network where information is available the public. In this discussion, that network is called the external DMZ. The internal DMZ is accessible to the public, but is accessible from the enterprise network. It is intended to pr the SCADA control center and remotes sites from the enterprise network and any entity th provided SCADA information (e.g., regulatory bodies like NERC). Thus, a compromise of a system in the enterprise or regulatory network will not compromise the SCADA network.

FIREWALLS

Definition

A firewall is a hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy [5].

Architecture

There are four general firewall architectures: packet filtering, stateful inspection, applicati layer, and bastion hosts (the latter are also variously called multi-homed hosts, gateways, proxies).

Packet filters operate at the network layer (layer 3) of the Transmission Control Protocol (T model. Pure packet filtering firewalls check the packet header (typically for type, and sour and destination address) but do not examine the information in the transport layer (layer4 application layer (layer 5). Consequently, attacks on layers 4 & 5 are typically neither bloc nor detected. The primary advantage of packet filters are low cost and minimal impact on network performance. It is often useful to implement packet filtering in a router in front of stateful inspection firewall. This has the dual advantage of providing defense-in-depth and reduces the workload on the stateful firewall.

Stateful inspection firewalls examine the same information as a packet filter (i.e. layer 3) also adds a check on transport layer (layer 4) information. This further check allows it to h traffic such as TCP and connectionless UDP. Such firewalls are more effective in detecting threats, but have higher cost, with greater performance impact, and are more complex to configure and operate.

One of the limitations of current stateful inspection firewalls that examine transport layer protocols is that many do not recognize ICS/DCS/SCADA protocols.

Application layer firewalls (also known as proxy servers) add the capability of examining s application traffic including web services, FTP services, and others. Coverage for ICS/DCS/SCADA applications is presently limited and performance impact is typically great than other firewall types. The benefits of using this method are significant, as the proxy se is the only thing significantly exposed to the untrusted network. The disadvantage of the approach is that it is application-specific. Each packet must be examined down to the application layer (which may be slow) and must be “tuned” to each application allowed.

Bastion hosts or gateways/proxies/multi-homed hosts are general purpose computers with two-network cards. For example, one might be attached to the enterprise network and the other to the ICS/SCADA network. The literature generally advises against the use of dual-h systems because they can be more vulnerable to attack than the dual-homed firewall sinc

are hosted on a general-purpose computer. However, they are low cost solutions and have
been used successfully when they have been "hardened" by:

1) turning off all but the few essential services/daemons and protocols required,
2) limiting user accounts, requiring strong authentication to access the system,
3) not sharing authentication services with trusted hosts on the network,
4) configuring to only open essential ports,
5) configuring for full logging with high integrity (read-only encrypted local logs or logg to a remote system or a read-only device),
6) shutting down as many utilities and configuration tools as is possible,
7) keeping the system fully patched,
8) removing all unnecessary applications, and
9) running an IDS on the system [13][14].

A second major differentiator of firewalls is their placement. Network firewalls are located the ingress/egress point of a protected network (e.g., at a security zone boundary). Host-b firewalls are installed on end devices (e.g., servers, workstations). Many sites implement l network and host-based firewalls as a defense-in-depth measure.

Recommendations

Add a firewall between each security zone.

Ensure a firewall exists between the enterprise network and the SCADA network. Do not a direct communication between the enterprise network and the ICS/SCADA network. This limitation can be implemented by the use of a Demilitarized Zone (DMZ) as described ear this document. If direct traffic between the enterprise zone and operations zone (e.g., engineering access) is required, provide strong authentication and encryption using, for example, a VPN connection.

Add a firewall between the wireless network and the network it connects to.

If a remote station supports a routed network, consider adding a firewall between the SCA network and the remote station.

Perform egress filtering between zones. This will allow the blocking of malware that may got onto the systems via mobile devices that bypass many of the security controls. This f also allows the detection and blocking of exfiltration traffic and unauthorized peer-to-peer traffic.

Firewall Rules

Firewall rules form the basis for filtering traffic between two networks and are designed to one of four actions: 1) Allow/Accept the connection; 2) Allow/Accept the connection based meeting a condition (e.g., encryption); 3) Block/Reject the connection with notification to t source; and 4) Block/Drop the connection without notification to the source. These actions must be specified for both in-bound and out-bound connections to/from the protected network.

Typical conditions for allowing connections require additional action such as: 1) authentica the client; 2) encrypt/decrypt the payload; 3) scan for viruses; and 4) test source address against a whitelist of allowed addresses or against a black list of disallowed addresses. Whitelisting can also be implemented on servers. For example, Microsoft Server 2003 and newer can restrict applications under Group Policy allowing only certain applications to ru

Firewall rules are often created that have conflicts. Consequently the processing order of t rules is an important consideration since a preceding rule can override a following rule.

A few of the most important generic rules are as follows:

1. Block with no notification all inbound traffic destined for the firewall (Stealth rule tha makes the firewall invisible to attack scanners).
2. Block all outbound traffic originated from the firewall (the firewall should not be mak direct connections to external systems).
3. Block all inbound traffic where the source address is an address internal to the protected network (no inbound traffic should contain an address internal to the network).
4. Block all outbound traffic where the source address does not belong to the protecte network (all outbound traffic should have a legal source address).
5. For the process control network ingress and egress traffic disallow http session, ftp session, e-Mail, telnet, ssh, DNS, and any other traffic that is not Historian master o slave traffic, specific to engineering, or vendor maintenance. If these classes of communication to the enterprise or an external network are essential to operations, they should be performed on separate devices (other than process operator console and over a segregated physical or virtual network.
6. For the case of vendor maintenance, the safest path is to allow a session only durin specific maintenance activities and then block it.
7. If engineering or remote maintenance access is needed from the enterprise network any other location, it should be via a VPN tunnel that is enabled using strong authentication. Split tunnels should be disallowed.
8. Nth The last rule is the default rule and should always be Block/Deny without notifica everything not explicitly allowed by the preceding rules.

This is an extremely short list of rules. Actual implementations often operate with a hundr more rules. Consequently it is easy to establish conflicting rules and it is a good idea to ru rule set against a program such as Nipper® that analyzes rules for inconsistencies and/or conflicts [15]. There are many other tools available to aid in building, editing and auditing firewall rule sets.

Firewalls have the capability to log traffic at multiple levels of detail. Decisions will have to made whether to short log or long log each rule. These decisions should be made based o performance requirements and the criticality of the resource being protected.

ICS/SCADA Specific Firewall

While traditional IT firewalls used to isolate networks are generally unaware of ICS/SCADA protocols (e.g., Modbus, DNP3), there is scattered documentation available on the design implementation of firewalls with limited ICS/SCADA awareness. In recent years many firew vendors have begun tailoring their products to the ICS community.

Guidance for SCADA and process control firewall design is available from the UK Centre fo Protection of National Security Infrastructure at: http://www.cpni.gov.uk. There is also be information available from the Department of Homeland Security at http://www.us-cert.gov/control_systems/.

Digital Bond offers firewall rules guidance at: http://www.digitalbond.com/scadapedia/security-controls/best-practices-for-firewalls-in-digital-control-and-scada-systems/

Recommendations include: 1) Authenticate before allowing configuration changes; 2) Perf Self-testing; 3) Perform Logging; and 4) Do not deploy with default settings.

A firewall is available for Modbus TCP implemented under Linux and can be found at Sourc Forge: A download is available at: http://modbusfw.sourceforge.net/

Issues/Clarification

Firewalls may introduce unacceptable latency in ICS/SCADA communications especially in case of Phasor Measurement Units (PMU). Some firewall functions achieve their protection checking packet header information (and even payload content) against lists that are maintained of acceptable and unacceptable addresses. A denial of service attack can be mounted on such a firewall by overloading it with packet to be checked. For PMU data, wh are typically reported tens of times per second (much more frequently than SCADA), such attacks may be too easily able to create unacceptable delays.

The firewall may be bypassed if there are other paths that can reach ICS/SCADA devices. entry points to the ICS/SCADA network should be configured to pass through the firewall. that is not possible additional mitigations should be applied to the system being accessed

Effective firewall rules are essential to the successful implementation of protection. The ru are complex and multiple research studies have often found misconfigured firewall rule se

Multicast traffic is becoming increasingly popular in control environments since it reduces network load and has excellent time synchronization characteristics. However, in complex firewall-protected networks, multicast routing becomes more complex and requires additio protocols and firewall rules.

Hopefully the information presented here illustrates that firewall configuration and maintenance is not a trivial task. Architecting and segmenting a network with security zo relies on proper firewall configurations. It is essential for a secure architecture that those responsible for firewall configuration and maintenance are properly trained and qualified.

INTRUSION DETECTION SYSTEM/INTRUSION PROTECTION SYSTEM (IDS/IPS)

Definition

Intrusion Detection System (IDS): A hardware and/or software product that gathers and analyzes information from various areas within a computer or a network to identify possib security breaches, which include both intrusions (attacks from outside the organization) a misuse (attacks or malfeasance from within organizations) [6]. Both network-based and h based systems are available. Host-based IDS systems monitor security within network components such as servers or workstations while a network-based IDS monitors the traff between network components and networks.

Intrusion Prevention System (IPS): These systems are devices that can detect intrusive ac and attempt to stop the activity, ideally before it reaches its target(s) [6]. IPS systems car recommended to detect, but automated prevention is generally not recommended at laye and lower for SCADA systems, because the preventive action could result in unintended consequences.

Discussion

An early host-based method of detecting intrusions was based on the capability of a syste log security events. Early systems relied on manual methods to examine the logs on a sys or systems, for anomalous behavior. Logs tended to be large and reading them is labor intensive and often neglected because of the level of effort and monotony of the work. However, in most successful compromises, evidence of the attack can almost always be fo in the logs unless the attacker has taken special care to expunge the logs of the comprom events. Advanced logging systems log the information to a read-only device or a location remote from the system being monitored, preserving the information. More recently, log analysis software has been developed to automatically examine logs and generate alerts central location. More sophisticated systems canonize the logs into a standard form, store information in a database, and use structured queries to examine and correlate security e OSSEC is an example of an open source host-based intrusion detection system using a centralized system for analysis and alerting [16][17]. The most important characteristic of centralized logging and analysis is the capability to automate the analysis activity and ger alerts that trigger additional manual analysis.

Another detection approach is to install a tool that calculates a cryptographic checksum (i hash) on critical files, store the hashes in a secure location, and alert an administrator whe unauthorized change is made to critical files (e.g., a configuration file or registry entry is changed or a new account is added).Such a tool can also be used to monitor controlled changes. The system is examined after the authorized change to ensure that only the authorized change was made. A well-known software package that performs this function Windows and Linux systems is Tripwire [18].

Network Intrusion Detection Systems (NIDS) record and analyze network traffic informatio related to security events, notify administrators of suspicious events, and generate report network IDS uses one of two detection techniques; signature matching or anomaly detect Statistical-based anomaly detection systems determine normal network activity (e.g., bandwidth used, protocols, ports, and communicating devices) and alert on anomalous tra Signature-based systems monitor network traffic and alert on known attack patterns. NIDS often subject to weaknesses due to encoding that masks malicious traffic, out-of-order pac sequencing, and encrypted malware communications.

Host Intrusion Detection Systems (HIDS) perform the same functions as a NIDS using sign matching and/or anomaly detection, but are designed to overcome issues with encoding, sequencing, and encryption since they can view the incoming traffic after it is decoded, correctly sequenced, and/or decrypted. The problem is that the end device must be capab running the HIDS and the HIDS must correctly detect the attempted intrusion. In addition, is often more expensive to implement and maintain than NIDS.

Finally, a honeypot can also be used to detect intrusions. A honeypot is a system configure attract an intruder. It is essentially a trap set up to detect, deflect, and identify malicious a order to respond to and defeat attempts at compromising operational systems.

Recommendations

Implement remote syslog for auditing and logging requirements. Events should be forward a syslog server each time an auditable event occurs to ensure event capture. This can be accomplished for Windows, Macintosh, Unix, and many Linux variants [20].

Use the logging capability of the firewall and consider the use of additional software to an firewall logs. There is a free product that can perform this analysis available from Digitalbo

called Portaledge [21]. It requires the PI Server from OSIsoft, the appropriate OSIsoft licen
and reads logs from Cisco PIX and Juniper firewalls.

Add IDS/IPS capability for each security zone with coverage that monitors traffic crossing t
firewalls to detect potential intrusions attempting to enter the zone. Additional IDS/IPS sys
can be used to cover each network segment within a security zone to detect insider intrus
attempts.

The IDS for the ICS/DCS/SCADA network should be capable of monitoring control system protocols in use at the site such as Modbus TCP, DNP3, ODVA, Ethernet/IP ICCP, and others

SNORT is a popular open source IDS system with signatures available for DNP3, Ethernet/I
ModBus TCP, and some general SCADA vulnerabilities from Digital Bond[11] The general vulnerability signature set identifies attacks on previously disclosed control system vulnerabilities. There is no charge for the download, but registration as a digitalbond.com subscriber is required. Some commercial vendors now support the DigitalBond Quickdraw
in their IDS offerings including: 3com/Tipping Point, Cisco, Counterpane/BT, Fortinet, Indus
Defender, ISS/IBM, Juniper, McAfee, Secureworks, Symantec, and Tenable Security.

Industrial Defender also offers a SNORT-based Network Intrusion Detection System (NIDS)
is aware of Modbus TCP, DNP3, ODVA, and Ethernet/IP ICCP[12]. The SNORT sensor device
designed to report to Industrial Defender’s centralized Security Event Monitor (SEM).

Limit the use of IPS and rely on IDS and/or log analysis for detection and the determinatio
appropriate actions to take. While IPS has automatic response capabilities, they may inter
with ICS/SCADA operations creating more problems than they are stopping and should be considered potentially dangerous unless clearly proven safe.

Issues/Clarification

A few custom systems have emerged from research that are ICS/DCS/SCADA protocol awa
but are limited in the protocols supported. A survey of SCADA-specific IDS systems is avai
[10].

IDS/IPS capabilities must be fully tested before deployment to ensure they do not interfere
ICS/SCADA systems.

COMMUNICATIONS LINKS

Definition

A communications link, or channel, is a single path provided by a transmission medium us transport analog or digital information between a source and receiver.

Commonly used transmission paths used to support communications include guided medi such as copper wire and fiber optics and unguided media such as radio, microwave, and la Services commonly used to support ICS/SCADA communications include: 1) Dial-up teleph lines; 2) Leased/Owned dedicated lines; 3) Microwave; 4) Satellite; 5) Radio; 6) Wireless networks; and 7) The Internet.

While each media type and/or service is susceptible to various security problems (e.g., eavesdropping, interception, re-direction, re-play, and modification), the major concern sh be focused on determination of the requirements that are important to the organization: Consideration must be given to: 1) secrecy, or confidentiality of the transmission; 2) authentication of the sender and/or receiver; 3) proof that the message received was originated by the sender (i.e., non-repudiation) and; 4) that the message has not been alt in transit (integrity control).

Encryption is used to provide secrecy/confidentiality. Strong authentication (at least two-fa is used to establish identity. Non-repudiation can be provided by a cryptographic digital signature, and integrity is provided by a hash function to create a message digest or Mess Authenticating Code (MAC).

Recommendations

Cryptography should be used to provide one, or more, of the required protections. Howeve is important to use proven cryptographic algorithms that are well known, are not themselv secret, and have stood the test of time. Examples include NIST approved algorithms such Advanced Encryption Standard (AES), Triple-Data Encryption Algorithm (TDEA), or Triple Da Encryption Standard (TDES) for secrecy, CMAC for authenticity, and Secure Hash Standard 256, 384, or 512) for integrity. A more detailed list of algorithms recommended by NIST fo Smart Grid Cyber Security is available [23].

ENCRYPTION

Definition

Encryption is the process of changing plaintext into ciphertext through the use of a cryptographic algorithm [7].

There are two major types of encryption, symmetric key and asymmetric key. The first, symmetric key, uses one shared key to encrypt and the same key to decrypt. The second, asymmetric key, uses different keys for encryption and decryption. It is also known as pub key encryption since one key is publicly known and the other is kept secret. The strength o encryption, or its resistance to breakage depends on the key length, the quality of the alg and keeping the key secret (in symmetric encryption) or keeping the private key secret (ir asymmetric encryption).

The infrastructure to implement public-key encryption includes software and hardware, of course, as well as a set of policies and procedures to be followed. The systems involved m include a component (called a Certificate Authority) that manages digital certificates, and another (called a Registration Authority) that uses this information in routine operation. Th infrastructure (called a PKI) is not yet standardized, and is not yet widely implemented in utility environment.

Encryption can be a double edged sword. While it can perform necessary and useful servic the system being protected, attackers are more frequently using encryption to hide inform from (and therefore to bypass) firewalls and/or network IDS systems. Therefore, sites shou consider strategies that can identify legitimate and rogue encryption so traffic containing encryption can be blocked. Another option is to disallow encrypted files through the firewa One way this can be accomplished is by using in-line encryptors.

Recommendations

SECRECY

Use a strong algorithm (e.g., the Advanced Encryption Standard (AES)) to encrypt traffic th travels over communications links that are not under the direct control of your organizatio That is, encrypt link traffic that passes through facilities/over media owned by others or w the media is not physically secured. This should be a default requirement for any wireless communications.

INTEGRITY

Integrity is “guarding against improper information modification or destruction, and incluc ensuring information non-repudiation and authenticity.”*7+

At a minimum one should implement controls to ensure data integrity on important proces and critical path, e.g., the connection between the control room and field devices. NIST approved algorithms for generating secure hash-based message authentication codes (HM (e.g. SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) should be used where technically feasible. On low-bandwidth serial connections other protocols may be necessary (e.g. Se SCADA Communications Protocol (SSCP) or Streaming Encryption Protocol (SEP)).

ACCESS CONTROL AND AUTHENTICATION

Definition

Access control is the process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical fac (e.g., federal buildings, military establishments, border crossing entrances, etc.).

Authentication is the process of verifying the identity or other attributes claimed by or ass of an entity (user, process, or device), or to verify the source and integrity of data [9].

Recommendations

Implement access control at all entry points to the enterprise/control center/ICS/SCADA networks. Authenticate all users attempting access to a protected security zone using a st authentication mechanism (e.g., Virtual Private networking (VPN), two-factor authenticatio Avoid the use of insecure applications such as plaintext telnet and ftp replacing them with secure versions that perform the same functions. If a device cannot support secure login, restrict IP addresses that can access these devices.

TOOLS THAT SUPPORT THE RECOMMENDATIONS

There are a number of tools that can be used to implement the proposed recommendatior Some tool sets are robust while others are much more limited. The SANS Institute has developed a list of tools that have been confirmed by users to automate part or all of the 20 Critical Security Controls [21].

REFERENCES

*1+ Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 729
Revision 1, National Institute of Standards and Technology, February 2011, pg 68. Availabl
http://csrc.nist.gov/publications/PubsNISTIRs.html

[2] Zerbst, J-T., E. Hjelmvic, and I. Rinta-Jouppi, “Zoning Principles in Electricity Distributio
Energy Production Environments”, Proceedings of the 20th International Conference on
Electricity Distribution, Prague, June 8-11, 2009. Available at:
http://www.cired.be/CIRD09/pdfs/CIRED2009_0838_Paper.pdf

[3] ANSI/ISA 99.02.01-2009, “Security for Industrial Automation and Control Systems”,
American National Standards Institute, 2009. Available for a fee at:
http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDis
.cfm&ProductID=10234
[4] Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 7298
Revision 1, National Institute of Standards and Technology, February 2011.pg 61. . Availab
http://csrc.nist.gov/publications/PubsNISTIRs.html

[5+ Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 729
Revision 1, National Institute of Standards and Technology, February 2011, pg. 77. . Availa
at: http://csrc.nist.gov/publications/PubsNISTIRs.html

[6+Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 7298
Revision 1, National Institute of Standards and Technology, February 2011, pg. 102. . Avail
at: http://csrc.nist.gov/publications/PubsNISTIRs.html

[7+ Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 729
Revision 1, National Institute of Standards and Technology, February 2011, pg. 68. . Availa
at: http://csrc.nist.gov/publications/PubsNISTIRs.html

*8+ Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 729
Revision 1, National Institute of Standards and Technology, February 2011, pg. 4. . Availab
http://csrc.nist.gov/publications/PubsNISTIRs.html

[9+ Kissel, R., editor, “Glossary of Key Information Security Terms”, NISTIR Report No. 729
Revision 1, National Institute of Standards and Technology, February 2011, pg. 14. . Availa
at: http://csrc.nist.gov/publications/PubsNISTIRs.html

[10+ Zhu, B., and S. Sastry, “SCADA-Specific Intrusion Detection/Prevention Systems: A Su
and Taxonomy”, First Workshop on Secure Control Systems, part of 13th International

Conference on Hybrid Systems; Computation and Control. April 12, 2010, Stockholm, Swe
Available at: https://www.truststc.org/conferences/10/CPSWeek/program.htm

[11] Digital Bond Quickdraw SCADA IDS Signatures. Available at:
http://www.digitalbond.com/tools/quickdraw/

[12] Industrial Defender Network Intrusion Detection System. Available at:
http://www.industrialdefender.com/products/nids.php
[13] Kurt Dillard, "Intrusion Detection FAQ: What is a Bastion Host". SANS Institute. Availa
http://www.sans.org/security-resources/idfaq/bastion.php

[14] Gite, V., "Configure Linux As Bastion Host", NnixCraft web site, June 26, 2009. Availab
http://www.cyberciti.biz/faq/linux-bastion-host/

[15] Titania Nipper, Network switch, router, and firewall auditing software. Available at:
https://www.titania-security.com/nipper/overview

[16] OSSEC Documentation Page. Available at: http://www.ossec.net/doc/

[17+ Robertson, Chad, "Practical OSSEC", SANS InfoSec Reading Room, July 5, 2011. Avail
http://www.sans.org/reading_room/top25.php

[18] Tripwire home page. Available at: http://www.tripwire.com/

[19+ "U.S. Code-Cracking Agency Works as if Compromised", Reuters Canada, December
2010. Available at: http://ca.reuters.com/article/technologyNews/idCATRE6BF6BZ2010121

[12+ Nawyn, Kenneth, "A Security Analysis of System Event Logging with Syslog", SANS R
Room, October 31, 2003. Available at:
http://www.sans.org/reading_room/whitepapers/logging/

[21] Protaledge is available at: http://www.digitalbond.com/tools/portaledge

[22] A list of the 17 user vetted tools is available at: http://www.sans.org/critical-security-controls/user-tools.php

[23] National Institute of Standards and Technology, "Guidelines for Smart Grid Cyber Sec
Vol. 1, Smart grid Cyber Security Strategy, Architecture, and High-Level Requirements", N
7628, August 2010. Available at: http://csrc.nist.gov/publications/nistir/ir7628/mistir-7628_vol1.pdf

*A1+ Hadley, M.D., J.B. McBride, T.W. Edgar, L.R. O'Neil, and J.D. Johnson, "Securing Wide
Measurement Systems", PNNL-16705, Pacific Northwest National Laboratory, June 2007.
Available at: http://energy.gov/oe/downloads/securing-wide-area-measurement-systems

[A2] ASAP-SG Wide-Area Monitoring, Protection, and Control (Synchrophasor) Security Prof
(Draft) v0.08 is available at:
http://www.smartgridipedia.org/images/5/5e/WAMPAC_Security_Profile_-_v0_08.pdf

[A3] ASAP-SG Third Party Data Access Security Profile v1.0 is available at:
http://www.smartgridipedia.org/images/6/65/3PDA_Security_Profile_-_v1_0_-_20110518.pd

[A4] ASAP-SG AMI Security Profile v2.0 is available at:
http://www.smartgridipedia.org/images/9/90/AMI_Security_Profile_-_v2_0.pdf

ICS/SCADA SPECIFIC BIBLIOGRAPHY

The following documents provide guidance specific to ICS/DCS/SCADA cyber security protection.

British Columbia Institute of Technology (BCIT), “Good Practice Guide on Firewall Deploym for SCADA and Process Control Networks (Prepared for National Infrastructure Security Co-ordination Centre)”, National Infrastructure Security Co-ordination Centre (NISCC), February 2005. Available at: http://www.cpni.gov.uk/docs/re-20050223-00157.pd

A widely referenced guide covering multiple types of firewalls, descriptions of 8 alternativ segregating the process control/SCADA network for an enterprise network, recommended firewall rules for specific services, and addresses firewall issues with regard to data histor remote access requirements, and multicast traffic.

Byers, E., B. Chauvin, J. Karsh, D. Hoffman, and N. Kube, “The Special Needs of SCADA/PC Firewalls: Architecture and Test Results”, IEEE 10th Conference on Emerging Technologies and Factory Automation, Catania, Italy, 2005. pp. 884-892. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1612765 and/or from: http://www.tofinosecurity.com/professional/special-needs-scadapcn-firewalls-architectures and-test-results (free registration required).

Argues that current SCADA/PCN firewall are often poorly implemented, but that they can b successfully implemented based on test results for the configuration of four firewalls.

Homeland Security, “Recommended Practice for Patch Management of Control Systems”, Department of Homeland Security, December 2008. Available at: http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

Focused on the overall patch management issue for ICS/SCADA systems including the requirements for a successful patch management program, required analysis prior to patc and patch deployment processes.

National Security Agency, “A Framework for Assessing and Improving the Security Posture Industrial Control Systems (ICS)”, Version 1.1, Systems and network Analysis Center, Natio Security Agency, August 20, 2010. Available at: http://www.nsa.gov/ia/guidance/security_configuration_guides/ics.shtml

Covers the mapping of all ICS networked assets and communications links, assessment of consequences of a loss of assets, an assessment of threat sources attack vectors and atta difficulty, and prioritizing defensive measures.

Stouffer, K., J. Falco, and K. Scarfone, “Guide to Industrial Control Systems Security”, Natio Institute of Standards and Technology, Special Publication 800-82, dated June 2011. Availa at: http://csrc.nist.gov/publications/PubsSPs.html

SP 800-82 covers an overview of industrial control systems, describes threats and vulnera how to create a business case for implementing ICS protection, covers the elements for establishing an ICS security program, developing a firewall-protected network architecture recommends a list of security controls that are recommended for implementation.

Peterson, D., “Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Netwo ISA, 2004. Available at: http://www.techrepublic.com/whitepapers/intrusion-detection-and-cyber-security-monitoring-of-scada-and-dcs-networks/126355

Now dated, covers existing use of IDS and log monitoring in SCADA systems, limitations d lack of applications and protocol awareness, and suggests the development of SCADA awa IDS signature (which is beginning to occur). Urges the analysis of existing SCADA logs.

Department of Homeland Security CPNI “Cyber Security Assessments of Industrial Control Systems” November 2010. Available at: http://www.us-cert.gov/control_systems/pdf/Cyber_Security_Assessments_of_Industrial_Control_Systems.

Describes what elements should be included in a security assessment of industrial control systems. It is descriptive but not prescriptive. This documents aims “to assist asset owne maximize the return on their investment when commissioning assessments of their ICSs.”

GENERAL BIBLIOGRAPHY

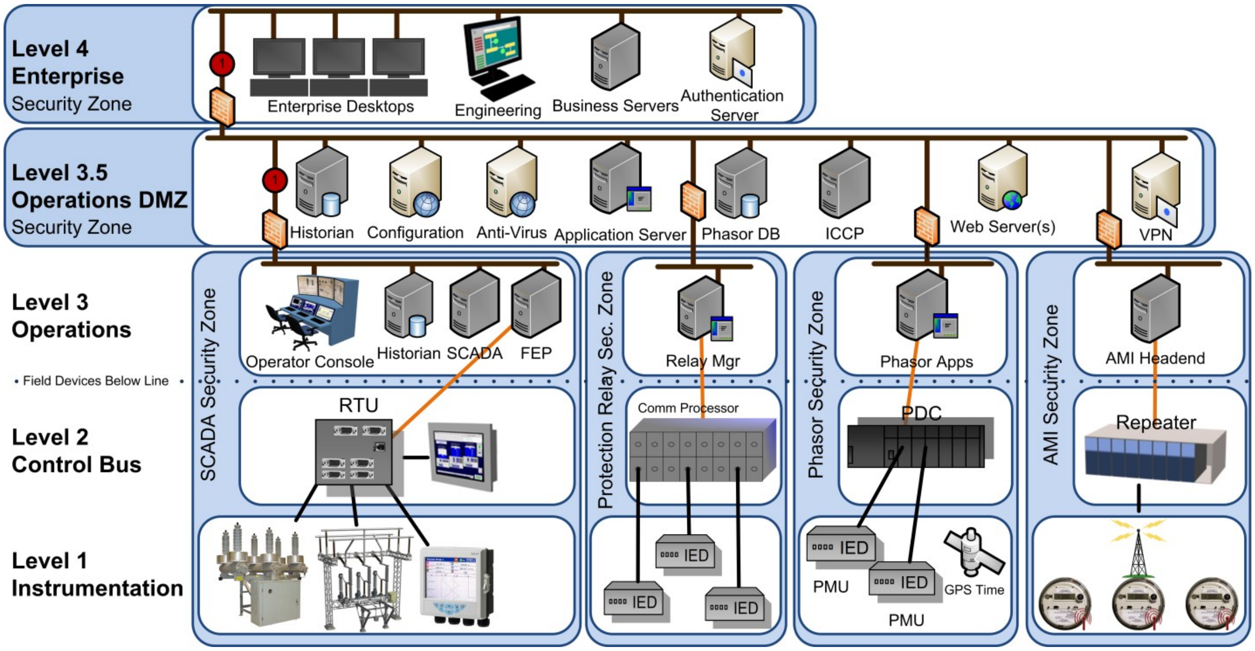
Cyber Security Operations Centre, “Top 35 Mitigation Strategies”, Australian Government Department of Defense, July 21, 2011. Available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

National Institute of Standards and Technology, “Recommended Security Controls For Fede Information Systems and Organizations”, NIST Special Publication 800-53, Revision 3, Aug 2009. Available at: : http://csrc.nist.gov/publications/PubsSPs.html

Appendix I of SP 800-53 provide supplemental guidance specifically tailored to the require of industrial control systems.

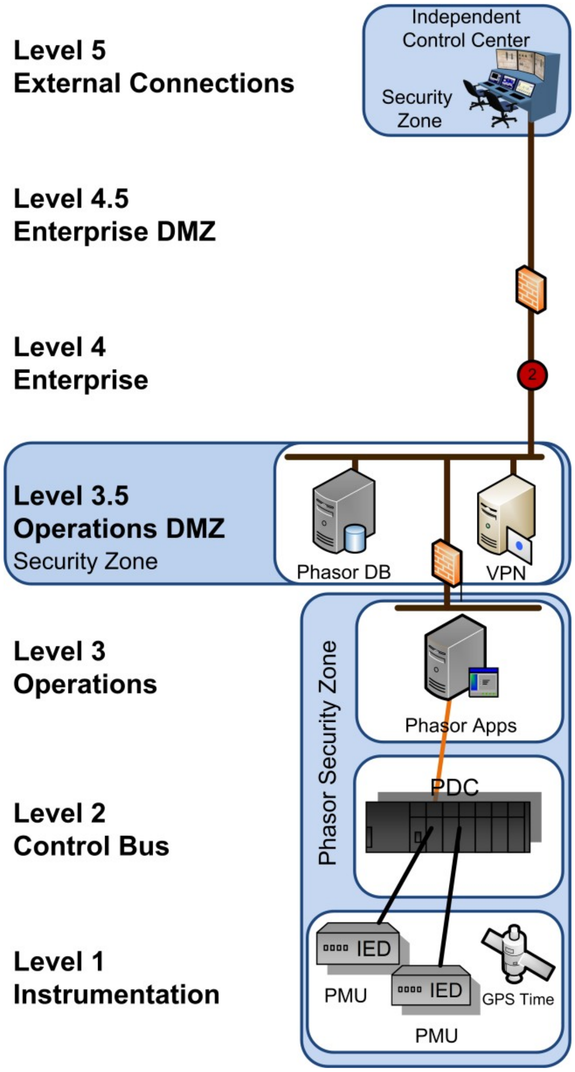
APPENDIX A – Use Cases

Use Case 1: Enterprise Network to Operations Network.



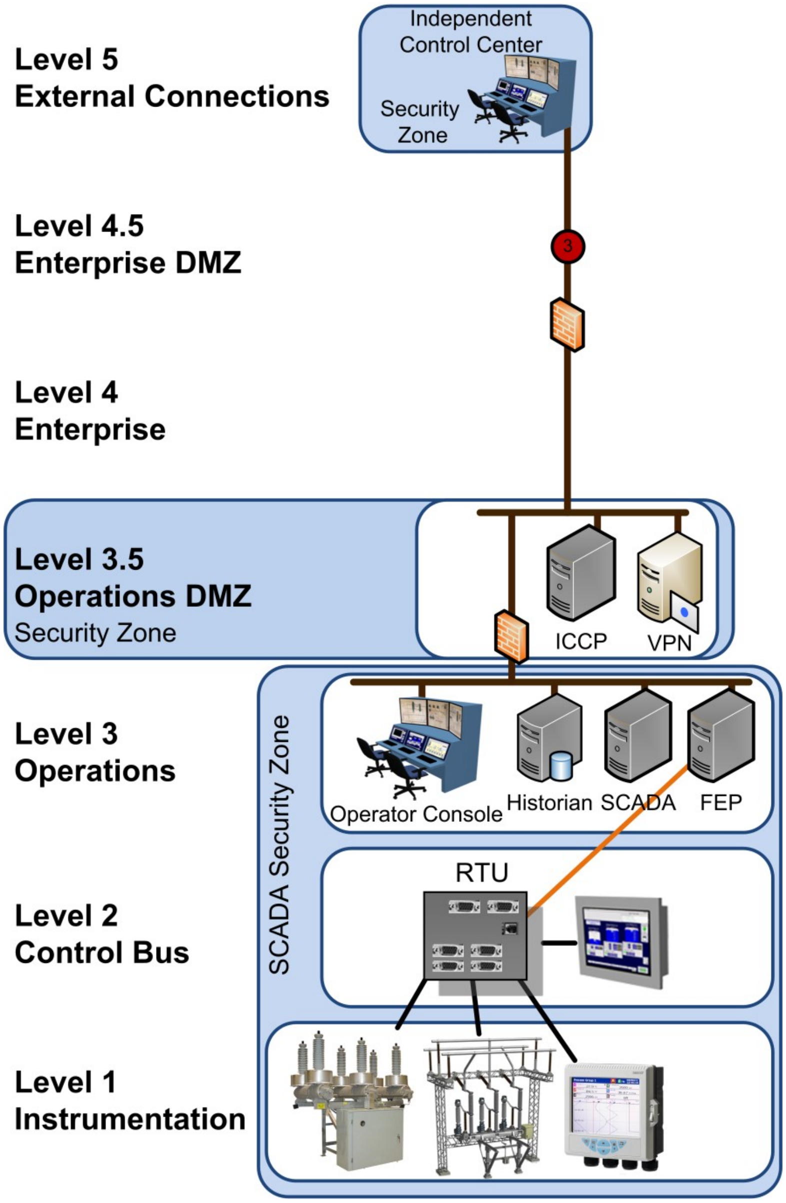
The Enterprise network should be considered a hostile network. It is complex, supports ma vulnerable protocols and even if strongly protected is susceptible to zero-day attacks. Consequently, the operations network needs to be protected from systems in the enterpri network that may have been compromised. This means that information shared between enterprise network and the control center (e.g., Historian, patch management servers, etc need to be staged in a DMZ with no transit traffic allowed. Where direct access is required as from engineering workstations, it should be via strong authentication, such a VPN or us two-factor authentication, accessing workstations should be whitelist allowed, and the nu of protocols allowed between the networks should be limited to those few that are critical necessary for operations. Implement IDS within both networks.

Use Case 2: Operations Network to External Control Center Network (Phasor Data).



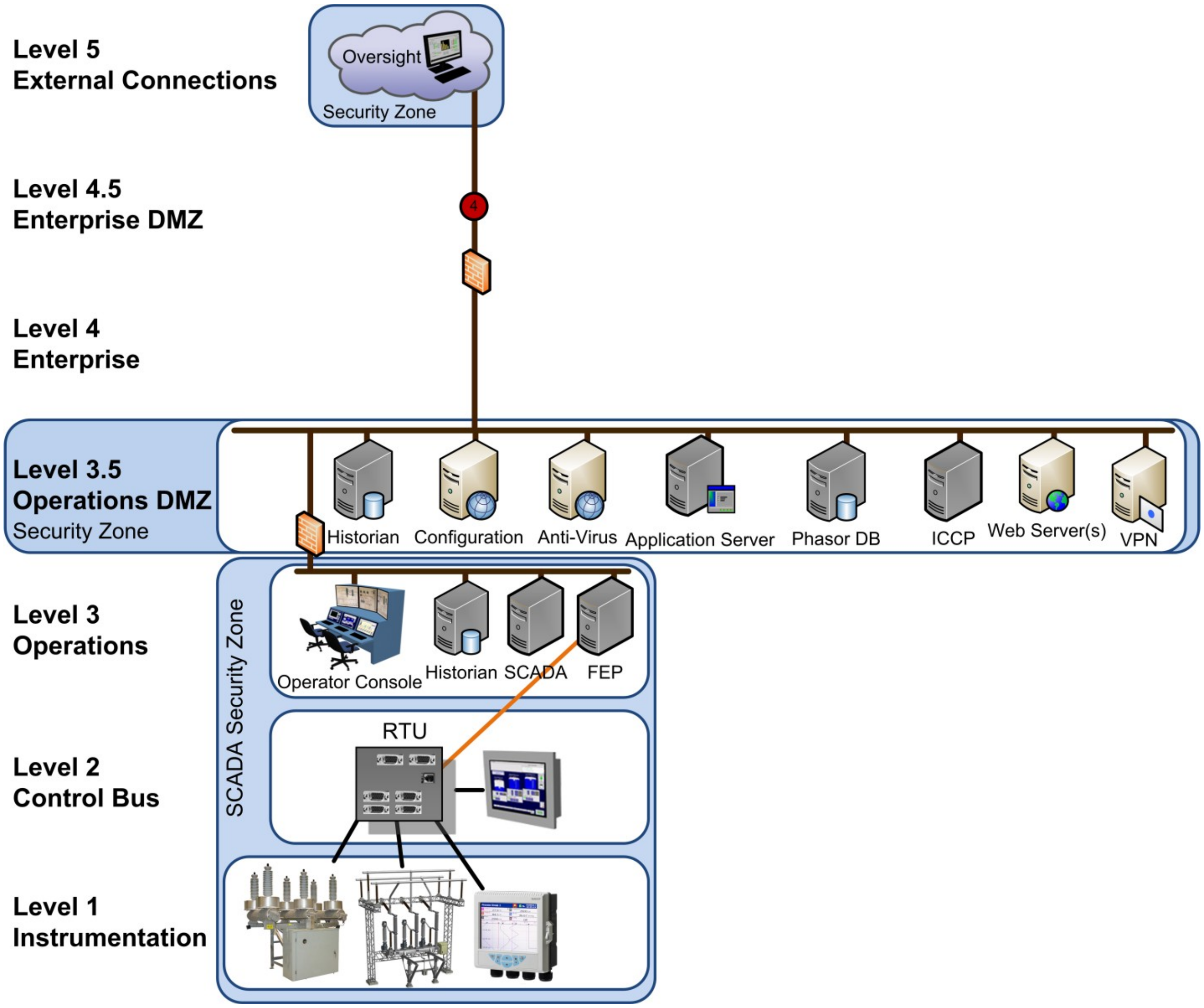
Wide Area measurement Systems (WAMS) security has been addressed in a separate repo and will not be repeated here [A1]. This report focuses on risks and vulnerabilities in cybe security, reliability, data quality and human performance as they relate to WAMS. The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) is developing a secu profile titled Wide-Area Monitoring, Protection and Control (Synchrophasor) Security Profile [A2] to further address this use case. It is currently in early draft form.

Use Case 3: Operations Network to External Control Center Network Data.



The Inter-Control Center Communications Protocol is used for communications control cen over Wide Area Networks and is subject to the same attacks experienced by other routabl protocols. While there is a security enhanced version of ICCP, TASE.2 that strengthens sec it requires a Public Key Infrastructure, which is not widely implemented in the utility indus The ASAP-SG Third Party Data Access Security Profile v1.0 [A3] provides detailed informat about securing this use case.

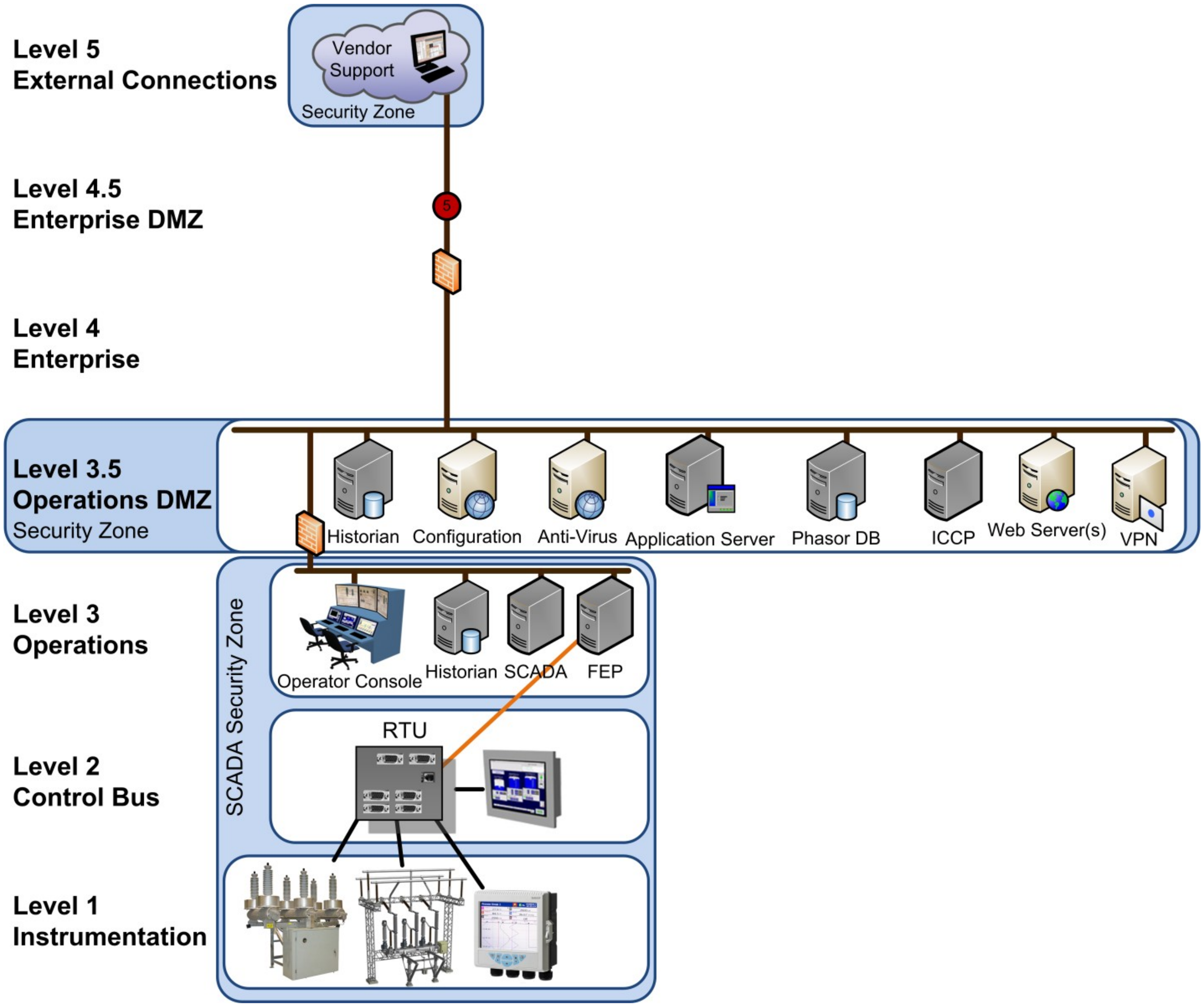
Use case 4: Operations Network to NERC, Regulatory Data.



Sites are required to report to various regulatory bodies (e.g., NERC). Reporting is typically electronic via a communications link that poses a potential threat to the site. The threat c minimized by isolating the system that performs the reporting, typically a historian such t required reports are staged to the reporting server and no transit traffic is allowed from th server to the control or ICS/SCADA networks. Reports should be generated, deposited on t server and then either pushed to the regulator or made accessible to the regulator. If secr integrity, and/or non-repudiation is required, it should be implemented with robust cryptography.

The ASAP-SG Third Party Data Access Security Profile v1.0 [A3] provides detailed informat about securing this use case.

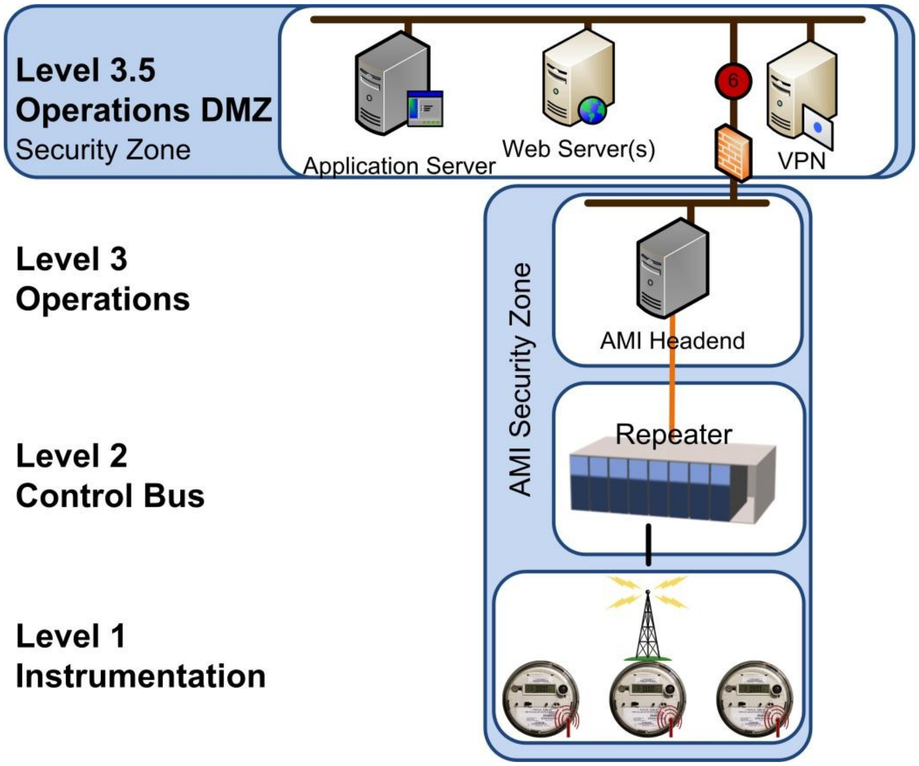
Use Case 5: Operations Network to Vendor Network, Support & Maintenance.



Third party access to cyber resources within the control center and/or remote sites is typic required to support installations, upgrades, troubleshooting, and remedial maintenance. T primary issue with third party access is with remote communication links established to su vendor activities. Such a link provides a potential path for the introduction of malware into system being serviced. Remote access should be via VPN and/or use of strong authenticat Wherever possible, the accessed system should be isolated from other systems on the ne during the work activity, any vendor performing work onsite should be escorted, access sl be at the lowest privilege level feasible and all work activities should be observed by tech staff.

The ASAP-SG Third Party Data Access Security Profile v1.0 [A3] provides detailed informat about securing this use case.

Use Case 6: Operations Network to Advanced Metering Infrastructur



Automated meter reading using wireless technology is rapidly growing and with the introduction of “Smart grid” technology allows fine-grained control over consumer loads. However, the introduction of wireless technology, whether in the smart grid or as part of t enterprise, control center, or remote site infrastructure bring with it serious security conce The wireless network should be isolated from other networks by a firewall and implemente with strong encryption and authentication. Many AMI vendors use licensed frequencies an proprietary protocols to gather meter data. The adherence to security of these solutions c vary dramatically and special consideration should be given when evaluating these syster The ASAP-SG AMI Security Profile v2.0 [A4] provides detailed information about securing t use case.

APPENDIX B: Crosswalk with NISTIR 7628

Background

The NISTIR 7628 is a hefty and detailed document that provides high-level guidance on se smart grid systems. It can be used to find guidance on all aspects of cyber security for sn grid systems. The Secure Data Transfer Guidance for Industrial Control and SCADA Syster meant to be a helpful hands-on guide to securely moving data around a network. It is not intended to be as broadly encompassing of security issues as the NISTIR 7628. Consequer not all of the requirements recommended in the NISTIR 7628 are found in the recommendations of this document.

Crosswalk

This appendix is intended to highlight how the recommendations given in this document r to the guidance given in the NISTIR 7628.

Secure Data Transfer	NISTIR 7628
• Generic SCADA Architecture	• Vulnerability C.4.1.1 Inadequate Security Architecture and Design Security Zones • Vulnerability C.4.3.5 Inadequate Network
Segregation • **Disallow Unneeded Protocols**	• Vulnerability C.4.3.2 Unneeded Services Running • Vulnerability C4.3.6 Inappropriate Protocol Selection
Demilitarized Zone (DMZ)	• DHS – 2.15.28 External Access Protection
Firewalls	• DHS - 2.8.7 Boundary Protection • DHS – 2.8.7.2 Supplementary Guidance • DHS – 2.15.15 Information Flow Control • DHS – 2.15.28 External Access Protections • Vulnerability C.4.3.5 Inadequate Network Segregation
Protect all entry points	• DHS – 2.8.18 System Connections
Intrusion Detection • **Logs** • **Intrusion Detection Systems**	• DHS – 2.14.3 Malicious Code Protection • DHS – 2.14.4 System Monitoring Tools and Techniques • Vulnerability C 4 3.3 Insufficient Log Management • Vulnerability C.4.3.4 Inadequate Anomaly Tracking • Vulnerability C.4.3.9 Physical Access to Device
Communication Links	• DHS – 2.8.8 Communications Integrity
Cryptographic Secrecy	• DHS – 2.8.9 Communications Confidentiality • DHS – 2.8.7 Boundary Protection

	• DHS – 2.15.24 Remote Access
Cryptographic Integrity	• DHS – 2.8.7 Boundary Protection • DHS – 2.14 System and Information Integrity • DHS – 2.14.7 Software and information Integrity • DHS – 2.15.Remote Access • DHS – 2.15.28 External Access Protections • Vulnerability C.5.1 Inadequate Integrity Checking
Cryptographic Authenticity	• DHS – 2.8.20 Message Authenticity
Use Validated Cryptography	• DHS – 2.8.12 Validated Cryptography
Access Control and Authentication	• DHS – 2.15 Access Control • DHS – 2.15.28 Remote Access

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov