APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-CCS-004-16
Published: October 26, 2016

Control and Communications Security Working Group

Securing Control and Communications Systems in Rail Transit Environments

Part IIIb: Protecting the Operationally Critical Security Zone

Abstract: This document covers recommended practices for securing control and communications security systems in the Operationally Critical Security Zone (OCSZ) in rail transit environments.

Keywords: operationally critical security zone (OCSZ), control and communications security, cybersecurity, Demilitarized Zone (DMZ), rail transit vehicle, SCADA (supervisory control and data acquisition), wireless communication, Virtual private network (VPN), incident response, secure coding

Summary: This document provides control and communications security systems designed to protect a transit agency's OCSZ, including traction power and non-life-safety critical SCADA systems. Systems in this zone must be protected from cyber-risks to ensure proper functioning of the transit system.

Scope and purpose: This *Recommended Practice* is not intended to supplant existing safety/security standards or regulations but to supplement and provide additional guidance. Passenger transit agencies and the vendor community now evolve their security requirements and system security features independently for most of the systems listed above. The purpose of this *Recommended Practice* is to share transit agency best practices; to set a minimum requirement for control security within the transit industry; to provide a guideline of common security requirements for control and operations systems vendors; to adopt voluntary industry practices in control security in advance of, and in coordination with, government regulation; and to raise awareness of control security concerns and issues in the industry.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Control and Communications Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Chair, Joy Thompson

Vice-Chair, Ted Ellis

Secretary, John Moore

Facilitator, Dave Teumim

APTA Program Manager, Dave Hahn

John Moore
Neal Mondschein
Joy Thompson
Steve Thomas
Dan Hillman
Chris Heil
Leigh Weber
Ali Edraki

Ted Ellis
Ahmed Idrees
John Moore
Dave Teumim
Sheri Le
Bill Tsuei
Alesia Cain
Kevin Garben

John Weikel

Introduction

This introduction is not part of APTA SS-CCS-RP-004-16, "Securing Control and Communications Systems in Rail Transit Environments."

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Securing Control and Communications Systems in Rail Transit Environments, Part IIIb

1. Introduction

This *Recommended Practice* is Part IIIb in a series of documents. Part I, released in July 2010, addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. Part II presents Defense-In-Depth as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones, the Safety-Critical Security Zone (SCSZ) and the Fire/Life-Safety Security Zone (FLSZ). Part IIIa, released in early 2015, addresses attack modeling security analysis, while this document, Part IIIb, addresses protection of the Operationally Critical Security Zone (OCSZ).

1.1 Intent of the series

The intent of this document is to provide guidance to transit agencies on securing control and communications systems for their rail environments. This *Recommended Practice* spearheads an effort within APTA to extend cybersecurity best practices to the transit industry.

It represents the contribution of "leading-edge" information from transit agencies that already have a control security program, as well as recommendations from the U.S. Department of Homeland Security (DHS), the Transportation Security Administration (TSA), the National Institute of Standards and Technology (NIST), vendors who serve the transportation and IT communities, as well as thought leaders in cybersecurity. APTA intends for this *Recommended Practice* series to serve as a guide for transit agencies to develop a successful and comprehensive cybersecurity program.

This *Recommended Practice* is not intended to supplant existing safety or security standards and regulations. It instead provides an overview of the need for control and communications protection, and it fills in potential gaps in current standards and regulations.

1.2 Parts of the series

Due to the comprehensive amount of information to be conveyed, this *Recommended Practice* series is divided into multiple parts, shown in **Table 1**.

TABLE 1
List of *Recommended Practices*

Part I	Published July 2010	Elements, Organization and Risk Assessment/Management
Part II	Published 2013	Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones
Part IIIa	2015	Attack Modeling Security Analysis
Part IIIb	2016	Protecting the Operationally Critical Security Zone

This division of text material parallels the progression of recommended steps a transit agency would follow to develop and implement a control and communications security program.

1.2.1 Elements, organization and risk assessment/management

Part I addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program and establishes the stages in conducting risk assessment and managing risk.

1.2.2 Defining a security zone architecture and protecting the Safety-Critical Zone

Part II assumes that the agency has completed the risk assessment and risk management steps of Part I and covers how to define a security architecture for control and communications systems based on the Defense-in-Depth model. It also defines a minimum set of controls for the most critical zones, which are the safety-critical security zone. The primary application is intended to be for new rail projects or major upgrades rather than for retrofitting legacy systems. Preliminary suggestions and some references on how to approach legacy system retrofits for control security are given in Appendix B of this document.

1.2.3 Protecting the Operationally Critical Security Zone

The Operationally Critical Security Zone (OCSZ) is defined in Part II of this series. As can be seen in **Table 2**, it contains control and communications systems, such as traction power and non-life-safety critical SCADA systems, which are very important to the correct functioning of a rail transit system, such as transporting passengers, minimizing downtime and allowing the transit system to operate efficiently and economically. It is important that systems in this zone be protected from cyber-risks, risks to proper functioning of the transit system as well as direct and indirect risks to passengers, transit staff, and the public.

TABLE 2
Zone Names

Importance	Zone	Example System
Most Safety-Critical	Safety-Critical Security Zone (SCSZ)	Field signaling and interlocking
↕	Fire/Life-Safety Security Zone (FLSZ)	Fire detection/suppression
	Operationally Critical Security Zone	Traction power SCADA, Facilities Monitoring, Centralized Train Control
	Enterprise Zone	Fare systems, turnstiles, accounting systems, schedule systems
Most Public	External Zone	Communications with the Internet, business partners, vendors and others

For instance, a cyberattack upon a traction power SCADA system may cut traction power, stopping trains, but, unlike an attack on a SCSZ or FLSZ system, under normal circumstances it does not result in immediate threats to life safety.

> **NOTE:** Worker safety for traction power and electrical systems is achieved by use of lockout/tagout procedures, power down, and ground. System safety is achieved locally via protective and interlocking relays. For instance, traction power emergency cutoff and protective relaying are included in Figure 2 as FLSZ systems.

1.2.4 Use of attack modeling security analysis

Attack modeling, described in Part IIIa of this series, is a method for analyzing security in rail transit security zones. It uses the graphical technique of "attack trees" to diagram out and study how a system may be compromised, either accidently or by those with harmful intent. It is closely related to a "fault tree" analysis, which has been used in safety studies but does not include a provision for harmful intent.

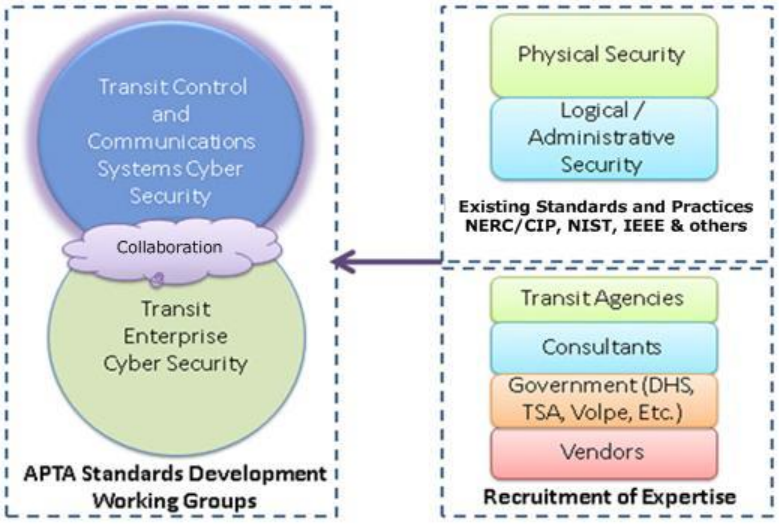
Attack modeling may be used to allay security concerns of transit agencies on new control and communications systems, or to evaluate the security implications of alternate design approaches. For other possible uses of attack modeling, please see Section 2.2 of Part IIIa.

1.2.5 APTA's approach

APTA has divided the cybersecurity effort into two teams (see **Figure 1**):

- The Enterprise Cybersecurity Working Group
- The Control and Communications Security Working Group (CCSWG)

FIGURE 1
The APTA Total Effort in Transportation Cybersecurity



1.2.5.1 Enterprise Cybersecurity Work Group

The Enterprise Cybersecurity Work Group develops APTA standards pertaining to mass transit cybersecurity. Specifically, it provides strategic recommendations for Chief Information Officers and decision makers regarding business cybersecurity, information systems, fare collection and general cybersecurity technologies.

1.2.5.2 Control and Communications Security Working Group

The Control and Communications Security Working Group (CCWSG) develops APTA standards for rail system control and communications security.

The CCSWG draws upon existing standards from the North American Electric Reliability Corporation's Critical Infrastructure Protection program (NERC-CIP), NIST, ISA, the Institute of Electrical and Electronics Engineers (IEEE), physical security knowledge, and logical/administrative security. Additional subject matter experts (SMEs) from transit agencies, transit vendors, government departments, (e.g., DHS, TSA, the John A. Volpe National Transportation Systems Center [Volpe-DOT]), and consulting organizations participated in defining and reviewing this *Recommended Practice*.

2. Cybersecurity approach

2.1 Introduction

Cybersecurity, for the purposes of this document, is defined as the means to reduce the likelihood of success and severity of impact of a cyberattack against transportation sector control systems through risk-mitigation activities.

2.1.1 Protection philosophy

Even with unlimited resources, it would not make sense to protect all things at the same level. The question becomes how best to prioritize a transit agency's protection method.

For rail, the most critical systems to protect are those that involve the highest risk to life and property: such as the control and communication systems that let the train or train operator start, control the speed of or stop the train. In addition, transit agencies need to ensure that trains run on their prescribed paths and that all crossings are properly controlled and protected.

Rail systems have many levels of safety built into them via redundant circuits, fail-safe control systems (vital logic) and other mitigations. The role of cybersecurity is to ensure that these existing systems cannot be duped into making a wrong decision, and to ensure that these systems cannot be directly controlled by anyone other than their owner/operator. Another goal is to reduce the likelihood of human error, such as forgetting to apply an update or applying an incorrect update to a part of the system.

The following are the key parts of security protection:

- **Prevention, and reducing likelihood of human error:** Keep anyone or anything from tampering with the system.
- **Tamper detection:** Detect when an unauthorized change has been or is being made.
- **Auditable:** If someone does tamper with the system, determine who, what, where, when and how. Ensure that appropriate personnel are notified of abnormal or unauthorized activity and can respond in a timely manner.

2.1.2 Cybersecurity risk zones for rail transit

Table 3 and **Table 4** provide two generic models of control and communications security zones. If a particular transit agency has a unique set of requirements and wishes to define control and communications security zones differently, then a thorough risk assessment considering these unique requirements and resultant zones should be conducted. An example would be for a full communications-based train control (CBTC) system.

Cyber-protection of the next two zones is addressed by the APTA Enterprise Cybersecurity Work Group.

TABLE 3
List of Zones (APTA Enterprise Cybersecurity Work Group)

External Zone	The external zone includes Internet-accessible services, remote operations and facilities, and remote business partners and vendors. It is *not* trusted.
Enterprise Zone	The enterprise zone, or corporate zone, includes, where applicable, hardware and services that are made available to the control system via the agency's corporate network and includes agency business systems, fare collection systems, email, VPN, central authentication services, etc.

Cyber-protection of the following three zones is addressed by the APTA Control and Communication Security Working Group.

TABLE 4
List of Zones (APTA Control and Communications Security Working Group)

Operationally Critical Security Zone (OCSZ)	The control center zone includes the centralized supervisory control and data acquisition (SCADA), train control, transit passenger information system and other centralized control hardware and software, and the equipment from these control center zones, extending out to remote facilities such as train stations and trackside equipment.
Fire/Life-Safety Security Zone (FLSZ)	See Section 2.1.3. of Part II
Safety-Critical Security Zone (SCSZ)	See Section 2.1.3. of Part II

2.1.3 How were the zones derived and defined?

The working group performed a high-level generic risk assessment of the example system, determining which systems are most critical to the operation. The group also looked at the people within the organization who are responsible for maintaining and operating the systems. The fare collection people, for example, should not be able to change the behavior of the signaling and switching control system. Likewise, the signaling people should not be able to change the fare system. Separation of duties should be in place for each part of the organization, ensuring that business, accounting and engineering controls (checks and balances) are in place.

There is a separation of access and a separation of authority between these zones. An important part of an effective cybersecurity program is to give the right people access to the right places and to give them exactly the privilege they need to perform their primary jobs.

The SCSZ contains any system that if "hacked" and modified would cause an immediate threat to life or safety — for instance cause a collision or derail a train. Examples:

- vital signaling
- interlocking
- automatic train protection (ATP)

The FLSZ contains any system whose primary function is to warn, protect or inform in an emergency. Examples:

- emergency management panel
- emergency ventilation systems
- fire detection and suppression systems

- gas detection systems
- seismic detection

The OCSZ is defined in Part II of this series. It contains control and communications systems, such as traction power and non-life-safety-critical SCADA systems which are very important to the correct functioning of a rail transit system, such as transporting passengers, minimizing downtime and allowing the transit system to operate efficiently and economically. It is important that systems in this zone be protected from cyber-risks, risks to proper functioning of the transit system as well as direct and indirect risks to passengers, transit staff, and the public.

Examples of OCSZ systems would be:

- Traction power
- Passenger Information Display
- Dispatch/ATS System

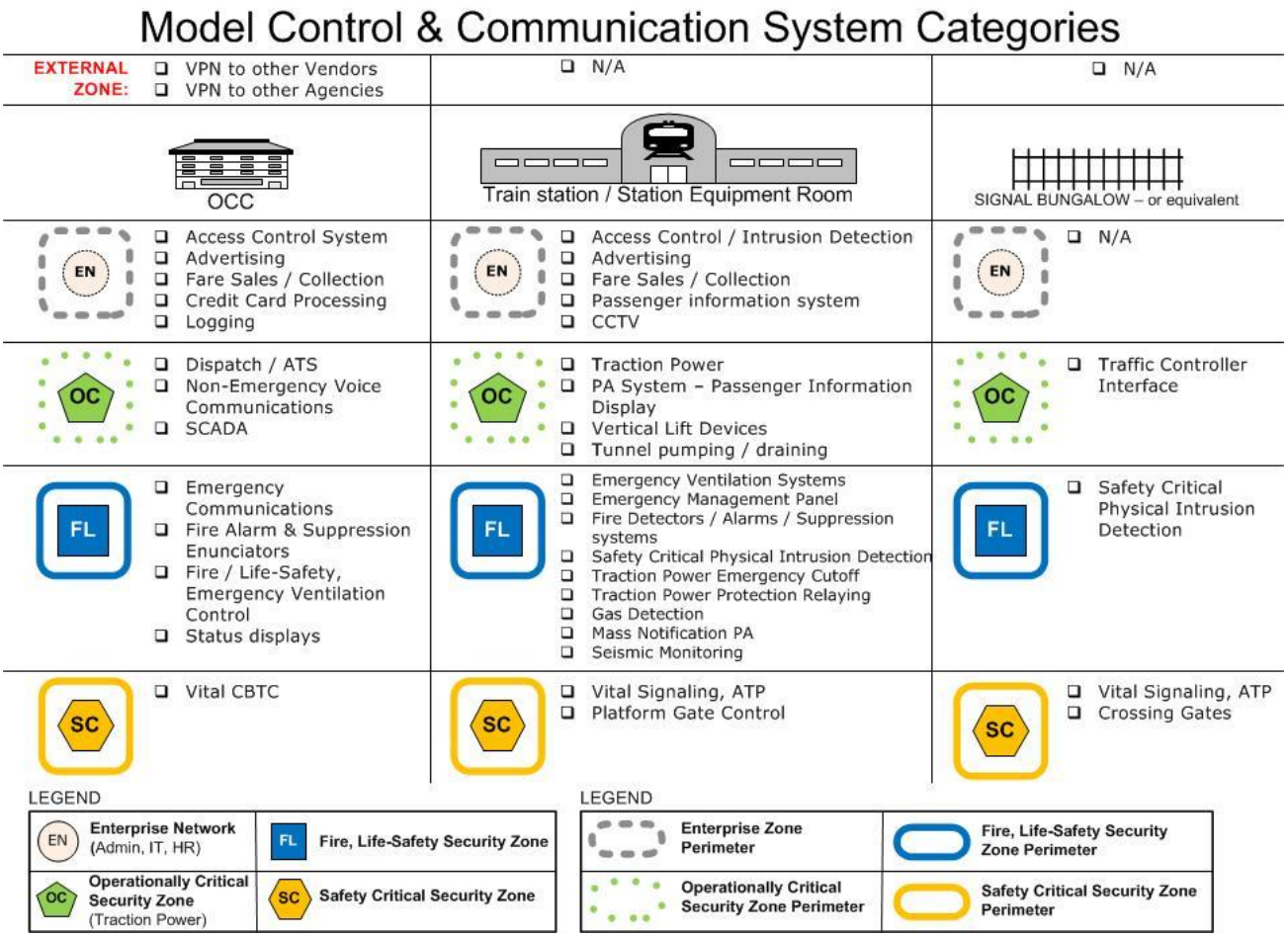
For instance, a cyberattack upon a traction power SCADA system may cut traction power, stopping trains, but unlike an attack on a SCSZ or FLSZ system, under normal circumstances it will not result in immediate threats to life safety.

Additional examples:

- A cyberattack upon a platform Passenger information display board (PID) or PA system could confuse passengers with the wrong information, and have them get on the wrong train, or miss their train.
- A cyberattack upon pumping and drainage devices could stop them from working, flooding susceptible areas, and causing equipment or wiring damage from water buildup.

Figure 2, taken from Part II, gives a detailed look at the allocation of systems to these security zones across physical locations.

FIGURE 2
Model Zone Chart for Transit Systems



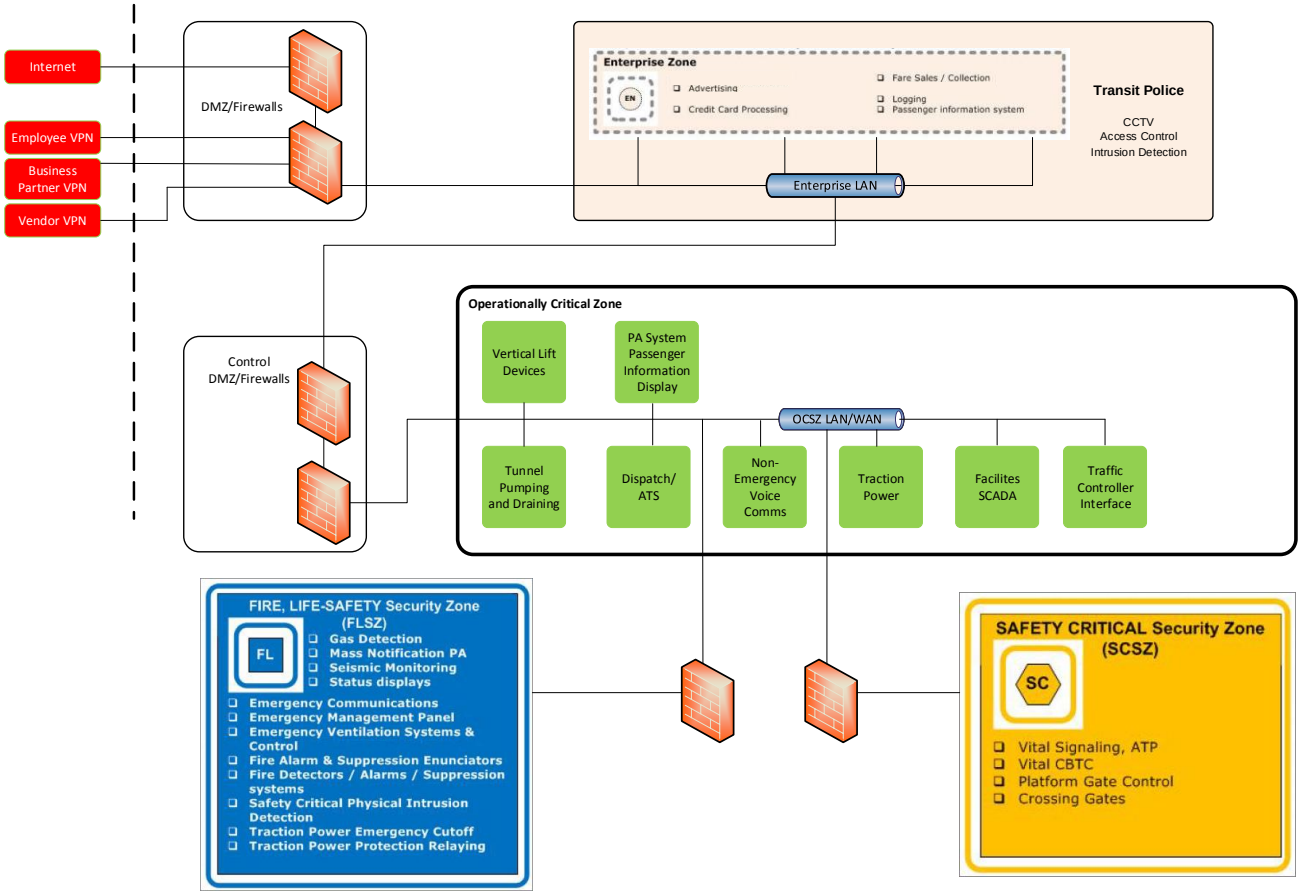
In the next section, the work of Part II will be expanded to add detail on how the OCSZ and Enterprise Zones are included in the overall architecture of a transit agency. DMZs (Demilitarized Zones) are added to provide additional zones of protection and segregation, and further protection between the OCSZ and the Enterprise Zone.

2.1.4 Network architecture to show boundaries and interfaces between OCSZ and Enterprise Zones, and External Zones

Figure 3 illustrates the information shown in **Figure 2**, with added detail on the interface between the OCSZ and the Enterprise Zone, and the Enterprise Zone and the External Zone (to the Internet and business partners).

NOTE: DMZ details for the OCSZ to Enterprise Zone are shown in **Figure 4**.

FIGURE 3
Transit Agency Network Architecture



2.1.5 Explanation and additional details on the drawing

- **Figure 3** represents each system in the OCSZ zone (e.g., traction power) as a separate entity (represented by a green rectangle), which may or may not connect to the OCSZ LAN/WAN depending on if it has connections to other OCSZ systems.
- It separates the OCSZ Zone from the Enterprise Zone by a Demilitarized Zone (DMZ), which is figuratively shown by two firewalls.
- Shows the "External Zone (briefly indicated in **Figure 2** above connection to these previously mentioned DMZ firewalls in red), showing recommendations for Vendor VPN access and Employee VPN access.

  NOTE: VPN access from outside directly into either safety-critical security zone (FLSZ of SCSZ) or the OCSZ is not recommended.

- Even though the CCSWG is not directly involved in the Enterprise Zone or Enterprise Zone External Architecture, the figure suggests a separate DMZ firewall and external zone setup for the Enterprise Zone, with connections to the Internet and business employee VPN (as opposed to control engineer and control system vendor external VPNs into the OCSZ zone).

2.1.6 Explanation of the function and configuration of a DMZ

The computer networking usage of the DMZ concept evolved from the military term "demilitarized zone." In military usage, this refers to the "no man's land" between opposing forces, a neutral zone or buffer that gives each side advance warning if the other side crosses into this zone as a prelude to an attack.

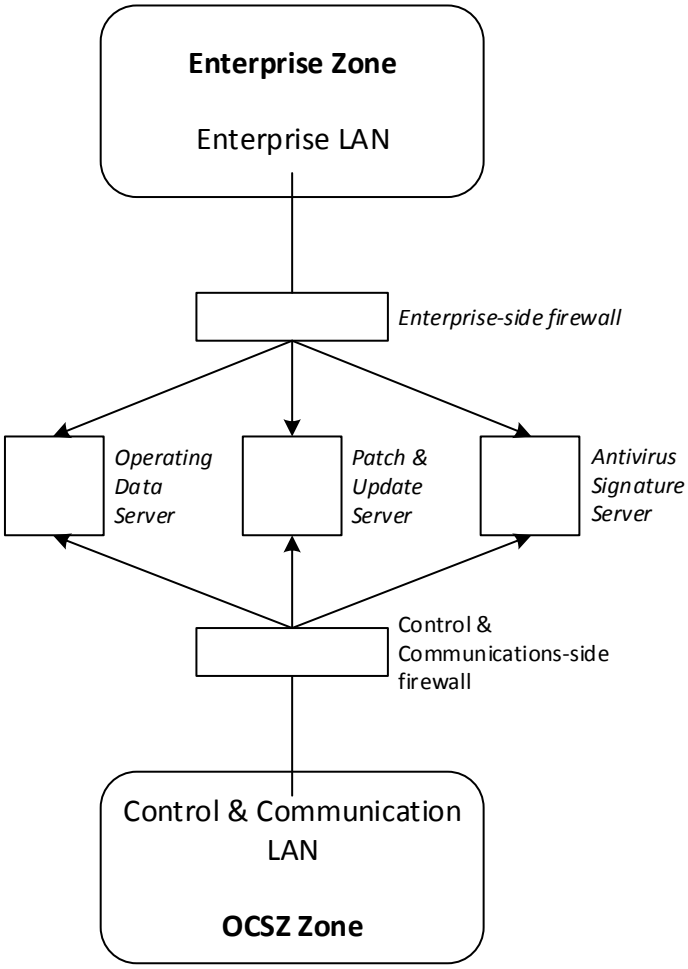
It has been adopted into the IT cybersecurity and control and communications security language as an intermediate security zone between a trusted zone (say an internal business LAN) and a hostile zone (for instance the open Internet).

Historically, a very primitive DMZ might contain a special server between two firewalls separating the opposing zones. It would separate and desynchronize in time the "read" and "write" functions of one zone to another. On this server, one zone would have write-only privileges to the server to upload data meant for the second zone. Then a separate read function, with no logical connection to the write routine, would upload this information to the second zone. The write and read software programs would be independent, and would act independently on the data deposited in storage to be transmitted.

A model of a present-day DMZ to separate the OCSZ zone from the Enterprise zone in a transit agency can be seen in **Figure 4**. Here the historical single data transfer server has "morphed" into separate servers for different data, such as historian, operating data and antivirus signature updates. Note that it is sometimes the practice for the Enterprise IT group to operate "their upper firewall," while the control and communications engineers operate "their lower firewall," perhaps with customized rulesets. What is important, if different organizational groups operate "their firewalls," is that both groups fully communicate and synchronize on the rulesets and configuration of the infrastructure.

The main point to observe is that there is no straight-through connection from firewall to firewall across the DMZ, using the same protocol. It is desirable for different protocols to be used to supply and retrieve data. For instance, operating data may be placed on the "operating data server" using FTP, and might be retrieved by Enterprise through a Web interface using HTTP or HTTPS.

FIGURE 4
Sample DMZ Diagram



A separate authentication server may be employed with the DMZ so as to validate employee remote or vendor connections coming through the Enterprise Zone to the OCSZ. VPN connections using IPSec or SSL are frequently included in the firewall internals in today's products on the market.

The following section provides the NIST 800-82 Part 2 final draft (2015) commentary on DMZs. It illustrates the APTA concept (described above) of placing info transfer servers, like operating data servers, patch servers, etc, into the DMZ, as a separate small independent zone between two firewalls.

2.1.6.1 NIST 800-82 section on DMZs

By placing corporate-accessible components in the DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the DMZ. Most firewalls can allow for multiple DMZs and can specify what type of traffic may be forwarded between zones. As [the NIST figure in the original document] shows, the firewall can block arbitrary packets from the corporate network from entering the control network and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, a clear separation can be maintained between the control network and other networks, with little or no traffic passing directly between the corporate and control networks.

If a patch management server, an antivirus server or other security server is to be used for the control network, it should be located directly on the DMZ. Both functions could reside on a single server. Having patch management and antivirus management dedicated to the control network allows for controlled and secure updates that can be tailored for the unique needs of the [Industrial Control System] ICS environment.

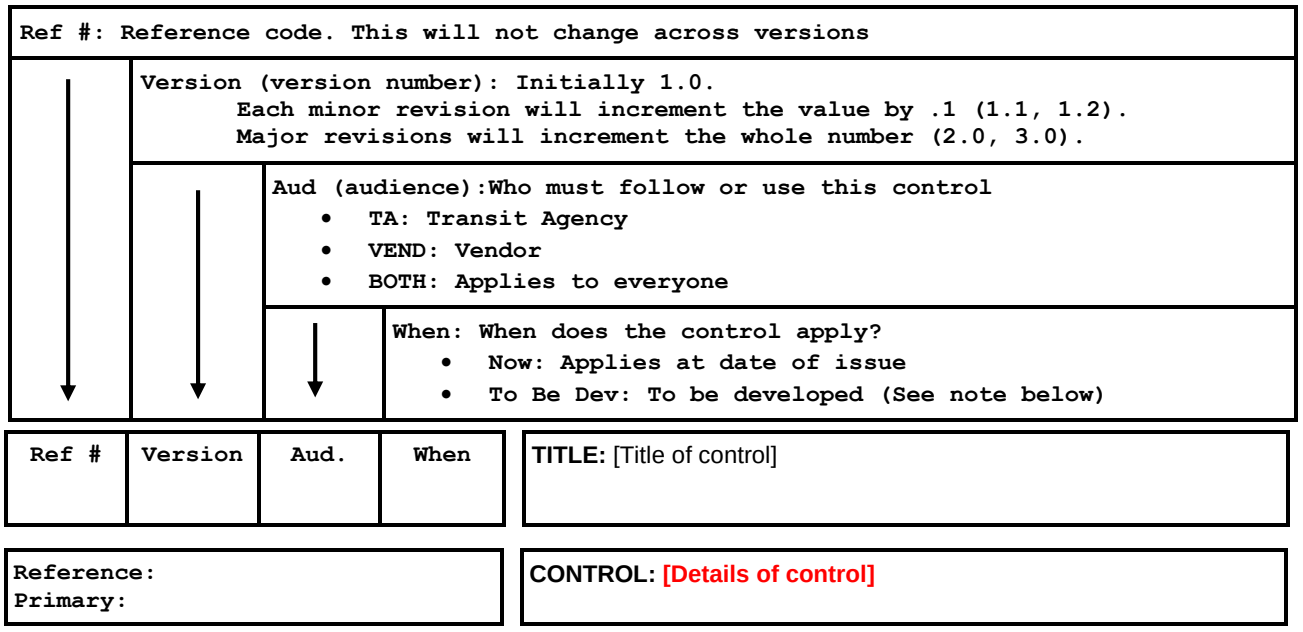
The primary security risk in this type of architecture is that if a computer in the DMZ is compromised, then it can be used to launch an attack against the control network via application traffic permitted from the DMZ to the control network. This risk can be greatly reduced if a concerted effort is made to harden and actively patch the servers in the DMZ and if the firewall ruleset permits only connections between the control network and DMZ that are initiated by control network devices. Other concerns with this architecture are the added complexity and the potential increased cost of firewalls with several ports. For more critical systems, however, the improved security should more than offset these disadvantages.

3. System security and minimum controls for OCSZ

3.1 Legend

The following pages expand and explain the recommended controls. Each section has this format. **Figure 5** explains the meaning of the headings.

FIGURE 5
Recommended Controls Legend



Notes:

- The "To be developed" designation for a security control indicates that the security control text is generally informative but not prescriptive, and that it will be developed further after Part IIIb is issued. It will be fully developed and then included in a future revision of Part IIIb. It is included in this document so the rail transit industry may start thinking about how this control could be developed.

- Transit agencies and vendors should keep adequate system documentation, including system drawings with description of security zones, electronic security perimeters and how the security controls in this document are being met as records for security auditing and assessment.

3.2 Overview

To partition the system according to the rules of the previous section, the security controls in **Table 5** should be applied.

TABLE 5
Overall Controls

Ref.	Applies to	Description	References and Citations	When to Apply
A	Both	The transit agency should draw electronic security perimeters around the OCSZ to separate it from the FLSZ and SCSZ, and from the Enterprise zone.	NIST 800 -18, 53, 82	Now
B	Both	All network-routable interfaces connecting the OCSZ to the SCSZ or FLSZ should use an isolation device (defined below) to ensure security separation.		Now
C	Both	The OCSZ should be separated from the Enterprise Zone using a DMZ, as shown in **Figure 3**. Connections to external authorized parties (Vendors and Transit agency control engineers working remotely) should be made through the DMZ from the Enterprise using VPN connections as described below.		Now

3.3 Electronic security perimeters around OCSZ

Ref #	Version	Aud.	When
A	1.0	TA	Now

TITLE: Electronic security perimeter around the OCSZ

Reference: SP 800-53
Primary:

CONTROL: **The transit agency should draw electronic security perimeters around the OCSZ to separate it from the SCSZ, FLSZ, and other zones**

3.3.1 Reason for control

Following the Defense-in-Depth strategy introduced in **Part II**, higher security zones need to be behind perimeters in order to segregate them from lower-security zones.

3.3.2 Discussion

The following definition will serve to illustrate the systems included in the OCSZ classification:

> It contains control and communications systems, such as traction power and non-life-safety-critical SCADA systems, which are very important to the correct functioning of a rail transit system, such as transporting passengers, minimizing downtime and allowing the transit system to operate efficiently and economically. It is important that systems in this zone be protected from cyber-risks, which threaten the proper functioning of the transit system.

3.3.3 Measures of effectiveness

Audit of systems during design, implementation and operational phases would show proper categorization of OCSZ equipment and the proper definition of the electronic security perimeters around the OCSZ.

3.3.4 Examples

- **Acceptable:** The OCSZ perimeter is clearly defined.
- **Not acceptable:** The OCSZ perimeter has not been defined.

3.4 Connecting security zones of different security levels

Ref #	Version	Aud.	When
B	1.0	TA	Now

TITLE: Connecting security zones of different security levels

Reference: SP 800-53
Primary:

CONTROL: **All network-routable interfaces connecting the OCSZ to the SCSZ or FLSZ should use an isolation device (defined below) to ensure security separation.**

3.4.1 Reason for control

The Defense-in-Depth strategy used in this *Recommended Practice* requires routable (TCP/IP based) network connections through a device which allows authorized traffic and to prohibit unauthorized traffic between the SCSZ and FLSZ and the OCSZ.

3.4.2 Discussion

An isolation device may be a hardware-based firewall to filter traffic at TCP/IP stack layers 2, 3 and 4 (corresponding to link layer, IP layer and TCP layer). If technology is available, filtering at the application layer is also desirable.

3.4.3 Measures of effectiveness

Unauthorized network traffic is recognized and stopped at the isolation device.

3.4.4 Examples

- **Acceptable:** Hardware-based firewall as described above.
- **Not acceptable:** Using a dual-homed personal computer (e.g. dual NIC cards) to connect to a SCSZ or FLSZ network and also a lesser security zone.

3.5 Physical and logical separation for OCSZ data transmission

Ref #	Version	Aud.	When
C	1.0	TA	Now

TITLE: Separation of the OCSZ from the Enterprise Zone using a DMZ

Reference: SP 800-53
Primary:

CONTROL: **Separate the OCSZ from the Enterprise Zone with a DMZ, as defined below and in the text Section 2.1.6. Connections to external authorized parties (vendors and transit agency control engineers working remotely) should be made through the Enterprise zone and then through the Enterprise to OCSZ DMZ**

3.5.1 Reason for control

To provide physical and logical separation for OCSZ data heading to the Enterprise Zone, and enterprise data heading to the OCSZ.

3.5.2 Discussion

The rationale using a DMZ to separate different zones has been described in Section 2.1.6.

The main point to observe is that there is no straight-through connection from firewall to firewall across the DMZ, using the same protocol. It is desirable for different protocols to be used to supply and retrieve data. For example, operating data may be placed on the "Operating Data Server" using FTP, and might be retrieved by enterprise through a Web interface using HTTP or HTTPS.

Connections to external authorized parties originally connecting into the Enterprise Zone DMZ, such as offsite remote workers or vendors, may be made through VPN provisions in the OCSZ DMZ firewalls, using secure VPN protocols, such as IPSec and SSL, and using suitable authentication.

3.5.3 Measures of effectiveness

A DMZ exists to perform physical and logical separation of the OCSZ to Enterprise zone data path.

3.5.4 Examples

- **Acceptable:** A DMZ zone exists to provide the above separation.
- **Not acceptable:** A DMZ does not exist. A single firewall is used, or nothing separates the OCSZ and Enterprise zones.

3.6 Security controls

Table 6 gives security controls applicable within the OCSZ Electronic Security Perimeters. Each control then has a dedicated section following the table.

Before implementing any cybersecurity controls, a thorough analysis must be performed to ensure that the controls cannot adversely impact any other necessary operational, reliability or safety functions implemented in the OCSZ.

TABLE 6
Controls

Ref.	Applies to	Description	References and Citations (NIST SP 800-53 Appendix F)		NIST SP 800 Family	When to Apply
1	Transit	A senior executive should be identified to be responsible and accountable for all control and communications security activities.	CA-6		Security Assessment and Authorization	Now
2	Transit	Create a training program for employees, vendors and partners around control and communications security.	AT-1		Awareness and Training	Now
3	Transit	Have methods and procedures in place to create, modify and remove access to OCSZ equipment for people (employees, contractors, vendors and inspectors) as their role in the organization changes, including hire/fire or contract awarded/ expired/terminated.	PS-4	PS-5 AC-6	Personnel Security	Now
4	Transit	OCSZ electronic equipment should be housed in a six-wall physical enclosure with one-factor authentication to access and warn on unauthorized physical access.	PE-1	PE-2; PE-3; PE-6	Physical and Environmental Protection	Now
5	Transit	Centralized or distributed configuration management system, manual or software based, should be used for software, executables and configuration files for each OCSZ device.	CM-1	CM-2	Configuration Management	Now
6	Transit	A process should exist to manage the changes to all OCSZ hardware and software with logs of the changes, including the purpose/rationale for the changes.	CM-3	CM-8; CM-9	Configuration Management	Now
7	Transit	Procurement documents to specify default hardening specification for OCSZ equipment, closing non-essential ports and services.	SA-1	SA-4	System and Services Acquisition	Now
8	Transit	Block any unneeded USB, CD and other entry ports on OCSZ devices and equipment. Single-factor cyber-authentication should be used on permitted ports.	SC-41	CM-7	System and Information Integrity; Configuration Management	Now
9	Transit	Sweep for rogue wired or wireless devices attached to OCSZ control/communications networks, every other month.	AC-18	SI-4	Access Control; System and Information Integrity	Now
10	Transit	Every other month check OCSZ computers, network devices and other devices that use software for software that is unauthorized or questionable.	AU-12	CM-7	Audit and Accountability; Configuration Management	Now
11	Transit	Use antivirus protection or software white-listing/ file integrity checker on fixed/portable/mobile PCs that connect to OCSZ equipment.	SI-3	SI-7	System and Information Integrity; System and Communications Protection	Now
12	Transit	The cybersecurity process should ensure that the backup/alternate OCC cannot be used as a route for sabotage or covert monitoring of activities.	CP-4		Contingency Planning	Now

TABLE 6
Controls

Ref.	Applies to	Description	References and Citations (NIST SP 800-53 Appendix F)		NIST SP 800 Family	When to Apply
13	Both	A comprehensive patch management program should be set up with vendors for OCSZ commercial off-the-shelf (COTS) or proprietary software and firmware	SI-2		System and Information Integrity	Now
14	Transit	Yearly passive vulnerability check should be performed by an authorized and qualified outside agency.	CA-2		Security Assessments	Now
15	Both	On-site physical presence by qualified and authorized staff should be required to change software or executables on OCSZ equipment. As an alternative, where software or executables are changed over an internal network, a cybersecurity change management procedure with verification and security checks should be implemented.	AC-17	MA-4	Access Control; Non-Local Maintenance	Now
16	Both	Method to collect and audit logs to meet the requirements of NIST SP 800-53, and SP 800-82. (to be developed)	AU-1	AU-2; AU-3; AU-4; AU-5; AU-6; AU-7 AU-8	Audit and Accountability	To Be Dev
17	Vendor	A vendor manager should be identified to be responsible and accountable for all control and communications security activities for each OCSZ product used by transit.	SA-4		Acquisition Process	Now
18	Vendor	Wireless security within the OCSZ used for monitoring only may use IEEE 802.11x (or other encrypted wireless protocols) with latest encryption technology (Currently WPA2). Wireless used for both monitoring and control should use a current VPN technology such as IPSEC or SSL to tunnel within the 802.11x, or other encrypted wireless protocols to give a similar level of additional protection as a VPN would give. (Example - ISA 100 standard)	SC-40	AC-18	System and Communications Protection; Wireless Link Security	Now
19	Vendor	Use host file integrity verification with cryptographic checksum on OCSZ controllers such as PLCs, where not precluded by large or complex file structures.	SI-7		System and Information Integrity	Now
20	Transit	A control and communications security incident response plan should be developed to handle security incidents (Including ICS-CERT as a resource)	IR-1(2 – 4)		Incident Response	Now
21	Vendor	Software and firmware coding review should be instituted by vendors on new code (for obvious flaws such as buffer overflows, etc.)	SI-2		Flaw Remediation	Now

TABLE 6
Controls

Ref.	Applies to	Description	References and Citations (NIST SP 800-53 Appendix F)	NIST SP 800 Family	When to Apply
22	Transit	Transit agency should change manufacturer default login credentials, such as for administrator or management access, upon installation of new equipment	CM-2 AC-2	Access Control	Now

3.6.1 Management responsibility

Ref #	Version	Aud.	When
1	1.0	TA	Now

TITLE: Management responsibility

Reference: SP 800-53
Primary: CA-6
CA-2, CA-7, PM-9, PM-10

CONTROL: A senior executive should be identified to be responsible and accountable for all control and communications security activities.

3.6.1.1 Reason for control

Security needs to have visibility to be successful. Security is more likely to be taken seriously when a senior executive is responsible and accountable in measureable ways that impact his or her job review and compensation.

3.6.1.2 Discussion

The senior executive is the official management person who authorizes operation of the OCSZ systems and explicitly accepts the risk (to the organizational operations and assets, individuals and other organizations) on the implementation of an agreed-upon set of security controls.

The authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such OCSZ system security risks.

The senior executive is encouraged to establish a continuous monitoring process so that changes to the system can be evaluated while still confirming the entire system as secure.

3.6.1.3 Measures of effectiveness

- A job description exists that defines this responsibility for a senior executive, with a feedback mechanism that helps evaluate satisfactory performance.
- The board of directors or similar body has charged the executive team with ensuring that control and communications security is a key part of their mission.

3.6.1.4 Examples

- **Acceptable:** Written documentation that defines senior executive responsibility and accountability for control and communication security activities.
- **Not acceptable:** No senior executive responsibility, or formal documentation describing the above.

3.6.2 Training program

Ref #	Version	Aud.	When
2	1.0	TA	Now

TITLE: Training program

Reference: SP 800-53
Primary: AT-1
PM-9

CONTROL: **Create a training program for employees, vendors and partners around control and communications security.**

3.6.2.1 Reason for control

Control and communications security is most effective when everyone is included and made aware of the threats. A training program must touch everyone in an appropriate manner to keep everyone vigilant.

3.6.2.2 Discussion

Control and communications security awareness and training procedures should be developed for the transit control and communications security program in general and for the OCSZ in particular.

The training program is for all employees, contractors and vendors who either work on-site or remotely access transit agency systems or devices.

3.6.2.3 Measures of effectiveness

- A training program exists that covers control and communications security for personnel who operate OCSZ equipment and/or physically access the OCSZ. The training is mandatory.
- Training is delivered as needed, if possible, just in time for an activity that is about to take place. For example, retrain a person about password quality when he or she is about to change passwords.

3.6.2.4 Examples

- **Acceptable:** Instructor-led or computer-based training at appropriate intervals, with testing for retention.
- **Not acceptable:** Simply giving personnel a training packet and requesting that they read it, with no follow-up.

3.6.3 Access control, personnel

Ref #	Version	Aud.	When
3	1.0	TA	Now

TITLE: Access control, personnel

Reference: SP 800-53
Primary: PS-4

CONTROL: **Have methods and procedures in place to create, modify and remove access to the OCSZ for people (employees, contractors, vendors, and inspectors) as their role in the organization changes, including hire/fire or contract awarded/expired/terminated.**

3.6.3.1 Reason for control

There is a need to ensure that only authorized people have access to systems they require for their jobs, and that access is removed when no longer needed.

3.6.3.2 Discussion

People need access to those systems that they are directly responsible for. Clear roles and responsibility need to be established, and access should be given only to those with a direct need for it.

Attention should be paid to the end of contracts and to termination of employees to ensure that access is removed immediately. When a person's responsibilities are changed (job change, promotion, duty change) he or she needs to have the former access removed and the new access added.

3.6.3.3 Measures of effectiveness

- An employee and contractor start/stop process is in place.
- Each person's roles and responsibilities are defined to provide access to the appropriate software and physical areas.
- An internal service level exists that these changes must be made within the shortest timeframe possible of the person being terminated for cause or put on leave.
- A similar process exists for the start and end of contractual relationships.

3.6.3.4 Examples

- **Acceptable:** Written procedures describing the above existing access control system process.
- **Not acceptable:** Informal or no procedures for access control as described above.

3.6.4 Access control, equipment

Ref #	Version	Aud.	When
4	1.0	TA	Now

TITLE: Access control, equipment

Reference: SP 800-53
Primary: PE-1
PM-9

CONTROL: **OCSZ electronic equipment should be housed in six-sided physical enclosure with one-factor authentication to access, and should warn on unauthorized physical access.**

3.6.4.1 Reason for control

This control is intended to ensure that the physical access to OCSZ equipment is restricted to those with proper authorization. A six-sided enclosure means that there is security from all four sides, the top and the bottom.

3.6.4.2 Discussion

One-factor authentication is an acceptable means of identity assurance in security situations that require personnel to provide one of three factors: something they know (e.g., password/passcode), something they have (e.g., RFID badge) or something they are (e.g., biometrics, fingerprints and retina).

3.6.4.3 Measures of effectiveness

- Security audit

3.6.4.4 Examples

- **Acceptable:** Locked room with all entrances, floor and ceiling secured; a locked equipment cage that has six sides; secure room must comply with all applicable building codes to ensure the safety of personnel.
- **Not acceptable:** Simply posting a "Do Not Enter" sign on an unlocked door.

3.6.5 Configuration management

Ref #	Version	Aud.	When
5	1.0	TA	Now

TITLE: Configuration management

Reference: SP 800-53
Primary: CM-1
CM-2 PM-9

CONTROL: **Centralized or distributed configuration management system, manual or software based, should be used for software, executables and configuration files for each OCSZ device.**

3.6.5.1 Reason for control

A transit agency needs to know the versions of software that are currently running and whether they are up to date. An audit would reveal if the versions are up to date, and if they are not, during which time periods the software was at risk.

3.6.5.2 Discussion

First, there needs to be a way to identify the version(s) of software and firmware that work together (and are tested together) to provide safe operation.

Second, there needs to be a method or process by which the transit agency ensures that compatible software versions are installed and running on all OCSZ devices.

Third, there needs to be a way to distribute and monitor the software configurations throughout the OCSZ zones of the transit system.

3.6.5.3 Measures of effectiveness

- An auditor can see a master list of all software and firmware authorized for any time period, showing compatibilities, incompatibilities and reasons.
- An auditor can see a diagram that explains where software and firmware originated, and how they are reviewed, controlled and ultimately installed in field equipment.
- There are controls in place to ensure that the authorized, unaltered software and configuration settings are verified as being in place in the field during an audit.
- A procedure exists for the auditor to reconcile differences found in the field verses a master configuration list.

3.6.5.4 Examples

- **Acceptable:** Written procedures describing a configuration management system.
- **Not acceptable:** Ad hoc handwritten lists of software compatibilities; no overall system exists, OCSZ filenames without a naming convention that positively identifies them, such as naming files “File1,” etc.

3.6.6 Configuration management, audit trail

Ref #	Version	Aud.	When
6	1.0	TA	Now

TITLE: Configuration management, audit trail

Reference: SP 800-53
Primary: CM-3
CM-8 CM-9
CM-1 CM-4 CM-5 CM-6 SI-2

CONTROL: A process should exist to manage the changes to all OCSZ hardware and software with logs of the changes, including the purpose/rationale for the changes.

3.6.6.1 Reason for control

In complex systems, it would be nearly impossible to manage the changes in a coherent and safe manner without a proven process.

Configuration management helps to update hardware and software across changes in a controlled and coordinated manner. It is important that logs exist to document what was done and any important equipment history along with it, such as why the change was made and who authorized it.

3.6.6.2 Discussion

The configuration management process should coordinate the proposal, justification implementation, test and evaluation of upgrades, and modifications before putting them into effect in OCSZ systems, and its control and communication paths. It is simply not acceptable to put a patch into the field before knowing that a OCSZ system will continue to function as required.

Configuration change control includes changes to components of the OCSZ system, changes to the configuration settings for software and hardware products (e.g., operating systems, applications, firewalls, routers, wireless devices and HMI), emergency changes and changes to remediate flaws.

A typical change management process has a change approval process and a chain of custody.

3.6.6.3 Measures of effectiveness

- An audit can determine when the system had all proper versions of software working together.
- An audit can quickly identify when the software on any network device is at the approved level.
- An audit can quickly identify when a network device's software is *not* at the approved level.

3.6.6.4 Examples

- **Acceptable:** A documented change management procedure.
- **Not acceptable:** An ad-hoc or no change management system exists

3.6.7 Security in procurement

Ref #	Version	Aud.	When
7	1.0	TA	Now

TITLE: Security in procurement

Reference: SP 800-53
Primary: SA-1 SA-4
PM-9

CONTROL: **Procurement documents to specify default hardening specification for OCSZ equipment, closing non-essential ports and services.**

3.6.7.1 Reason for control

OCSZ control and communications equipment is best delivered from the vendor with security pre-configured, at delivery. Transit agency purchasing needs a procurement process that includes language that will ensure that.

3.6.7.2 Discussion

Transit agency procurement documents should include requirements for vendors to:

- supply OCSZ equipment hardened, including the closing of non-essential ports and services; or
- if providing hardened equipment is not possible in certain instances, provide detailed documentation and procedures to perform it.

The intent is to reduce the ways that a device or system may be compromised on purpose or by accident.

Proper procurement may also reduce the risks associated in configuration and patch management, because unnecessary services will not be accidentally overlooked or not maintained. DHS's "Cybersecurity Procurement Language for Control Systems" as revised (Revision 4, September, 2009) may be used as a reference.

One effective way to do this, that has already been used successfully by one transit agency, is to append the whole DHS Procurement document per above as an attachment, along with a customized table showing which exact requirements from the document are being listed as purchase requirements for the present project.

3.6.7.3 Measures of effectiveness

- Audit of "as-received" OCSZ equipment.

3.6.7.4 Examples

- **Acceptable:** Adding a procurement security specification to RFP and purchase agreements.
- **Not acceptable:** No procedure exists, leaving unnecessary ports and services activated as a default configuration.

3.6.8 Physical security, attachments

Ref #	Version	Aud.	When
8	1.0	TA	Now

TITLE: Physical security, attachments

Reference: SP 800-53
Primary: SI-3 CM-7
SA-4 SA-8 SA-12 SA-13
SI-1 SI-4 SI-7

CONTROL: **Block any unneeded USB, CD and other entry ports on OCSZ devices and equipment. Single-factor cyber-authentication should be used on permitted ports.**

3.6.8.1 Reason for control

A transit agency needs to prevent unauthorized connections to OCSZ equipment. Attackers infect removable media such as USB drives, CDs and other devices in the hope that an unsuspecting person will connect them to the systems. Other attack methods include connecting unauthorized devices to the systems or network.

If someone does connect an authorized device to the system, it should insist on some single-factor type of authentication (such as a password) before accepting the connection. If antivirus is available on the OCSZ equipment, it should be configured to scan authorized mobile devices.

3.6.8.2 Discussion

Security attacks are often done by connecting an infected device to a secure device or network. To prevent the attachment of unauthorized devices, eliminate the ability to attach the device if that port not needed for operational activity. In the case where a device must legitimately be connected, the person connecting the device should be required to authenticate to the system to authorize the connection. In cases where mobile media is necessary for proper operations, due attention should be placed on device control mechanisms, mobile access control mechanisms and device encryption.

3.6.8.3 Measures of effectiveness

- Devices or physical protections are used to block unused ports and connectors in routers, switches, network devices and computers.
- Logical means are used to disable legitimate connection points without proper authentication.
- When a port is active, any connection attempt leads to a one-factor authentication.

3.6.8.4 Examples

- **Acceptable:** Unneeded ports are blocked.
- **Not acceptable:** Ports are left open.

3.6.9 Unauthorized devices, detection

Ref #	Version	Aud.	When
9	1.0	TA	Now

TITLE: Unauthorized devices, detection

Reference: SP 800-53
Primary: AC-18 SI-4
AC-3 AC-18 IA-2 IA-3 IA-8 SI-4

CONTROL: **sweep every other month for rogue wired or wireless devices attached to OCSZ control/communications networks.**

3.6.9.1 Reason for control

A transit agency needs to know if an unauthorized device is eavesdropping or intruding on its network. It should do this by regularly analyzing the network for such devices.

3.6.9.2 Discussion

Transit agencies want to prevent unauthorized collection of information from their systems. They also want to detect and remove devices that may masquerade as legitimate devices and may take control of part or their entire network. Devices are small and can be powered by battery, so it may be very difficult to find a device that is eavesdropping on your wireless telecommunications. Rogue devices may also be connected directly to your network.

A scan every other month of the network for detection of rogue devices not only prevents changes to the system that have not been authorized or tested, but also ensures that access points to your network are not bypassing access-control mechanisms put in place to protect the system.

> **CAUTION:** The method used to scan or sweep the network must be proved not to have a negative operational impact on the system.

3.6.9.3 Measures of effectiveness

- There is a scheduled review of devices connected to the network.
- The transit agency has a definition of what an authorized device is.

3.6.9.4 Examples

- **Acceptable:** A check for unauthorized devices is done, considering possible negative responses of the control network to the scan or sweep method used.
- **Not acceptable:** No sweep is done.

3.6.9.5 Unauthorized software, compliance

Ref #	Version	Aud.	When
10	1.0	TA	Now

TITLE: Unauthorized software, compliance

Reference: SP 800-53
Primary: AU-12
CM-5

CONTROL: **Check every other month of OCSZ computers, network devices and other devices that use software for software that is unauthorized or questionable.**

3.6.9.6 Reason for control

There is a wide array of software needed to run each aspect of a transit agency. The configuration management system should contain a master list of software that is approved and the version that should be run.

A period comparison of which software is available to each person, based upon job function, will show when there may be a risk.

3.6.9.7 Discussion

This control is intended to ensure proper configuration management of systems with approved software. Software that has not been identified, vetted through testing and determined safe for use could cause negative impacts to the system and may actually be or contain malicious software. It is therefore recommended that personnel perform checks of the system to verify that the system meets expectations. Any changes to the software on a system should be authorized per the configuration management and change control process.

A scan may also check for known but unacceptable software.

3.6.9.8 Measures of effectiveness

- Audit.
- The checks identify unapproved software, and an action plan is in place to:
    - determine if the found software should be added to the approved list; and remove software found to be unauthorized.

3.6.9.9 Examples

- **Acceptable:** Any scans used to check for unauthorized software should be compatible with the control system being scanned; use of a software audit configuration tool to establish a software baseline, then monitor and alert on unauthorized software present or config changes.
- **Not acceptable:** No software check performed.

3.6.10 Active malware protection

Ref #	Version	Aud.	When
11	1.0	TA	Now

TITLE: Active malware protection

Reference: SP 800-53
Primary: SI-3 SC-7(9), CM-1 CM-5 SA-1 SA-4 SA-8 SA-12 SA-13 SI-1 SI-4

CONTROL: **Use antivirus protection or software white-listing/file integrity checker on fixed/portable/mobile PCs that connect to OCSZ equipment.**

3.6.10.1 Reason for control

Cyberattacks often start with entry via a PC or laptop. The malicious code may be introduced via the Web, removable media such as a thumb drive or through rogue software installed as part of the code provided. The transit agency needs an active monitoring and reporting solution.

3.6.10.2 Discussion

Commercial off-the-shelf operating systems that are vulnerable to computer viruses, adware, spyware and similar malicious code should be actively protected via real-time monitoring products. Malicious code can also be encoded in various formats (e.g., Uuencode, Unicode) or contained within a compressed file.

A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code.

Transit agencies should have a process to ensure that any equipment entering their facilities has up-to-date scanning software, that it is active and that a recent scan has shown the PC or laptop to be free from infection.

3.6.10.3 Measures of effectiveness

- Identify the operating systems that must be actively monitored.
- Have a process to ensure that any equipment being brought into OCSZ areas is free and clear of malicious code.

3.6.10.4 Examples

- **Acceptable:** Antivirus software with updating process for signature database; white-listing/file integrity check software to detect malware or file modification.
- **Not acceptable:** No malware protection.

3.6.11 Operations control center, alternate

Ref #	Version	Aud.	When
12	1.0	TA	Now

TITLE: Operations control center, alternate

Reference: SP 800-53
Primary: CP-4
CP-1

CONTROL: **The cybersecurity process should ensure that the backup/alternate OCC cannot be used as a route for sabotage or covert monitoring of activities.**

3.6.11.1 Reason for control

The backup/alternate OCC is, in theory and often in practice, a fully operational center. However, it is not fully staffed, and this makes it a target for saboteurs to plant monitoring devices. It also makes an ideal place to inject malicious code.

3.6.11.2 Discussion

The transit agency needs to test and/or exercise contingency plans to identify potential weaknesses. In addition to keeping the alternate OCC either partially or fully operational, the transit agency must actively monitor it for suspicious activities.

The disaster recovery plans and business continuity plans should explore the vulnerabilities that can exist when the alternate OCC is partially through fully operational. There may be unexpected communication paths between the primary and alternate OCCs.

3.6.11.3 Measures of effectiveness

- The backup or alternate OCC is always included in all testing and vulnerability assessments.
- The backup or alternate OCC and its telecommunications systems are routinely updated to match the primary OCC, or plans exist to bridge the differences.

3.6.11.4 Examples

- **Acceptable:** The Backup OCC has been examined as an entry/sabotage route
- **Not acceptable:** No attention has been given to the above

3.6.12 Patch management

Ref #	Version	Aud.	When
13	1.0	BOTH	Now

TITLE: Patch management

Reference: SP 800-53
Primary: SI-2
CA-2 CA-7 CM-3 MA-2 IR-4 RA-5 SA-11 SI-1 SI-11

CONTROL: **A comprehensive patch management program should be set up with vendors for OCSZ commercial off-the-shelf (COTS) and proprietary software and firmware.**

3.6.12.1 Reason for control

Firmware and software need to be modified for both functionality and vulnerability. The transit agency must coordinate with the vendor so that updates can be applied without compromising safety and security. Certified vendor patches should be supplied for both proprietary and COTS firmware and software that is part of the vendor's supplied equipment.

3.6.12.2 Discussion

OCSZ systems have various components, some of which should be updated only in a coordinated manner with their associated control system, HMI or the underlying operating system with the hardware vendor or integrator's approval. Other components, often the HMI, may be updated based upon the software vendor's recommendation. Care must be taken to test the updates before applying them in the field.

For control systems, the ICS-CERT database run by the Department of Homeland Security records and tracks vulnerability and patch update information. Vendors of OCSZ software and firmware should work with ICS-CERT on any discovered vulnerability. The speed and nature of the response to the vulnerability should depend on the severity of the vulnerability and the potential consequences that exploitation of this vulnerability would have on field equipment.

For instance, the discovery of a remotely exploitable shell with an easy-to-deduce or default password, or a buffer overflow allowing remote administrative privileges, would be judged to be more serious than a difficult to exploit denial-of-service attack.

> **NOTE:** Guidance for setting up a patch management program may be found in the DHS CSSP "Recommended Practice for Patch Management of Control Systems," December 2008 (see References).

The time schedule agreed upon for supplying a patch should allow enough time for thorough vendor evaluation of the vulnerability and regression testing, yet occur within a reasonable period of time.

The decision about when the transit agency applies the patch should be made by the transit agency based on criticality, operating schedules and assurance of adequate patch testing offline before patches are installed. Additionally, configuration management software compatibility lists should be consulted to ensure that patching one piece of software doesn't adversely affect correct operation of another.

3.6.12.3 Measures of effectiveness

- A patch management program exists for each vendor's OCSZ products.
    - This program includes adequate testing to ensure the applied patch does not affect existing operations.
- An assessment process exists for the risk of not applying a patch:
    - Whether a system is completely and truly isolated (very rare).
    - Whether a patch affects this system (many patches are for features not used).
    - What other co-requisites are needed to install this patch.

3.6.12.4 Examples

- **Acceptable:** Vendors working with ICS-CERT and transit agencies on a documented patch management program
- **Not acceptable:** No patch management program exists.

3.6.13 Security compliance, validation

Ref #	Version	Aud.	When
14	1.0	TTr	Now

TITLE: Security compliance, validation

Reference: SP 800-53
Primary:

CONTROL: **A yearly passive vulnerability check should be performed by an outside authorized and qualified agency.**

3.6.13.1 Reason for control

A transit agency should have an outside agency assess, at least annually, its vulnerability to cyberattack in the OCSZ. The vulnerability assessment is to use control and communications security criteria current at the time of the assessment.

The senior executive of the transit agency should sign off on the results of the assessment and put mitigations in place as necessary to keep the transit system safe and secure.

3.6.13.2 Discussion

The assessment is to ensure that the continuous improvement processes are addressing the needs to keep the transit system cyber-secure.

The transit agency should have baselines and configuration management monitoring systems that ensure that the entire system is operationally correct and the least vulnerable to cyberattack as can be done reasonably.

3.6.13.3 Measures of effectiveness

- A contract exists for this activity.

3.6.13.4 Examples

- **Acceptable:** Using an outside agency with experience and qualifications on testing control systems.
- **Not acceptable:** Active vulnerability scans used on IT-type network equipment, which may affect control and communications equipment adversely.

3.6.14 Access control, Operationally Critical equipment

Ref #	Version	Aud.	When
15	1.0	BOTH	Now

TITLE: Access control, software changes

Reference: SP 800-53
Primary: AC-17 MA-4
AC-3 AC-18 AC-20 IA-2
IA-3 IA-8

CONTROL: **On-site physical presence by qualified and authorized staff should be required to change software or executables on OCSZ equipment. As an alternative, where software or executables are changed over an internal network, a cybersecurity change management procedure with verification and security checks should be implemented.**

3.6.14.1 Reason for control

Restricting both physical and electronic access is important to security.

3.6.14.2 Discussion

Whenever an OCSZ device is being accessed, it preferably should be done in person. For SCSZ or FLSZ equipment, Part II of this series specifies that the change should be done at the device. This method is also preferable for OCSZ software changes; however, an alternate option would be to devise a plan where software may be changed over an internal control and communications network, provided that satisfactory change management, verification and security checks are implemented as part of the plan.

For instance, a cryptographic integrity check on the file(s), as per control 3.6.18, may be used to ensure the transferred file(s) have not been modified.

3.6.14.3 Measures of effectiveness

- Audit

3.6.14.4 Examples

- **Acceptable:** On-site physical presence; strategy to securely change software over an internal control and communications network.
- **Not acceptable:** Remote change of software from a distance using a web interface or telephone modem without a security strategy or plan.

3.6.15 Audit and accountability, logs

Ref #	Version	Aud.	When
16	1.0	TA	To Be Dev

TITLE: Audit and accountability, logs

Reference: SP 800-53
Primary: AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 PM-9

CONTROL: **Method to collect and audit logs to meet the requirements of NIST SP 800-53 and SP 800-82.**

3.6.15.1 Reason for control

Audit logs provide accountability and forensic information. Their collection helps determine when cybersecurity was in place and when an issue was present. Logs should be analyzed regularly to reveal unexpected conditions.

3.6.15.2 Discussion

Audit logs are used to determine if there are anomalies or repeated bad behaviors by users, which should be addressed by retraining.

The audit and accountability policy should be included as part of the general control and communication security policy for the organization.

3.6.15.3 Measures of effectiveness

- An audit shows which devices have audit logs and have configured the logging to the level necessary for an audit without disrupting operations.
- The transit agency has a process to align the information from different logging systems to track across its system events that substantially occurred at the same time. In a finely tuned system, one can determine exactly the order of changes and events across systems. The challenge is the time difference (albeit slight) across disparate systems.

3.6.15.4 Examples

- **Acceptable:** TBD
- **Not acceptable:** TBD

3.6.16 Responsibility, vendor product management

Ref #	Version	Aud.	When
17	1.0	VEND	Now

TITLE: Responsibility, vendor product management

Reference: SP 800-53
Primary:CA-6
CA-2 CA-7 PM-9 PM-10

CONTROL: A vendor manager should be identified to be responsible and accountable for all vendor control and communications security activities for each OCSZ system used by transit agency.

3.6.16.1 Reason for control

Transit agencies need to know whom to contact at a vendor to answer control and communications security questions about a vendor's products.

3.6.16.2 Discussion

Each transit agency needs to have a single point of contact at each vendor who is knowledgeable about the cybersecurity aspects of OCSZ devices used by the transit agency.

The vendor needs to have someone responsible for keeping up to date on cybersecurity issues and for ensuring that its devices, products and architecture are secure. The vendor can have many people involved in this process; however, each relevant device and product should have at least one cybersecurity point of contact.

3.6.16.3 Measures of effectiveness

- Transit agency customer satisfaction.

3.6.16.4 Examples

- **Acceptable:** Control and communications security knowledgeable experts at vendor customer service locations who know both the equipment in question and cybersecurity.
- **Not acceptable:** "Just-in-time" or "ad hoc" researching of control and communications security questions and problems from transit agencies, leading to search of a vendor organization for cybersecurity knowledgeable people. Vendors with no cybersecurity knowledge base on their products.

3.6.17 Communications, wireless security

Ref #	Version	Aud.	When
18	1.0	VEND	Now

TITLE: Wireless security

Reference: SP 800-53
Primary: SC-5 AC-18
SC-1 AC-1

CONTROL: **Wireless communications security. Wireless security within the OCSZ used for monitoring only may use IEEE 802.11x (or other equivalent encrypted wireless protocols) with latest encryption technology (Currently WPA2). Wireless used for both monitoring and control should use a current VPN technology such as IPSEC or SSL to tunnel within the 802.11x (or other additional wireless protocols), to give a similar level of additional protection as a VPN.**

3.6.17.1 Reason for control

Wireless communications that are used within an OCSZ system must be protected, for reasons outlined in the Discussion section below. The degree of security protection depends on the purpose and use of the information transmitted on the link. If the information transmitted on the link is "passive," i.e., used for monitoring purposes only, an up-to-date wireless protocol, such as 802.11x with current encryption technology and algorithms, currently WPA2 and AES, may be used.

For a further description of security options available within the 802.11x protocol, such as dynamic update of security credentials, please see NIST publication 800-48.

> **NOTE:** Wireless technologies such as 802.11x are very widely used for home and commercial purposes, and are constantly being probed and attacked by hacker communities for any weakness or accidental misconfiguration in setup, operation or maintenance. Therefore, if the information being transmitted is used for both monitoring and control — for instance for SCADA commands to a traction power station or tunnel pumps — then additional security protection is warranted. A VPN protocol, such as IPSec or SSL, to act as a secure tunnel within the 802.11x envelope, or an equivalent protocol offering similar additional protection should be added, for an additional layer of protection. (Note that other critical industry sectors, such as the chemical processing and factory automation sectors, have adopted this approach, as documented in the ISA Wireless specification S100.)

3.6.17.2 Discussion

This control is intended to protect wireless communications with acceptable protocols that provide authentication and encryption. The purpose is to prevent:

- revealing operational data to snoopers;
- unauthorized access, especially sending commands to the critical system; and
- unauthorized tampering with information being sent to the OCC or to another system.

3.6.17.3 Measures of effectiveness

- Wireless communication is protected with authentication and encryption.
- OCSZ monitoring-only data is protected with latest 802.11x security; and control data is protected in addition with a VPN tunnel within the 802.11x envelope, or equivalent protection.

3.6.17.4 Examples

- **Acceptable:** As above.

- **Not acceptable:** OCSZ data sent in the clear, or with outdated security technology (such as WEP encryption for 802.11x wireless protocol).

3.6.18 Validate PLC and controller integrity

Ref #	Version	Aud.	When
20	1.0	VEND	Now

TITLE: Validate PLC and controller integrity

Reference: SP 800-53
Primary: SI-7
SI-1

CONTROL: **Use host file integrity verification with cryptographic checksum on OCSZ controllers such as PLCs, where not precluded by large or complex file structures.**

3.6.18.1 Reason for control

It is important to know that the software/firmware that a PLC or controller is running is the approved, tested and validated software and firmware. Transit agencies need to detect tampering, and a non-cryptographic checksum may be spoofed.

3.6.18.2 Discussion

Each PLC and controller should have a known configuration of software and firmware. The transit agency should be able to confirm that files on each OCSZ PLC or controller have not been tampered with. One way to do this is by comparing cryptographic checksums with the checksums stored in a configuration-managed database.

Comparing the PLC or controller's software and firmware to a controlled version that has not and cannot have been tampered with ensures that the operational PLC or controller also has not been tampered with.

3.6.18.3 Measures of effectiveness

- There is a master copy of PLC and controller firmware and software saved in a disconnected and protected method for each unique configuration of PLC and controller.
- A process exists to perform this test for every PLC and controller periodically. The testing order should not be predictive so that a malicious actor cannot exploit the window between tests.

3.6.18.4 Examples

- **Acceptable:** Using a current NIST-approved cryptographic checksum such as SHA-2.
- **Not acceptable:** Using only CRC or similar checksums to verify file integrity; not using checksums at all.

3.6.19 Incident response plan

Ref #	Version	Aud.	When
20	1.0	Transit	Now

TITLE: Incident response plan

Reference: SP 800-53
Primary: SI-7
SI-1

CONTROL: A control and communications security incident response plan should be developed to handle control and communications security incidents.

3.6.19.1 Reason for control

With the increase in cyberattacks on critical infrastructure sectors, including transportation, the likelihood of a successful cyberattack on a rail control and communications system in the OCSZ or other zones is increased. There are many government and industry resources to help transit agencies formulate a response plan, to respond to an attack if it happens and to do the necessary forensics to ensure that the malware is completely eradicated and the system is protected again.

3.6.19.2 Discussion

A typical transit agency may not have the skills, equipment and training to respond to a sophisticated attack, such as an APT attack (advanced persistent threat). A government agency like the DHS ICS-CERT has resources, including remote assistance along with a "flyaway response team," to help infrastructure should an incident occur. It is in a transit agency's best interest to formulate and rehearse a plan that would make use of internal agency and government resources to minimize downtime and equipment damage should an incident occur.

For additional information, see the ICS-CERT website and NIST 800-61 "Computer Incident Handling Guide."

3.6.19.3 Measures of effectiveness

- A plan exists, with roles and responsibilities clearly laid out.

3.6.19.4 Examples

- **Acceptable:** A plan is written and approved, and staff are trained.
- **Not acceptable:** No plan exists.

3.6.20 Software and firmware code review by vendors

Ref #	Version	Aud.	When
	1.0	VEND	To Be Dev

TITLE: Software and firmware code review by vendors

Reference: SP 800-53
Primary: SI-7
SI-1

CONTROL Software and firmware coding reviews should be instituted by systems and device vendors on new code for OCSZ devices and systems, for obvious security flaws like buffer overflows, escalation of privilege, hardcoded passwords, etc.

3.6.20.1 Reason for control

Data on the number and seriousness of hacking attacks over the years shows a dramatic increase in present times. Much OCSZ software and firmware is written in the coding languages C and C++. Successful hack

attacks take advantage of coding flaws in these languages that have been known about for many years. The flaws include the following:

- buffer overflows
- integer overflows
- illegal escalation of privilege
- lack of input filtering

Software developers should be aware of these flaws, and software development management should institute training programs to teach secure coding and to use testing tools and techniques to catch these flaws if they are already in the software. The code reviews should be an integral part of the vendor's software development lifecycle. (See Appendix B for further details on secure coding)

3.6.20.2 Discussion

Catching software errors and bugs in the coding stage is much more cost-effective than catching the same errors in testing, and very much more cost-effective than having to issue a patch if the vulnerability is caught by an independent security researcher when the device is out in the field. Then a patch has to be issued, which involves regression testing, notification of the users and negative publicity.

3.6.20.3 Measures of effectiveness

- Effort is put into establishing a secure coding effort.

3.6.20.4 Examples

- **Acceptable:** A secure coding program is in place for newly written OCSZ control and communication software programs.
- **Not acceptable:** No secure coding program exists.

3.6.21 Change Default Vendor Passwords

Ref #	Version	Aud.	When
	1.0	VEND	To Be Dev

TITLE: Change Default Vendor Passwords

Reference: SP 800-53
Primary: SI-1

CONTROL **Transit agency should change manufacturer default login credentials, such as for administrator or management access, upon installation of new equipment**

3.6.21.1 Reason for control

Frequently new software and hardware comes with a default vendor password, which is commonly known, and available in vendor manuals. These vendor passwords should be changed to transit agency-strength passwords when new equipment is put into commission.

3.6.21.2 Discussion

Frequently hackers probing a system find that system administrators and engineers have not changed default passwords, and can use a default password, which is easily obtained from vendor manuals or hacking sites, to break into a system. The new equipment commissioning procedure should include changing all default passwords, even for options or features of the system that may not be used for operations.

3.6.21.3 Measures of effectiveness

- Audit to check administrator and user passwords

3.6.21.4 Examples

- **Acceptable:** Default passwords have been changed as demonstrated by audit
- **Not acceptable:** Default passwords still exist

4. Future RP Sections – Part 3c – Securing the Train Line

4.1 Securing the train line control and communications

Train-sets are becoming more networked, computerized and automated every year. The following classes of systems are identified as a minimum set, which would be an input to the security zone classification process, similar to what has been done for the stationary rail assets in Part II and Part IIIb.

- Safety-critical assets, including vital systems such as brakes, acceleration, over-speed control and ATP, along with personnel protective and emergency systems. For instance, passenger door control, emergency interlocks and shutoffs would be included.
- Train-to-wayside communications, which would include vital, operational and maintenance data streams.
- Operational systems and networks, such as for video-feeds, diagnostic and maintenance data.
- Passenger entertainment and wireless (Wi-Fi) networks, to supply connectivity for passenger laptops and personal communications devices.

It is not known yet how the above systems will be segmented into security zones in Part IIIc.

Related APTA Standards

APTA RP-CCS-1-RT-001-10, "Securing Control and Communications Systems in Transit Environments." http://www.apta.com/resources/standards/security/Pages/default.aspx

References

CENELEC standard EN 50159 "Railway Applications - Communication, Signaling and Processing Systems - Safety Related Communication in Closed/Open Transmission Systems", September 2010

Federal Information Processing Standards (FIPS) Pub 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

International Society of Automation, "Security for Industrial Automation and Control Systems: Part 1: Concepts, Terminology, and Models," ISO 62433.

"Security for Industrial Automation and Control Systems: Part 2: Integrating Security into the Manufacturing and Control Systems Environment," ISO 62433

International Society of Automation, "Security Technologies for Industrial Automation and Control Systems," ANSI/ISA Technical Report TR99.00.01, 2007.

International Society of Automation "Wireless Security," ANSI/ISA Report S100.0,

National Institute of Standards and Technology (NIST), "Risk Management Guide for Information Technology Systems," Sept 2012. http://csrc.nist.gov/publications/PubsSPs.html#800-30

NIST publication 800-48 (Wireless Security) (Latest edition)

National Institute of Standards and Technology (NIST), "Recommended Security Controls for Federal Information Systems and Organizations, NIST 800-53, Revision 4, April 2013 http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology (NIST), "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," Revision 1, June 2010. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

National Institute of Standards and Technology (NIST), "Applying NIST SP 800-53 to Industrial Control Systems," August 2006. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Apply-SP-800-53-ICS-final-22Aug06.pdf

National Institute of Standards and Technology (NIST), "Guide to Industrial Control Systems (ICS) Security," Rev 2, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Security Agency (NSA), "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments." http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

U.S. Department of Homeland Security National Cybersecurity Division, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

U.S. Department of Homeland Security National Cybersecurity Division "Recommended Practice for Patch Management of Control Systems", December 2008. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_Patch_Management_S508C.pdf

Definitions

automatic train protection (ATP): A wayside and/or onboard train system to apply emergency brakes if a signal is missed by the train operator.

automatic train supervision (ATS): Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.

black box: A device that records information, which cannot be changed or manipulated in any manner. The information recorded is used for forensic purposes. It is used in the same sense as an aviation flight recorder.

commercial off-the-shelf (COTS): Products that are readily available commercially and may be used "as is."

communications-based train control (CBTC): A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the "moving block" principle for safe train separation rather than fixed blocks with track circuits.

configuration management: A practice and process of handling hardware, software and firmware changes systematically so that a device or system maintains its integrity over time.

cryptography: A way to encode (hide) information such that the sender intends that only the recipient should understand the message. There are many methods to encrypt and decrypt a message. Some are shared such that many can decipher (decode) the message, and others are specific to a pair of entities that wish to communicate a secret.

cybersecurity: The field of protecting digital computers and networks from accidental or malicious modifications.

cyclic redundancy check (CRC): An error-detection code used in digital networks to detect accidental changes in data during transmission or storage.

Defense in Depth: A layered approach to information security that uses multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented.

electronic security perimeter (ESP): Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate it from other zones.

emergency cutoff (blue-light) system: A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.

Enterprise Zone: The zone of a transit agency that handles its routine internal business processes and other non-operational, non-fire, non-life-safety and non-safety-critical information.

fail-safe: A device that fails in a manner that protects the safety of personnel and equipment.

fiber-optic strand: A portion of a cable in a fiber-optic network. Each strand carries information unique to it and is isolated from all the other strands.

Fire/Life-Safety Security Zone (FLSZ): A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.

human-machine interface (HMI): The control interface between humans and machines.

interlocking: An arrangement of railway signals and signal appliances so interconnected that their movements must succeed one another in proper sequence.

IPSec: A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.

malware: Short for malicious software. Such software is created and used by people, usually with bad intentions, to disrupt computer operations or obtain, without consent, confidential information.

man-in-the-middle (MitM): A type of cyberattack where an interloper inserts him- or herself in between two communicating devices, without either side being aware of the interloper.

NIST SP 800-53: NIST Special Publication 800-53, entitled "Recommended Security Controls for Federal Information Systems and Organizations" (see References). Revision 3, August 2009, was used in preparing this document.

NIST SP 800-82: NIST Special Publication 800-82, entitled "Guide to Industrial Control Systems (ICS) Security" (see References). The June 2011 final version was used in preparing this document.

operations control center (OCC): A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.

Operationally Critical Security Zone (OCSZ): A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.

passenger information display: An electronic information system that provides real-time passenger information, such as arrival of trains and their status, reason for the status and destination. Additionally, it may display other information, including advertisements, announcements, time, emergency notifications, etc.

patch management: A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.

programmable logic controller (PLC): An industrial computer used for automation of mechanical processes.

Safety Critical Security Zone (SCSZ): The zone that contains vital signaling, interlocking and ATP within rail transit.

SCADA: A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.

Secure Hash Algorithm (SHA): A family of cryptographic hash functions used to calculate a unique sum for a digital file to be used to check for later file modifications.

traction power: A network supplying power to electrically powered railways.

trusted (network): Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.

two-factor authentication: A method of authenticating a user whereby at least two distinct factors are verified. These factors may include something the user has, something the user knows or something the user is or does.

USB: Used to denote a device that uses USB as a communications method — e.g., thumb-drive/memory stick.

vital: A term applied within rail safety to denote fail-safe operation. (Derived from IEEE Standard 1483, 2000 glossary, "vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.")

vital signaling: The portion of a railway signaling network that contains vital equipment.

virtual private network (VPN): A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the Internet. A VPN in and of itself is not necessarily secure.

white-listing: Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.

Wi-Fi: In the broadest sense, all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

Abbreviations and acronyms

AES	Advanced Encryption Standard
ATP	automatic train protection
ATS	automatic train supervision
CBTC	communications-based train control
CCSWG	Control and Communications Security Working Group
CCTV	closed-circuit television
CD	compact disc
CIA	confidentiality, integrity, availability
CO	carbon monoxide
COTS	commercial off-the-shelf
CRC	cyclic redundancy check
CSSP	Control Systems Security Program
CVE	Common Vulnerabilities and Exposures
DHS	U.S. Department of Homeland Security
ESP	electronic security perimeter
FIPS	Federal Information Processing Standard
FLSZ	Fire/Life-Safety Security Zone
FTP	file-transfer protocol
HMI	human-machine interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems – Computer Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers (commonly just IEEE)
IPSec	Internet Protocol Security

ISA	International Society of Automation
IT	information technology
MitM	man-in-the-middle
NATSA	North American Transportation Services Association
NERC	North American Electric Reliability Corporation
NERC-CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OCC	operations control center
OCSZ	Operationally Critical Security Zone
PA	Public Announcement
PC	personal computer
PID	Public Information Display
PLC	programmable logic controller
PTC	positive train control
RFID	radio frequency identification
SCADA	Supervisory Control and Data Acquisition
SCSZ	Safety Critical Security Zone
SHA-2	Secure Hash Algorithm, second version
SME	subject matter expert
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
TA	transit agency
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	U.S. Transportation Security Administration
USB	universal serial bus
VLAN	virtual local area network
Volpe	John A. Volpe National Transportation Systems Center of the U.S. Department of Transportation
VPN	virtual private network
WEP	Wired Equivalent Privacy

Summary of document changes

- None

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	March 25, 2016	May 7, 2016	June 2, 2016	October 7, 2016	October 26, 2016
First revision					
Second revision					

Appendix A: How to Approach Security Retrofits for Legacy Systems

[Reference Section: Part II, 1.2.2 - Defining a security zone architecture and protecting the Safety-Critical Zone]

Preliminary suggestions and selected references

The following are a few preliminary suggestions and selected references for retrofitting security upgrades for legacy equipment presents special issues for transit agencies. Using the defense in depth model, mitigating security controls may be put in effect such as:

- Extra protection around the perimeter of these devices, such as insulating these devices from external connections
- Increased use of personnel or physical security measures as compensating or mitigating controls

Security control – how to provide isolation

[Reference: Part II, Section □ -

Connecting security zones of different security levels*]*

Additional comments on the following statement in the "Discussion" section of the security control requiring security isolation - "If technology is available, filtering at the Application Layer is also desirable."

Possible isolation techniques

You may be able to use the application layer of the Ethernet/TCP/IP (internet) stack for communication isolation. Some security controls affecting the application layer are listed in this document, such as configuration management (Section **Error! Reference source not found.**), use of antivirus or whitelisting s oftware (Section **Error! Reference source not found.**), and detecting unauthorized software (Section **Error! Reference source not found.**).

However, there are a host of techniques that are generally more sophisticated, and require more technical knowledge to research, develop, design and implement. They are:

- A secure software plan by the vendors. At the application layer, techniques that eliminate buffer overflow, format string vulnerabilities, and other coding vulnerabilities may be introduced.
- Deep packet inspection firewalls – Depending on the protocol used, there may be application layer firewalls that look at every application layer packet to separate out illegal or unauthorized commands to networked equipment.

Appendix B: Writing Secure Software and Firmware for OCSZ Systems

Typical OCSZ Control System Components

Looking at the systems listed for OCSZ in Figure 3 there are at least the 3 types of devices listed below:

- **PLCs and microcontrollers** (usually found in train station equipment rooms, wayside bungalows, and tunnel equipment cages. These devices usually have embedded code in firmware (no hard drives), and are often written in C/C++.
- **HMI Operator programs.** This application software presents a pictorial or menu-driven picture of train movement, power flows, etc. to control room operators, and this application software is typically mounted on Windows ® or Unix based workstations. Programming code varies, as it could be written in C++, Visual Basic ® or Java, or other popular languages.
- **Networking components** (routers, switches, firewalls, etc.). These may be located any place in the control and communications network, and software languages vary by vendor. Operating systems and applications are often proprietary.

All three of the above types of components could benefit from a vendor secure coding effort. However, the support for secure coding programs among equipment vendors still needs to grow, and encouragement and purchase requirements from the transit agency community will help this process along.

4.1.1 Starting a secure coding program

To begin such a program, the following factors are necessary as a minimum:

- Developers trained in secure coding techniques
- An established and repeatable software development lifecycle, including cybersecurity tasks and checkpoints
- Software audit and testing tools, as needed
- Supportive management, to allow the development team time, resources, and support to complete their tasks. This is sometimes difficult to obtain because of time pressure to release new code.

Secure coding methodologies

At the present time, there are at least three popular methods to guide a secure coding program:

- **Microsoft ® SDLC (Software Development Life Cycle).** This is the most involved of the programs, and builds off of Microsoft's efforts in past years. This is one of the most rigorous and costly programs to implement secure code correctly, and was used for operating system software (which can have 40 million lines of code). It has been used by Microsoft since 2004.
- **OWASP CLASP ®.** This is termed a "lightweight secure coding procedure, primarily written for web applications but in the opinion of APTA also applicable to embedded code for PLCs, etc. It is listed on the DHS ICS-CERT website as a good candidate to consider, and appears at first glance to be a good, practical candidate for transportation software, not requiring a huge investment in training, cost, or time.
- **Touch Points.** This is also a "lightweight" secure coding methodology, popularized by the company Citigel, which puts an emphasis on static code review among other tasks.

Advantages/payback for instituting a secure coding program for vendors

Secure coding programs allow vendor to catch more software bugs, both security and non-security related earlier in the process, before testing and release.

Implementation provides the following advantages:

- Reduce warranty and patch coding and release under time pressure later on.
- Increase safety and decrease operational costs, as a security bug may affect safety or reliability of equipment out in the field.
- Decrease the chance of a security researcher or hacker finding a vulnerability, with accompanying negative publicity, and necessity of issuing a patch, and going on the DHS Common Vulnerabilities and Exposures (CVE) database.
- Increase customer confidence and positive publicity, as transit agencies are concerned about cybersecurity, and may include requirements in purchase specs.
- Goodwill for contributing to a secure rail infrastructure to transit agencies and the public.

Disadvantages of not instituting a secure coding program

Risk of:

- Warranty issues if software bugs cause operational, safety, or security issues.
- Cost of quick patch release when security bugs are found
- Possible lawsuits
- Negative publicity on the web
- Negative image and calls from concerned customers
- Vulnerability used as an exploit in a virus, Trojan horse, etc.