



American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA-SS-CCS-RP-002-13

Published June 28, 2013
Control and Communications
Security Working Group

Securing Control and Communications Systems in Rail Transit Environments

Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

Abstract: This document covers recommended practices for securing control and communication systems in rail transit environments.

Keywords: communications based-train control (CBTC), control and communications security, cybersecurity, positive train control (PTC), radio, rail transit vehicle, SCADA (supervisory control and data acquisition), train control, signalling

Summary: This Recommended Practice is **Part-II** in a series of documents to be released. **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)**. Later parts will cover recommended practices for less critical zones, the rail vehicles, and provide other guidance for a transit agency.

Scope and purpose: This *Recommended Practice* is not intended to supplant existing safety or security standards or regulations. It is instead intended 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; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

This *Recommended Practice* represents a common viewpoint of those parties concerned with its provisions, namely, transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a transit system's operations. In those cases, the government regulations take precedence over this standard. APTA recognizes that for certain applications, the standards or practices, as implemented by individual transit agencies, may be either more or less restrictive than those given in this document.

© 2013 American Public Transportation Association. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the American Public Transportation Association.



Participants

The American Public Transportation Association greatly appreciates the contributions of the following individuals, who provided the primary effort in the drafting of this *Recommended Practice*.

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

Chuck Weissman, *Chair*

David Teumim, CISSP, *Facilitator*

John Moore, Secretary

Leigh Weber, CISSP, *Editor*

David Trimble, Assistant Editor

Theo Lawrence

Kevin Garben

Brad Murray

John Weikel

Darryl Song

Henry Zhou

Mark Hartong

Rick Lawson

Andrey Milojevic

Mark Fabro

APTA Standards Project Team

Martin Schroeder, MSME, PE,

APTA Chief Engineer

Kevin Dow, *APTA Program Manager*

Samantha Smith, *APTA Program Manager*

Contents

1. Introduction.....	1
1.1 Intent of the series.....	1
1.2 Parts of the series	1
1.3 Background.....	2
2. The need for cybersecurity in rail transit control systems.....	4
2.1 Overview.....	4
2.2 Challenges.....	5
2.3 Where do the risks lie?	6
2.4 Comparison of enterprise IT with industrial control systems	8
3. Cybersecurity approach	9
3.1 Introduction.....	9
3.2 Defense-in-Depth (layered defense)	12
3.3 Detection-in-Depth	14
3.4 Cybersecurity risk zones	15
3.5 Defense-in Depth for transportation systems.....	18
3.6 An example transit system.....	19
3.7 Applying Defense-in-Depth to a model transit system.....	20
4. System security and minimum controls for Safety Critical Zones 29	
4.1 Legend	29
4.2 Overview.....	30
4.3 Controls	34
5. Applying security controls to zones	58
5.1 Safety-critical signaling	58
5.2 Safety-critical Fire Life Safety	58
6. Preview of the <i>Recommended Practice</i> series, Part III	59
6.1 Protecting the OCSZ.....	59
6.2 Securing the train line control and communications.....	60
6.3 Attack modeling for transit control and communications systems	60
Appendix A: Control and communications system account worksheets.....	61
Appendix B: Out-of-Scope Item Discussion	65
References	66
Definitions	68
Abbreviations and acronyms	71

Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

1. Introduction

This *Recommended Practice* is Part II in a series of documents to be released. 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 in 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 III will cover recommended practices for less-critical zones and the rail vehicles and provide other guidance for a transit agency.

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 cyber security 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. This document, 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:

TABLE 1
List of Recommended Practices

Part I	Published July 2010	Elements, Organization and Risk Assessment/Management
Part II	This document	Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones
Part III	To be determined	<ul style="list-style-type: none"> • Address the Operationally Critical Security Zone • Address Security Zones onboard the Train Set • Attack Modeling for Rail Transit

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 (this document) will assume 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.

1.3 Background

Many systems need to interoperate to allow a transit agency to provide service to the public. New technologies, combined with the pressure to be more cost-efficient, have transit agencies interconnecting more of their systems. Many of the systems were never envisioned as being interconnected or accessible, directly or indirectly, via a powerful network. Neither the components nor the systems used every day to control trains, signals, controls and communications were designed with an organized set of cybersecurity criteria anticipating today's cyber threats.

The long design life of highly reliable systems adds another challenge to addressing control and communications security. Businesses that do not use Industrial Control Systems (ICS) may replace 100 percent of their systems within a five-to seven-year window. Transit, which uses ICS, rarely replaces all of its systems, and those that are replaced may last much longer than 30 years.

Transit agencies should consider the following questions:

- Can a computer or mobile device be used to collect intelligence about the operational network(s)?
- Can an outsider use the network to take control of the system(s)?
- What can an unhappy insider do to the network?
- How can policies, lines of responsibility, training and compliance audits help secure the agency's assets?

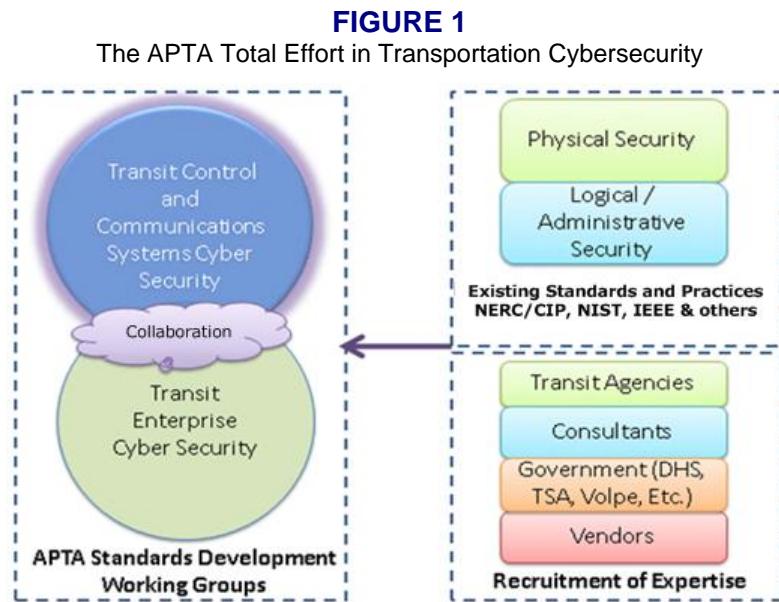
- How can software change management lessen the chances of software configuration problems?
- What could a computer virus do to your computer systems?

1.3.1 APTA's approach

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

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

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 consultants participate in defining and reviewing this *Recommended Practice*.



1.3.1.1 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.

1.3.1.2 Control and Communications Security Working Group

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

2. The need for cybersecurity in rail transit control systems

2.1 Overview

A transit agency is a very complex organization that has equipment that moves along railroad tracks. The systems that have been used to control and communicate are located along the routes in wayside bungalows, stations, road crossings, signal towers, tunnels, maintenance yards, power stations, refueling depots, equipment storage yards/parking lots, storage depots, local control rooms and operations control rooms. There are also key parts of the control system buried under or alongside the rail lines and signals that are transmitted in the rails or via specialized aerial paths.

A transit agency has to combine dozens of systems, including the following:

- access control systems
- advertising
- closed-circuit television (CCTV)
- control and communication
- credit card processing
- detection systems for environmental threats (CO, CO₂, poisons)
- emergency communications
- emergency notification
- emergency ventilation systems
- fare sales/collection
- fire detection/alarms/fire suppression
- grade crossings
- lighting
- passenger information systems
- people-moving systems (elevators, escalators, people movers)
- police dispatch
- pumping systems
- signals and train control
- ticketing systems
- traction power
- vertical lift devices (elevators, escalators)
- vital communication-based train control (CBTC), automatic train protection (ATP) and signaling

This *Recommended Practice* characterizes these systems with respect to personnel and passenger security.

TABLE 2
Zone Names

Importance	Zone	Example System
Most Safety Critical ↑ Most Public	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
	Enterprise Zone	Fare systems, turnstiles, accounting systems, schedule systems
	External Zone	Communications with the Internet, business partners, vendors and others

In the past, many of these systems did not have any need or method to communicate with each other. The connections between and among them were usually direct connections such that one wire connected to another device without any sharing communications—except the cable that the wire was enclosed in.

Today's environment has changed so that the communication between and among devices is digital via Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP) or a similar networking standard. This standardization gives new capabilities. It also gives rise to unanticipated attack paths on these key systems. This *Recommended Practice* is designed to help transit agencies identify their risk to cyber-attack and to augment the knowledge found in other DHS, ISA, NIST and related documents. It explores the unique aspects of transit and discusses how to apply well-defined cybersecurity techniques to keep transit agencies' systems operational and under control.

2.2 Challenges

Transit agencies have spent anywhere from dozens to more than 100 years running their systems and have dealt with a vast array of issues and threats with an excellent record of safety, on-time performance and reliability. The challenge today is to add cybersecurity awareness and cyber defense measures to the transit agency culture in the same manner that safety has been added to the culture of manufacturing and transportation. This will reduce the risks to transit agencies and their supplier base from cybersecurity incidents and possible liability should an incident take place.

2.2.1 Shared infrastructure

Due to the vast distances that transit agencies traverse, there is a tendency to use the same physical communications conduits and, in some cases use multiplexing technologies, for various operations. This reuse may create vectors for cyber-attack. Other shared infrastructure—such as broadcasting via radio signals over well-known frequencies and transmitting “in the clear,” i.e., unencrypted commands and text—are also avenues that may be used to usurp control of a control system.

2.2.2 Systems with long life cycles

Some elements of transit systems have very long lives, measured in decades, not years. Business systems can be fully replaced in several years under ordinary replacement schedules. Transit systems, however, are not replaced in significant ways for decades.

2.2.3 Real-time and time-sensitive information

Control systems by nature have real-time and time-sensitive requirements that are not common in traditional IT systems. Control systems are also expected in many cases to have no downtime. Antivirus, whitelisting, firewall and other current cyber-defense technologies that may inject delays in communications or block execution of programs carry the risk of unintentionally disrupting system functions and therefore must be carefully evaluated.

2.3 Where do the risks lie?

Transportation agencies traditionally considered their communications and control systems to be proprietary (security by obscurity) and not to be connected to the outside world and therefore assumed to be secure. *This assumption and attitude is no longer valid or acceptable.*

2.3.1 Connectivity changes

Until recently, the security of control systems could be addressed by carefully limiting physical access to elements of the control system, such as modems, terminals and control computers, and relying on obscurity. Systems were primarily implemented using proprietary hardware and software communicating non-standard protocols over privately owned modem lines and had no practical connections to other systems, such as IT and business systems or the outside world. To compromise the system would require specialized knowledge and access to locked equipment rooms. Attacks, if successful, would generally be isolated to one remote site, could not easily propagate, and could not be stored.

Modern control systems components and architectures are virtually indistinguishable from business information system components and architecture. Servers and workstations utilize standard off-the-shelf computer hardware and operating system technology. Servers and workstations both use available open system architectures and commercial-off-the-shelf software. TCP/IP and other published industry standard protocols (often not secured) are used for inter-process and remote site communications over wire and wireless connections. Information and products are widely available to the general public for almost every component of a modern control system.

2.3.2 Malware infection methods

Vulnerabilities exist even for unconnected systems through the following methods of indirect malware infection:

TABLE 3
Malware Infection Methods

Supply chain	Undesirable software/functions may already be embedded or pre-loaded in off-the-shelf equipment. Vendors may deliver infected or un-validated software.
Human factors	Irresponsible use of portable media (USB) for unauthorized data/program transfer.
Inadequate physical security	Who is touching or can touch “secure” equipment?
Inadequate configuration management	Unknown connections may be made through a change to the system.
Unexpected/indirect connections	There are paths from one system to another that may not be anticipated or understood.

Extensive use of open and off-the-shelf technologies expose systems to vulnerabilities once limited to traditional IT systems and personal computers. Agencies can no longer rely on proprietary networks, hardware and software for protection. Open standards and proliferation of readily available tools (both legitimate and malicious) make things easier for people with bad intent. It is no longer necessary to hack the system. One only needs to gain access and then utilize available tools.

Connection to the outside world and corporate business and enterprise systems is inevitable if not already in existence. Agencies are facing increasing pressure from both inside and outside the organization to obtain and share data. Web-enabled public information systems and remote business partner interfaces are a growing trend.

Wide geographic area deployment of equipment, sometimes in unprotected public locations, presents additional security vulnerability to transportation systems.

2.3.3 Different approaches to cyber security

There is a fundamental difference in approach to protecting a business information system compared with an industrial control system (compare **Table 4** and **Table 5**).

- **Business system:** The business is most concerned about keeping information *confidential*; that is, it does not want private information such as social security numbers, credit card numbers, salaries or medical information to be made public. A business also needs to know that when it gets the information, that it is the correct and complete set of information—in other words, that the information has integrity. If the information is not available, that is inconvenient but not a critical problem. The company may ask its customer to call back at another time.

TABLE 4
Business IT Priority

Confidentiality	HIGH IMPORTANCE
Integrity	HIGH IMPORTANCE
Availability	Lower Importance

- **Control system:** The control system needs information to be *available* so that calculations can be made, so that trains can be stopped or started and so that crossing gates go up and down appropriately. The information's integrity is important, and its confidentiality may be the least important. There are cases where integrity is as important as or more important than *availability*. For example, it is always important to know where the system's trains are and that the switches and crossing gates are in their correct positions.

TABLE 5
Transit Control System Priority

Confidentiality	Lower Importance
Integrity	HIGH IMPORTANCE
Availability	HIGH IMPORTANCE

Table 6¹ summarizes the potential impact definitions for each cyber security objective—confidentiality, integrity, and availability. (Please note that the FIPS table was developed for business systems.)

TABLE 6
FIPS Cyber Security Categorization

Security Objective	Low	Moderate	High
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.[44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.
Availability: Ensuring timely and reliable access to and use of information.[44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.

2.4 Comparison of enterprise IT with industrial control systems

Figure 2 summarizes several cyber security topics as they apply to traditional IT systems and industrial control systems.²

The key differences between enterprise IT and ICS are the following:

- Difficulty of testing and applying patches to ICS because those systems affect life safety and, separately, are for systems that are meant to run uninterrupted 24 hours a day.
- ICS systems have a very long life cycle measured in decades, compared with many IT components that last only three to eight years.
- Note that “Secure Systems Development” is usually not an integral part of industrial control systems development, however it is being practiced more during hardware/software development lifecycle.

¹ FIPS Pub 199, February 2004, Standards for Security Categorization of Federal Information and Information Systems

² US-CERT, http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

FIGURE 2

Comparison of Enterprise IT with Industrial Control Systems

NOTE: Compare the business / enterprise point of view (middle column) with the Industrial Control System (right column)

SECURITY TOPIC	INFORMATION TECHNOLOGY (IT)	CONTROL SYSTEMS (ICS)
Antivirus and Mobile Code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch Management	Easily defined; enterprise wide remote and automated	Very long runway to successful patch install; OEM specific; may impact performance
Technology Support Lifetime (Outsourcing)	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Cyber security Testing and Audit (Methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; non trivial process due to impact
Asset Classification	Common practice and done annually; results drive cyber security expenditure	Only performed when obligated; critical asset protection associated with budget costs
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and Environmental Security	Poor (office systems) to excellent (critical operations systems)	Excellent (operations centers; guards, gates, guns)
Secure Systems Development	Integral part of development process	Usually not an integral part of systems development
Security Compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

3. Cybersecurity approach

3.1 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 cyber-attack against transportation sector control systems through risk-mitigation activities.

3.1.1 What needs protection?

Transit systems are complex and consist of equipment, people, policies and processes that work together to transport people safely and in a predictable manner. There are many protections in place today, mostly focused on the physical security of the passengers and the transit system's assets. In general any device that uses a digital processor, communicates with digital devices, connects to a communication network via a wired or wireless connection, or that can be programmed could be considered for protection.

A rail transit system is comprised of several components:

1. **Transportation:** Rail(s) that guide the train-set, which includes switches to change track/guide and many other devices built into the track/guide to ensure wheel placement, and, end of track bumpers, etc.
2. **Control signaling system:** Signals (if present), road crossings and speed controls.
3. **Communications:** Between and among operating trains, crews, station attendants, police and the operations center
4. **Stations:** Below ground, at grade, or above ground. A system may be a mix of these station types.
5. **Notification methods:** Signs, electronic signs, public address (PA) systems, horns and other types of displays
6. **Train-sets:** which may have separate locomotives; these may be powered by different methods.
7. **Traction power systems:** For electrified railways

3.1.2 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.

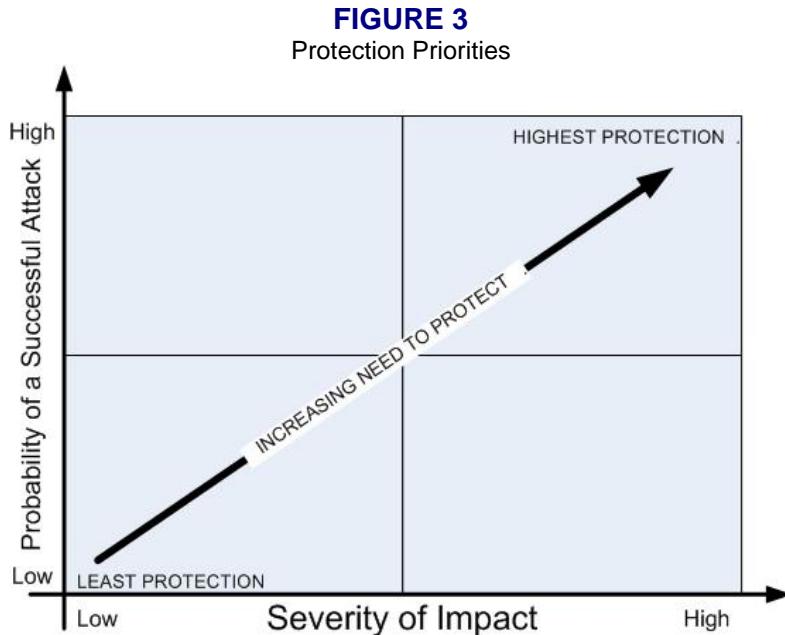
Rail systems have many levels of safety built into them via redundant circuits, fail-safe control systems (vital logic), and other mitigations. The role of cybersecurity is to ensure that these existing systems cannot be duped into making a wrong decision, and to ensure that these systems cannot be directly 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 protection:

- **Prevention:** 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
- **Tamper detection and auditability** ensure appropriate personnel are notified of unauthorized or abnormal activity and can respond in a timely manner to take action as required

In addition, transit agencies need to identify those systems, devices and processes that are most important or are most easily corrupted.

Figure 3 shows which systems need the most protection and which need the least. It is based upon the probability of a successful attack and the adverse impact such an attack would have.



3.1.2.1 Cybersecurity culture

Many cybersecurity breaches occur accidentally, when the wrong person is given access to an important system, people don't pay attention to what they are doing, or outsiders are given an opening into computer systems via a virus, malware or a phishing type attack (e.g. clicking on a link in an email).

There is a growing threat from focused, malicious groups including organized crime, “hacktivists” and state-sponsored cyber-war groups. It is very important that a transit agency’s cybersecurity culture stay on top of the evolving threat landscape in order to protect its passengers, staff and assets. Agencies need to be connected to sources of official (e.g., DHS Surface Transportation Information Sharing and Analysis Center [ST-ISAC]), as well as unofficial sources that forewarn about potential threats.

Just as transit agencies have created a safety-centric culture—saving lives and reducing accidents and accident severity—they need to foster and create a cybersecurity culture. This requires an awareness program; a training program; an assessment of cybersecurity threats; a reduction of the attack surface (the number of places and ways someone can attack transit systems); a cybersecurity program that addresses: threats, mitigations, the software/firmware update process, monitoring and detection methodologies; and the ability to be audited to check for compliance via logs and change-management systems.

Please see Part I of this series, “Securing Control and Communications Systems in Transit Environments” (APTA RP-CCS-1-RT-001-10), for information on starting a cybersecurity program.

3.1.2.2 Cyclical review

Cybersecurity is a rapidly changing set of threats. The people who want to disrupt or access transit systems keep coming up with new ways to cause harm. A program is needed that routinely examines:

- threats;
- strengths;
- weaknesses; and
- resources.

The program's goals are to define, protect from and reduce the probability of a cybersecurity incident. These reviews should be "built into" internal procedures, processes and operations.

3.2 Defense-in-Depth (layered defense)

In order for an agency to protect it's most valuable and important assets, it is thought safest to have layers of defenses so that outsiders have no direct access to an agency's most valuable assets. Defense-in-Depth implements multiple levels of security to provide layers of backup in the event a security control fails or an attempt is made to exploit new or unaddressed vulnerabilities. This strategy was conceived by the National Security Agency (NSA) and is an adopted recommended practice of the Department of Homeland Security Control Systems Security Program (DHS-CSSP).

Defense-in-Depth is the recommended strategy for securing communications and control systems for the transportation sector. Defense-in-Depth is a practical strategy for achieving cyber security objectives in today's highly networked environments. It is a best-practices strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability, cost, performance and operational considerations. It effectively addresses many cybersecurity scenarios by:

- increasing the amount of time and number of exploits needed to successfully compromise a system;
- increasing the likelihood of detecting and blocking attacks;
- allowing security policies and procedures to better align with agency organizational structure; and
- directly supporting the identification and implementation of cyber security risk (or impact) zones.

For a transit agency to successfully use the Defense-in-Depth model, it needs to define zones, giving each zone its own defensive layer. A zone may be contained within another zone or a zone may be parallel and separate from another zone. A zone has a boundary or an interface point that protects information and transactions as they move across zone boundaries (electronic security perimeters or ESPs; see Definitions).

Transit agencies need to combine Defense-in-Depth with Detection-in-Depth, a compliance program, and an audit program to ensure that all parts of the layered defense are in place, configured properly and working as designed.

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

3.2.1 Types of threats

Simply put, a transit agency needs to ensure that no one can interfere with its normal and proper operation. It should control what is going on and who has access and privilege to monitor, operate and react to changing conditions. It is a best practice to start from the assumption that all access is denied until a valid reason is given, then the least amount of privilege is given to the least amount of people. This practice is known as the "Principal of Least Privilege".

3.2.1.1 Accidents and errors

To reduce the chance of an innocent mistake becoming a serious problem, a transit agency should restrict each group to its own equipment and systems. To make our systems safe it must be acknowledged that we are all human. Mistakes are inevitable, so a good system builds in controls, logging and other procedures to ensure that people do their job, that they are reminded when they are accessing critical equipment or systems, and that they are challenged when they try to enter sensitive or secure locations. They may have to show ID, use a special key or enter a special value, such as a pass phrase or a password into a system before being able to access the system and make the change.

3.2.1.2 Intentional attacks

Whether from a disgruntled insider or from an outsider, attacks come in many forms. Some may attempt to breach security just to gather information, while others may intend to directly take control of systems or change the information displays in order to cause an accident or catastrophe.

3.2.2 Embedded/included software

Suppliers often include or rely upon software that they did not develop or do not maintain.

Examples:

- An open-source web-server
- File-transfer utilities
- Remote management utilities

These features may be important for the initial configuration of the device, or they may be present for other reasons, such as convenience. Each of these software applications needs to be monitored, controlled, configured and patched as necessary. (Note: see Section 4. - control 4.3.13 for a further discussion on patch management)

A transit agency must know if its vendor will support patched versions of the “convenience” applications, and it must also know the vulnerabilities that will exist if it does nothing. In general, if the “convenience” application is not required, it should either be removed or locked down so that an attacker cannot use it as an entry or control point.

3.2.3 Sources of threats

An insider (employer, contractor, etc.) may unintentionally compromise a system because they have been manipulated (social engineering attacks), or their computer or device has become compromised. If an insider’s equipment is not properly protected; or the change management system is lacking proper controls, then the control system can be compromised by the insider – unwittingly.

A disgruntled insider is one common form of an attack and is often the hardest one to protect against. Such an insider has plenty of information about the transit agency’s operation, and his or her colleagues are often willing to “bend” the rules on their behalf.

Threats also can come from outside—anyone from a teenager to a competitor to organized crime to a state-sanctioned cyber-war group.

3.2.4 Well-known attacks

Some examples of cyber-attacks on rail have already been publicly documented, including the following (see also Section 2.3.3, “Different Approaches to Security”):

TABLE 7
Well-Known Transportation Cyber Attacks

Class 1 freight railway virus attack in 2003	This class 1 freight railway virus attack caused a morning shutdown of signaling and dispatch systems in 23 states east of the Mississippi, also halting Amtrak trains in that area.
Polish tram hack in 2007	The Polish tram hack caused injury to 12 people and derailment and damage to four vehicles.
Denial of service attack	Denial of service attack against a backup network supporting signaling, causing speed restriction on the entire line.

More details of these attacks and their consequences, and details of cyber-attacks affecting other industry sectors, may be found in Part I of this series, under Appendix A.

3.2.5 Managing threats

All of the above factors contribute to special security challenges for transit control systems. Cybersecurity controls that may be effectively applied to traditional IT systems may not be appropriate for control systems and/or might compromise their function in unexpected and potentially unsafe ways.

3.2.6 Attack modeling

Attack modeling is an advanced technique for analyzing system threats, vulnerabilities and risks and will be introduced in Part III of this series.

3.3 Detection-in-Depth

A key concept that is a companion to Defense-in-Depth is Detection-in-Depth. Detection-in-Depth is a way to detect that an intruder has gained access to a transit facility. Detection methods must be created for each zone and defensive layer. The principle of least privilege tells us to first block ALL outbound traffic, and then create permission for known and necessary outbound connections.

In many IT environments, the isolation devices (e.g., the firewall³) have many rules to prevent unauthorized connections into the protected zone, but often there are no rules to prevent outbound connections. Malware takes advantage of this lack of protection; after the malware infects a device, the malware makes an outbound

³ A firewall is a dedicated device that adds a layer of security to your network. The firewall's main objective is to control the incoming and outgoing network traffic. It can do that by analyzing all data packets passing through it and determining which are allowed based upon preset rules.

connection to its creator. The creator then has complete control of the infected machine. Defense-in-Depth prevents this scenario by creating outbound connection rules in the isolation device and blocking such outbound connections. A Detection-in-Depth system would also include monitoring and profiling information to detect an unusual connection attempt from the machine and to detect that malware had infected the machine.

3.4 Cybersecurity risk zones

Figure 4 shows an overview of the key elements of a Defense-in-Depth strategic framework for a manufacturing facility.

A successful Defense-in-Depth approach requires agencies to partition control system components and functions into distinct zones based on specific security requirements. It is further recommended that the types of zones be limited in order to simplify the application of consistent controls. Each zone will require a unique security focus and strategy.

Architectural security zones segment hardware, software and networks into physically distinct areas with well-defined connections between them. Commonly, each architectural zone is managed by a separate business unit and is protected by a dedicated device, perhaps a firewall or other controlled device.

Cybersecurity risk zones (also known as impact zones) segment system functions into distinct impact areas with well-defined data exchanges among them. Cybersecurity risk zones present special planning challenges in that they exist within each architectural zone and potentially across them. Different business units may need to establish joint responsibilities in the security management and monitoring of a particular cybersecurity risk zone.

3.4.1 The DHS manufacturing model of Defense-in-Depth

The Defense-in-Depth strategy from DHS is available for manufacturing industries, as shown by **Figure 4**. This model is for a chemical plant or similar manufacturer. The following uses much of the language from DHS's "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies" (October 2009).

In a simplified model, a manufacturing facility has the manufacturing plant where the product is made and the offices where the rest of the work is done. The IT systems are roughly divided into the control domain, a closed environment, which helps run the plant, and the IT corporate systems, which are used for the business of running the business.

The "closed environment" of the control domains allowed industry to have a level of reliability that permitted the safe and efficient operation of the plant. For the most part, a person would need physical access to the plant and the control equipment to sabotage or modify its normal operation.

Table 8 shows the DHS model of security zones for manufacturing.

TABLE 8
DHS Zone Model for Manufacturing

Zone	Description	Security Priority	Ref. Number
External Zone	The area of connectivity to the Internet, peer locations, and backup or remote offsite facilities. This is not a demilitarized zone (DMZ), but it is the point of connectivity that is usually considered untrusted.	Lowest	N/A
Corporate Zone	The area of connectivity for corporate communications. Email servers, Domain Name System (DNS) servers, and IT business system infrastructure components are typical resources in this zone.	Medium	1
Manufacturing/ Data Zone	The area of connectivity where a vast majority of monitoring and control takes place. It is a critical area for continuity and management of a control network. Operational support and engineering management devices are located in this zone alongside data acquisition servers and historians. This zone is central to the operation of both the end devices and the business requirements of the Corporate Zone.	High	2
Control/Cell Zone	The area of connectivity to devices such as programmable logic controllers (PLCs), HMI and basic input/output devices such as actuators and sensors.	Very High	3
Safety Zone	The area that controls directly and often automatically the devices that control the safety level of an end device, such as safety instrumented system.	Extremely High	4

The simplified IT architecture provided a means for data sharing, data acquisition, peer-to-peer data exchange and other business operations. However, the security of any given system was based on the fact that few, if any, understood the intricate architecture or the operational mechanics of the resources on the control system local area network (LAN). This “security by obscurity” model does not address insider threats, however, it generally worked well for environments that had no external communication connections, thus allowing an organization to focus on physical security to safeguard their system.

NOTE: The underlying assumption in the control domain is that all of the components are trusted. The control system tries to detect data transmission errors, but it is not expecting sabotage. A control system, when confronted with problems will alarm and, if necessary, fail-safe.

What has changed? The control domain is now connected to the corporate IT infrastructure, and there are few, if any, organizations that do not have a connection to the Internet. Therefore, in today’s interconnected environment, it is conceivable and possible for someone acting remotely to access and modify a control system.

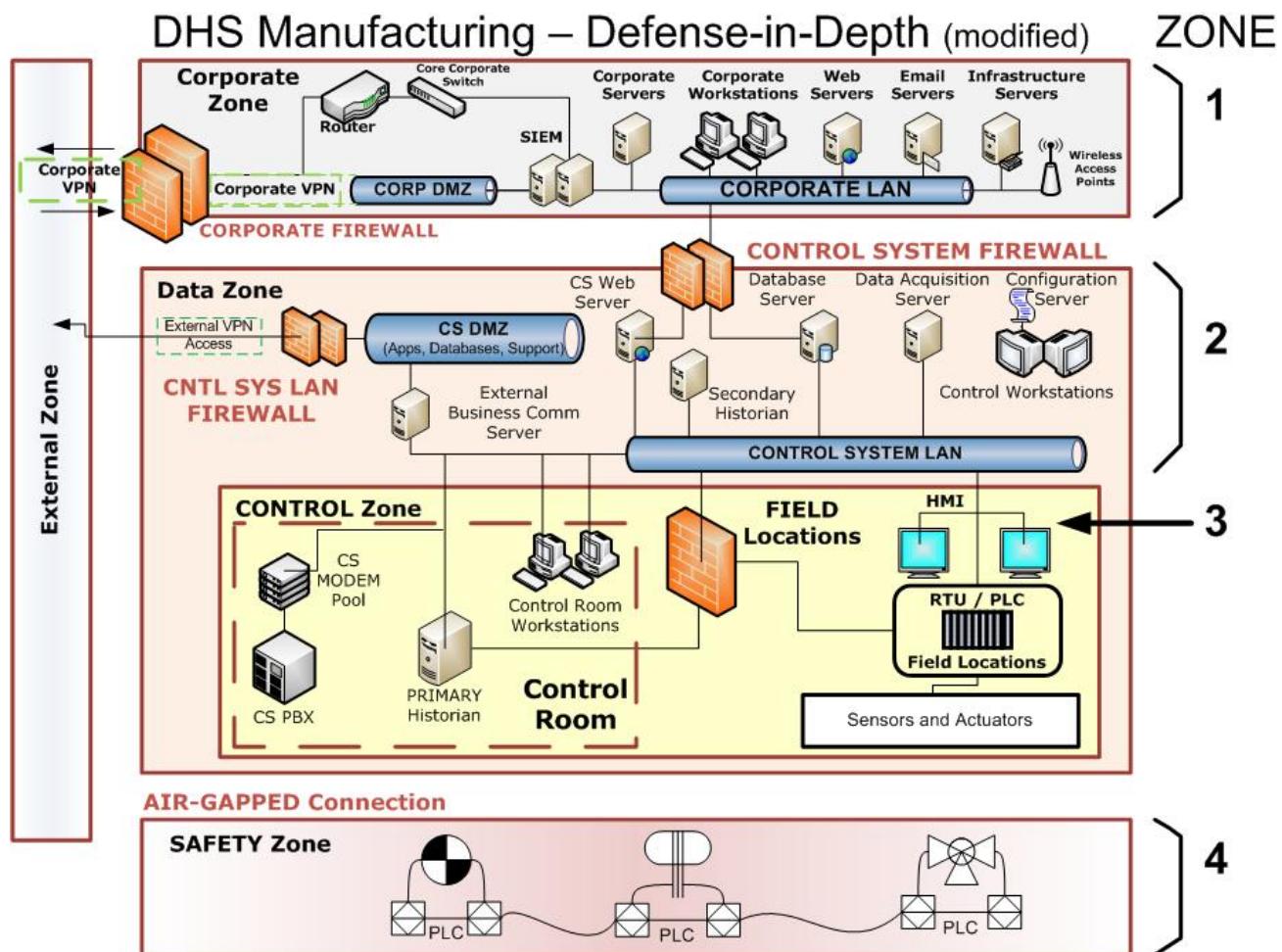
The merging of a modern IT architecture with a control system is challenging. The control system network probably does not have any cybersecurity countermeasures in place. How does one evaluate the risk and devise reasonable countermeasures to ensure the efficient and safe operation of a plant while still gaining the benefits of a very integrated IT architecture? The goals are to minimize the ability:

- for an attack attempt to go undetected;
- for an attack to be successful; and
- for an attacker to learn about the plant’s IT and control systems and their security.

NOTE: **Figure 4** is based upon the DHS Manufacturing Defense-in-Depth diagram in “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies.” It has been modified in these ways:

- The External Zone content is highly simplified.
- The Control Zone has been divided into Control Room and Field Locations.
- The Safety Zone has a different set of symbols shown.
- Various symbols have been modified.

FIGURE 4
DHS Defense-in-Depth for Manufacturing



The challenge for transit agencies is to take this design approach and apply it to a transportation system. There are differences in location, “product” and the overall geographic area served.

3.5 Defense-in Depth for transportation systems

3.5.1 What is different?

There are several differences between a rail transportation system and a single manufacturing site:

- distance
- communication
- power
- people
- access to property

3.5.1.1 Distance

A rail system covers vast distances, and each segment of the rail system has to communicate with its adjacent segments and with the operations control center (and backup operations control center). Transit agencies are expert at the physical security aspects of their systems. Cybersecurity adds a new dimension to the security program.

In addition, a rail system includes self-contained equipment rooms located along the tracks, known variously as signal bungalows and waysides.

3.5.1.2 Communication

There are various means of communication among the segments:

- wired communication
- wireless communication

The various types of wiring can be located underground, above ground, or through signals sent directly through the track.

A transit agency needs to communicate with maintenance crews on or near the track; with engineers/drivers (if applicable); between the train set and the wayside; and between and among the control and signal devices, such as signals, road crossing gates, track circuits, various maintenance and detection devices, passenger information displays, emergency information displays, advertising displays, and others.

Much of the communication needs to be done along long distances and in all kinds of weather, where line-of-sight communication can be difficult due to nature (snow, plant growth, downed trees), and in an electrically noisy environment that is difficult to shield. Also, train systems often use a different electrical ground default from all other commercial systems. Stray signals can be anathema to good communication system operation.

3.5.1.3 Power

A transit system often has its own traction power stations for electricity. There are power feeds from local utilities that need to be coordinated. Power is distributed via catenaries or third rail. Additional power is required to run all other equipment, including lighting, communications and signals. There are differences between a railroad electrical system and most other commercial systems; the most common difference is the use of floating ground.

3.5.1.4 People Everywhere

The purpose of a transportation system is to move people. They are the precious cargo of the system, and they expect and need to be delivered safely. In a manufacturing environment, there are relatively few people who need to access the site, and their movements can be carefully controlled.

Transit systems have many large, public areas, including entrances, exits, platforms, waiting areas and amenities (toilets, cafes, etc.) that must allow everyone access. There are other areas that need to be restricted, such as equipment and power rooms, tracks, signaling systems, employee areas and so on.

Although a manufacturing plant has people to operate and secure the plant, transportation systems can be a much more compelling target due to the vast number of people who use it and any attack's immediate impact upon passengers.

3.5.1.5 Access to property

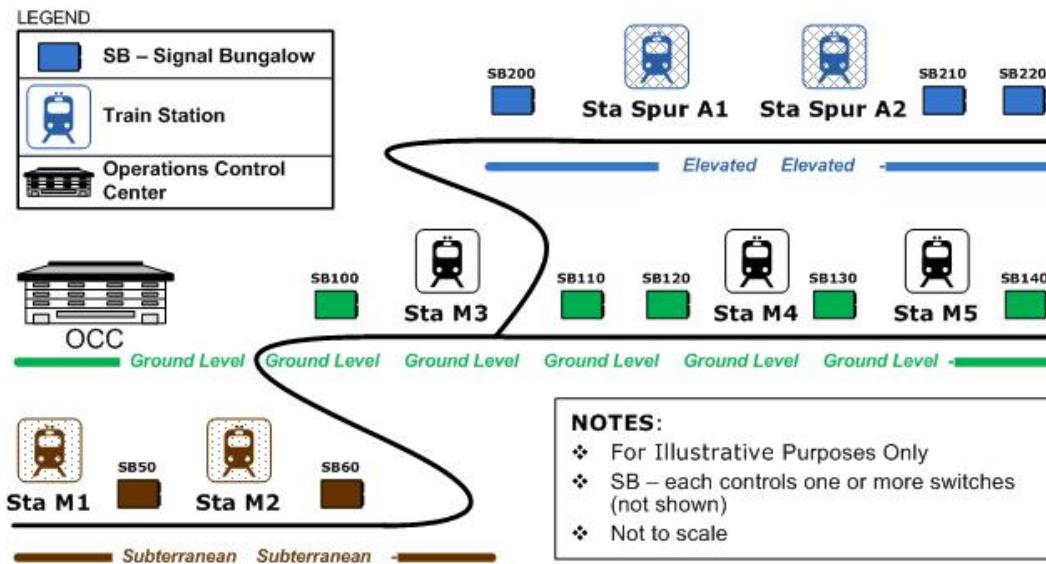
A manufacturing site, regardless of its size, can for the most part restrict who has access to it through physical means. Transportation system assets, on the other hand, are out in public. Physical security exists—much of it to keep the public from dangerous areas, such as power sources, third rails, overhead wiring, the path of trains and so on—but it is impossible to keep determined individuals away from the transportation system's assets. Transit agencies need to focus on prevention and detection of people accessing key areas, such as signal bungalows, wayside equipment and communication bays.

3.6 An example transit system

Consider an example transportation system (**Figure 5**). This is a fixed block model that has stations below ground, at-grade and elevated. There is a main line with several stations and a spur with two stations. There is an operations control center. Each station has its own equipment rooms, and along the track there are signal bungalows to control signals, switches, interlocking and road crossings. There are signals along the track, and fares are collected at each station. (For now, the maintenance yard will not be addressed.)

FIGURE 5
Example Rail Transit System

Example Transit System – Rail – Fixed-Block Signaling



3.6.1 Use of the example system

The transportation system shown in **Figure 5** will be used as a basis for many of the discussions in this document. This should be considered a fully functioning transportation system. It has employees, contractors, passengers, vendors and others present on the premises. It has parking lots for cars, station platforms, announcement and public information displays, advertising, fare collection systems, ticket sales, vending, trash, lighting, heat and air conditioning, emergency phones, hazard detection (fire, gas, water, seismic, biological), surveillance systems, restricted areas, locked doors, electric access card areas, equipment rooms, people movers (escalators/elevators), electrical panels, traction power systems, regular and emergency communications and much more.

3.7 Applying Defense-in-Depth to a model transit system

In the model transit agency, assume that the staff is also divided into separate divisions or reporting groups. This discussion will focus on the signals and communications group, track maintenance, fire response, life safety and the operations group. In addition, there are other groups for public relations, system police, IT, accounting and many others.

3.7.1 Putting it all together

Now that the model transit system—seven stations, two lines, and a typical staff organization—is defined, it's time to consider how this system can keep moving people in a predictable and safe manner. Although fare systems are important—protecting cash and passengers' personal identifying information—from the point of control and communications security, the most critical zones are the SCSZ and the FLSZ. (SCSZ is used for train signaling and communications. FLSZ systems are used to detect and remediate fire, smoke and other life safety concerns.)

3.7.2 Cybersecurity risk zones for rail transit

Table 9 and **Table 10** 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, a thorough risk assessment considering these unique requirements and resultant zones should be conducted. (An example would be for a full CBTC system).

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

TABLE 9
List of Zones (APTA Enterprise Cyber Security Work Group)

External Zone	The external zone includes Internet-accessible services, remote operations and facilities, and remote business partners and vendors. It is <i>not</i> 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 10
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 3.7.3.
Safety Critical Security Zone (SCSZ)	See Section 3.7.3.

3.7.3 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, and there are business, accounting and engineering controls (checks and balances) 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 job. This is often referred to as “least privilege,” because each person has the least amount of privilege needed to do his or her job and no more. Each person has exactly the permission needed.

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 and 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

3.7.4 Defining zones (system categories)

For each function and system used by a transit agency, the transit agency should assign it to exactly one zone. Some functions, due to their nature, are pre-assigned to a zone and may never be assigned to another zone. For other functions, an agency may choose the appropriate zone, based upon the circumstances of its transit system. Ventilation systems, depending upon their purpose, may be assigned to either the OCSZ or to the FLSZ. How does the agency choose? If the agency has only above-ground train stations with no need for emergency ventilation, it may assign ventilation systems to the OCSZ, but if it has below-ground train stations, it should assign the emergency ventilation portion of the ventilation system to the FLSZ.

Example: Vital rail signaling, interlocking and ATP should be in the SCSZ. For traction power in a station, controlling the power should be assigned to the OCSZ, while the traction power emergency cut-off (blue-light) system and protective relaying should be assigned to the FLSZ. These systems should not be in the Enterprise Zone, External Zone or SCSZ.

3.7.5 Cybersecurity zones across a large physical space

It's clear that security zones may be spread out across many physical locations. To be cyber-secure, the transit agency must find a way to implement the security zones across this vast space and to also control the physical access and permissions to these critical systems across the physical locations.

Figure 6 gives a detailed look at the allocation of these security zones across physical locations.

FIGURE 6

Model Zone Chart for Transit Systems

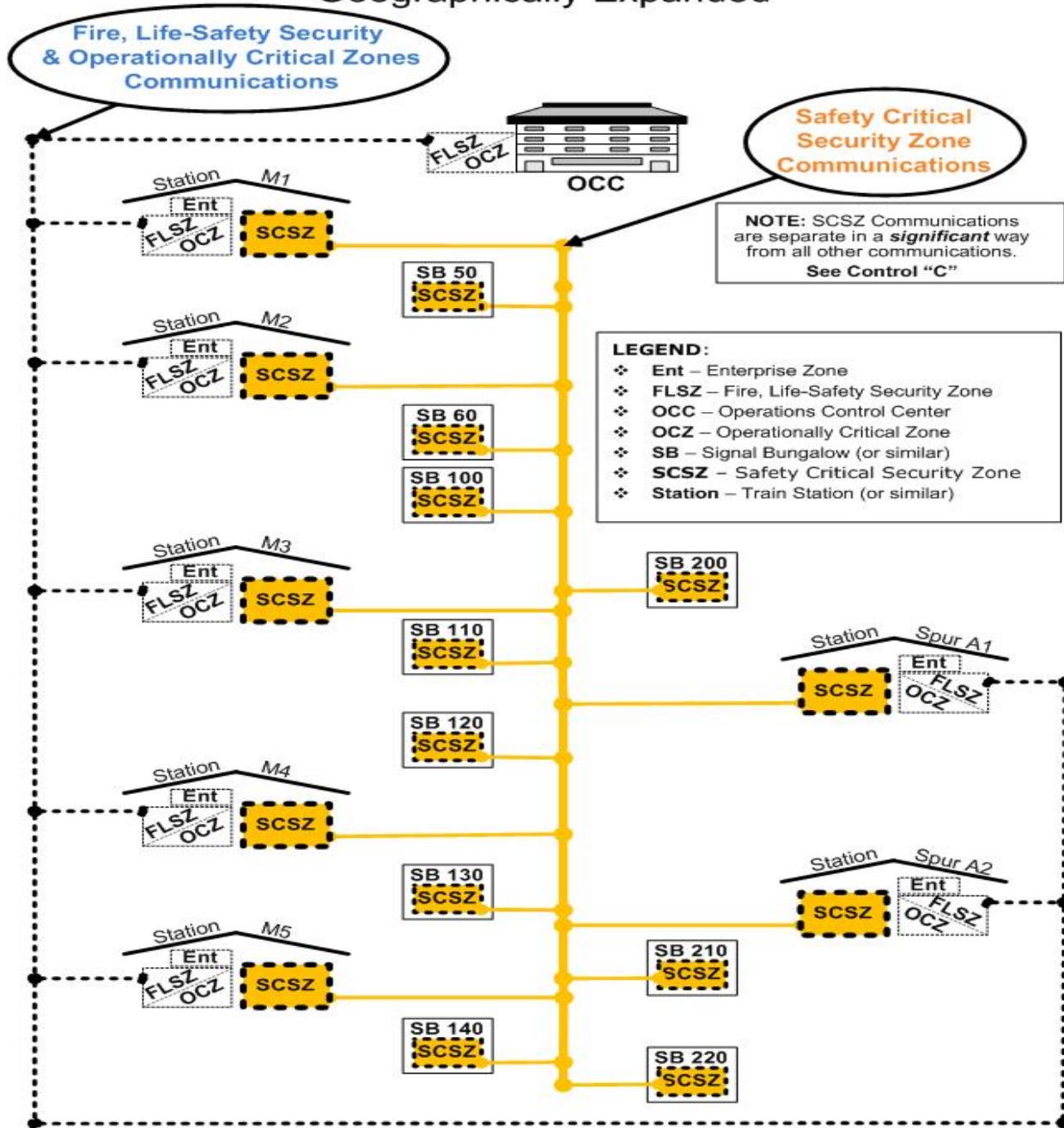
Model Control & Communication System Categories

EXTERNAL ZONE:	<input type="checkbox"/> N/A  OCC	<input type="checkbox"/> N/A  Train station / Station Equipment Room	<input type="checkbox"/> N/A  SIGNAL BUNGALOW – or equivalent
 EN	<input type="checkbox"/> Access Control System <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> Credit Card Processing <input type="checkbox"/> Logging	 EN	<input type="checkbox"/> Access Control / Intrusion Detection <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> Passenger information system <input type="checkbox"/> CCTV
 OC	<input type="checkbox"/> Dispatch / ATS <input type="checkbox"/> Non-Emergency Voice Communications <input type="checkbox"/> SCADA	 OC	<input type="checkbox"/> Traction Power <input type="checkbox"/> PA System – Passenger Information Display <input type="checkbox"/> Vertical Lift Devices <input type="checkbox"/> Tunnel pumping / draining
 FL	<input type="checkbox"/> Emergency Communications <input type="checkbox"/> Fire Alarm & Suppression Enunciators <input type="checkbox"/> Fire / Life-Safety, Emergency Ventilation Control <input type="checkbox"/> Status displays	 FL	<input type="checkbox"/> Emergency Ventilation Systems <input type="checkbox"/> Emergency Management Panel <input type="checkbox"/> Fire Detectors / Alarms / Suppression systems <input type="checkbox"/> Safety Critical Physical Intrusion Detection <input type="checkbox"/> Traction Power Emergency Cutoff <input type="checkbox"/> Traction Power Protection Relaying <input type="checkbox"/> Gas Detection <input type="checkbox"/> Mass Notification PA <input type="checkbox"/> Seismic Monitoring
 SC	<input type="checkbox"/> Vital CBTC	 SC	<input type="checkbox"/> Vital Signaling, ATP <input type="checkbox"/> Platform Gate Control
LEGEND		LEGEND	
 EN	Enterprise Network (Admin, IT, HR)	 FL	Fire, Life-Safety Security Zone
 OC	Operationally Critical Security Zone (Traction Power)	 SC	Safety Critical Security Zone
	Enterprise Zone Perimeter		Fire, Life-Safety Security Zone Perimeter
	Operational Critical Security Zone Perimeter		Safety Critical Security Zone Perimeter

Figure 7 illustrates how the SCSZ is connected along various rail lines and that it is separated from the FLSZ/OCSZ/Enterprise Zone in a significant way vis-à-vis control and communications security methods and communication.

FIGURE 7
Geographical Dispersion in a Rail System

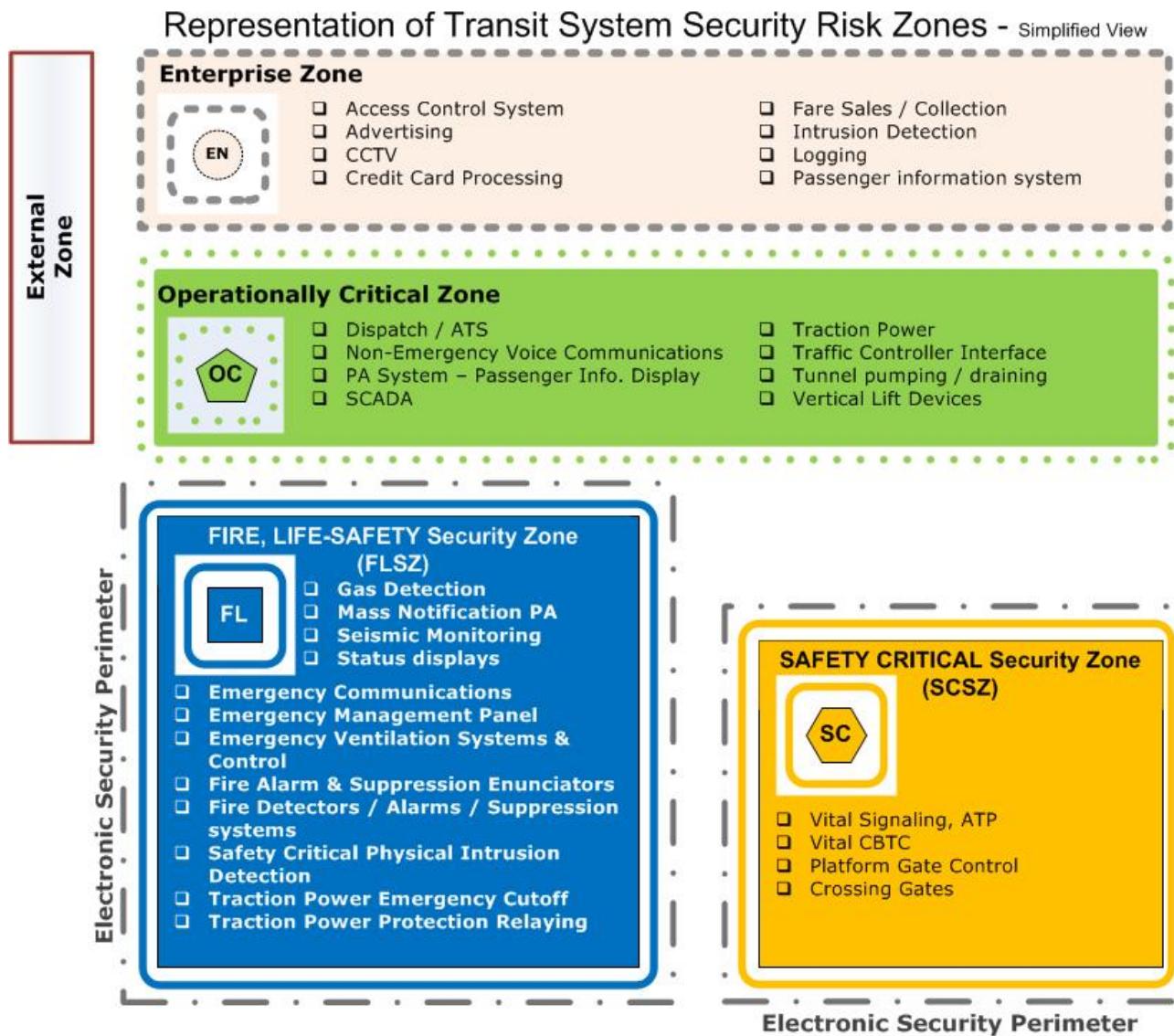
Example Transit System – Rail – Fixed-Block Signaling – Geographically Expanded



3.7.6 Representation of transit system security risk zones

Figure 8 shows our security zones in the aggregate, and how they relate to the functions needed by a typical transit agency. Note that the SCSZ and the FLSZ should have separate ESPs, Electronic Security Perimeters (**ESP**) as described in Section 4 of this document, and that each of the other zones need the appropriate level of protection for their zone (a topic that will be addressed in Part III of this series).

FIGURE 8
Transit System Security Risk Zones



3.7.6.1 System category rules

There is a careful balance between putting too much into the more secure zones while at the same time not giving extra opportunity for an attack. To ensure a properly protected system, only the most critical systems should be in the most critical zone.

There are supporting systems, communications and related features that, after careful risk analysis, may need to be included in the more secure zone. Putting something into a more secure zone should not be done lightly, but it must be done where necessary to achieve an acceptable level of risk.

NOTE: This *Recommended Practice* is based upon a typical, generic, transportation system. For agencies with different system requirements, a separate risk assessment resulting in modified zone definitions should be completed and documented.

3.7.7 General rules

This *Recommended Practice* gives a model for determining the zone for each function or process based upon the generic model system.

Warning: Do not combine the functions and services of one zone into another zone without proper mitigations. This may create covert channels that an attacker can use to control an agency's systems. For example, it is not good security practice to implement a clearly non-safety critical function into the SCSZ.

Perceived economies of scale or other business decisions often do not fully account for the risk and cost of mixing functions. It may make it impossible to enforce the necessary most-restrictive security controls across the entire zone to keep the transit system safe and secure.

In all cases the transit agency should document its choices and rationale.

3.7.7.1 Operationally Critical Security Zone

- **Should include:** traction power, ATS, dispatch
- **Should not include:** anything from SCSZ, External Zone or Enterprise Zone

3.7.7.2 Fire, Life-Safety Security Zone

- **Should include:** fire, hazard, monitors for seismic, biologics, poison gas, traction power emergency shutdown systems
- **Should not include:** anything from SCSZ, External Zone, Enterprise Zone

3.7.7.3 Safety Critical Security Zone

- **Should include:** all “vital” systems for signaling and interlocking, ATP
- **Should not include:** anything from other zones: External, Enterprise, OCSZ, FLSZ

3.7.8 An example of systems and the zone they belong in

Table 11 shows which zones make sense for some common categories.

TABLE 11

Zone Matrix

Category	Zones				
	External	Enterprise	OCSZ	FLSZ	SCSZ
Vital signaling					ONLY
Fare handling		ONLY			
Fire and safety				ONLY	
Traction power SCADA (non-emergency)			ONLY		
Non-emergency ventilation		Offices	Stations		
Emergency ventilation				ONLY	

In a networked system, clearly communications is involved in every zone. So as a category, communications cannot be restricted to solely one zone. This document gives guidance on how to segregate network traffic and gives several techniques to consider for separating communications functions into zones.

4. System security and minimum controls for Safety Critical Zones

4.1 Legend

The following pages expand and explain the recommended controls. Each page has this format. **Figure 9** explains the meaning of the headings.

FIGURE 9

Recommended Controls Legend

Ref #: Reference code. This will not change across versions				
		Version (version number): Initially 1.0. Each minor revision will increment the value by .1 (1.1, 1.2). Major revisions will increment the whole number (2.0, 3.0).		
		Aud (audience): Who must follow or use this control <ul style="list-style-type: none"> • TA: Transit Agency • VEND: Vendor • BOTH: Applies to everyone 		
		When: When does the control apply? <ul style="list-style-type: none"> • Now: Applies at date of issue • To Be Dev: To be developed (see note below) 		
Ref #	Version	Aud.	When	TITLE: [Title of control]
Reference: Primary:	CONTROL: [Details of control]			

NOTES:

- The “To be developed” designation for a security control indicates the security control text is informative, and that it will be developed after Part 2 is issued. It will be fully developed and then included in Part 3 of this Recommended Practice series (see Section 6.0), or in a future revision of Part 2. 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.

4.2 Overview

To partition the system according to the rules of the previous section, the security controls in **Table 12** should be applied. Generic drawings are supplied to indicate where each control should be applied.

TABLE 12
Overall Controls

Ref	Applies to:	Description	References and Citations	When to Apply
A	Both	The transit agency should draw electronic security perimeters around the SCSZ and FLSZ to separate them from each other and from the other zones.	NIST 800 -18, 53, 82	Now
B	Both	All network-routable interfaces connecting the SCSZ or FLSZ with a less-critical security zone should use an isolation device (defined below) to ensure security separation.		Now
C	Both	Separate fiber-optic strands or other acceptable isolation methods per control 4.2.3 should be required to connect physical separate SCSZ zones when using wide area networks (WANs) or local area networks (LANs).		Now

4.2.1 Electronic security perimeters around SCSZ and FLSZ

Ref #	Version	Aud.	When	TITLE: Electronic security perimeters around SCSZ and FLSZ
A	1.0	TA	Now	
Reference: SP 800-53 Primary:		CONTROL: The transit agency should draw electronic security perimeters around the SCSZ and FLSZ to separate them from each other and the other zones.		

Reason for control

Following the Defense-in-Depth strategy introduced in Section 3, higher security zones need to be behind perimeters in order to segregate it from lower zones.

Discussion

The following definition will serve to illustrate the systems included in SCSZ and FLSZ classification:

- **SCSZ:** A system that if inadvertently or deliberately sabotaged could cause an immediate threat to life safety (for example, electronic sabotaging of a vital signaling system could cause a train collision).
- **FLSZ:** A system whose primary function is to warn, protect or inform in the event of an emergency. For example fire alarms, emergency ventilation equipment, the physical intrusion detectors and alarms informing of a physical breach into a SCSZ perimeter. Sabotage, or serious malfunction, of this equipment could lead to a threat of life safety if an emergency were to occur.

Measures of effectiveness

- Audit of systems during design, implementation and operational phases would show proper categorization of safety-critical security equipment and the proper definition of the electronic security perimeters around each of the safety related zones (SCSZ and FLSZ).

Examples

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

4.2.2 Connecting security zones of different security levels

Ref #	Version	Aud.	When	TITLE: Connecting security zones of different security levels
B	1.0	TA	Now	
Reference: SP 800-53 Primary:		CONTROL: All network-routable interfaces connecting the SCSZ or FLSZ with a less-critical security zone should use an isolation device (defined below) to ensure security separation.		

Reason for control

The Defense-in-Depth strategy used in this *Recommended Practice* requires routable (TCP/IP based) network connections to have a device to allow authorized traffic and to prohibit unauthorized traffic between the SCSZ and FLSZ and other less-critical zones.

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 (see Appendix B for more information)

Measures of effectiveness

- Unauthorized network traffic is recognized and stopped at the Isolation Device

Examples

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

4.2.3 Physical separation for SCSZ data transmission

Ref #	Version	Aud.	When	TITLE: Separation for SCSZ data transmission over optical fiber or other medium
C	1.0	TA	Now	
Reference: SP 800-53 Primary:		CONTROL: Separate fiber-optic strands or other acceptable isolation methods per control 4.2.3 should be required to connect physical separate SCSZ zones when using wide area networks (WANs) or local area networks (LANs).		

Reason for control

There is a need to segregate safety-critical data as it travels between SCSZs separated by distance (for instance, from train stations to signal bungalows). Separation as described below should be provided.

This security control applies to optical fiber communication and where applicable below to copper wiring.

Discussion

There are at least two techniques to provide separation for WANs and LANs connecting physically separate WANs and LANs:

- Use a separate fiber or copper conductor for safety-critical security data.
- Use an equivalent optical technology that provides separation of data streams within the optical medium by use of different frequencies of light, as in wave-division multiplexing (WDM) or dense wave division multiplexing (DWDM).
- If the transit agency agrees, using a shared fiber or copper conductor for SCSZ data is permissible provided data integrity and authenticity is protected using cryptographic means (for instance using IPsec or similar protocols to protect the SCSZ data before blending with less critical OCSZ data)
 - Note: In Part 3, separation using other techniques, such as VLANs or MPLS, will be examined with the aid of attack modeling, and conclusions drawn as to their acceptability.

Measures of effectiveness

- Audit during design and implementation stages.

Examples

- **Acceptable:**
 - Separate fiber optic strand, or copper conductor.
 - optical technology providing equivalent data separation as described above
 - Cryptographic protection of SCSZ data on fiber or copper medium as described above
 - (See note in Discussion section above)
- **Not acceptable:**
 - Use of a dual-homed personal computer to bridge networks

4.3 Controls

Table 13 gives security controls applicable within the SCSZ and FLSZ Electronic Security Perimeters. Each control then has a dedicated page following the Table.

Before implementing any cyber security controls, a thorough analysis must be performed to ensure that the controls cannot adversely impact functions implemented in the SCSZ or FLSZ.

TABLE 13
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 SCSZs and FLSZs for people (employees, contractors, vendors and inspectors) as their role in the organization changes, including hire/fire or contract awarded/expired/terminated.	PS-4	Personnel Security	Now
4	Transit	SCSZ and FLSZ electronic equipment should be housed in a six-wall physical enclosure with two-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 SCSZ and FLSZ device.	CM-1	Configuration Management	Now
6	Transit	A process should exist to manage the changes to all SCSZ and FLSZ 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 SCSZ and FLSZ equipment, closing non-essential ports and services.	SA-1	System and Services Acquisition	Now
8	Transit	Block any unneeded USB, CD and other entry ports on SCSZ and FLSZ devices and equipment. Single-factor cyber authentication should be used on permitted ports.	SI-3 CM-7	System and Information Integrity; Configuration Management	Now

TABLE 13
Controls

Ref.	Applies to	Description	References and Citations (NIST SP 800-53 Appendix F)	NIST SP 800 Family	When to Apply
9	Transit	Bimonthly sweep for rogue wired or wireless devices attached to SCSZ and FLSZ control/communications networks.	AC-18	SI-4	Access Control; System and Information Integrity
10	Transit	Bimonthly check of SCSZ and FLSZ computers, network devices and other devices that use software for software that is unauthorized or questionable.	AU-12	CM-5	Audit and Accountability; Configuration Management
11	Transit	Use antivirus protection or software white-listing/file integrity checker on fixed/portable/mobile PCs that connect to SCSZ and FLSZ equipment.	SI-3	SC-7(9)	System and Information Integrity; System and Communications Protection
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
13	Both	A comprehensive patch management program should be set up with vendors for SCSZ and FLSZ commercial off-the-shelf (COTS) or proprietary software and firmware	SI-2		System and Information Integrity
14	Both	Yearly passive vulnerability check should be performed by an authorized and qualified outside agency.			Now
15	Both	On-site physical presence by qualified and authorized staff should be required to change software or executables on SCSZ and FLSZ equipment.	AC-17	MA-4	Access Control; Maintenance
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	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 SCSZ and FLSZ product used by transit.	CA-6		Security Assessment and Authorization
18	Vendor	Wireless communications security (to be developed)	SC-5	AC-18	System and Communications Protection; Access Control To Be Dev

TABLE 13
Controls

Ref.	Applies to	Description	References and Citations (NIST SP 800-53 Appendix F)		NIST SP 800 Family	When to Apply
19	Vendor	A tamper-resistant/evident “black box” should be installed locally or at a distance for SCSZ controllers such as vital PLCs for forensic uses. “Black box” to indicate all electronic accesses and changes.(to be developed)	AU-9		Audit and Accountability	To Be Dev
20	Vendor	Use host file integrity verification with cryptographic checksum on SCSZ and FLSZ controllers such as vital PLCs, where not precluded by large or complex file structures. (to be developed)	SI-7		System and Information Integrity	To Be Dev

4.3.1 Management responsibility

Ref #	Version	Aud.	When	TITLE: Management responsibility
1	1.0	TA	Now	
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.		

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.

Discussion

The senior executive is the official management person who authorizes operation of the SCSZ and FLSZ 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 SCSZ and FLSZ system security risks.

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

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.

Examples

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

4.3.2 Training program

Ref #	Version	Aud.	When	TITLE: Training program
2	1.0	TA	Now	
Reference: SP 800-53 Primary: AT-1 PM-9		CONTROL: Create a training program for employees, vendors and partners around control and communications security.		

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.

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 SCSZ and FLSZ 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,

Measures of effectiveness

- A training program exists that covers control and communications security for personnel who operate SCSZ and FLSZ equipment and/or physically access the SCSZ or FLSZ. 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.

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.

4.3.3 Access Control, Personnel

Ref #	Version	Aud.	When	TITLE: Access control, personnel
3	1.0	TA	Now	
Reference: SP 800-53 Primary: PS-4		CONTROL: Have methods and procedures in place to create, modify and remove access to SCSZs and FLSZs for people (employees, contractors, vendors, and inspectors) as their role in the organization changes, including hire/fire or contract awarded/expired/terminated.		

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.

Discussion

People need access to those systems that they are directly responsible for. Clear roles of 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.

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 a very short timeframe of the person being terminated for cause or put on leave.
- A similar process exists for the start and end of contractual relationships.

Examples

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

4.3.4 Access Control- Equipment

Ref #	Version	Aud.	When	TITLE: Access Control –Equipment
4	1 . 0	TA	Now	
Reference: SP 800-53 Primary: PE-1 PM-9		CONTROL: SCSZ and FLSZ electronic equipment should be housed in six-wall physical enclosure with two-factor authentication to access and warn on unauthorized physical access.		

Reason for control

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

Discussion

Two-factor authentication is an acceptable means of identity assurance in high-security situations that require personnel to provide two 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).

It is *not* the same as using the same access control method two times in a row (such as using the same key to open an outer and an inner door).

Measures of effectiveness

- Security audit

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

4.3.5 Configuration management

Ref #	Version	Aud.	When	TITLE: Configuration management
5	1.0	TA	Now	
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 SCSZ and FLSZ device.		

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.

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 where the transit agency ensures that the compatible software versions are installed and running on all SCSZ and FLSZ devices.

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

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 originate, 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.

Examples

- **Acceptable:**
 - Written procedures describing a configuration management system
- **Not acceptable:**
 - Ad hoc handwritten lists of software compatibilities; SCSZ filenames without a naming convention that positively identifies them, such as naming files “File1,” etc.

4.3.6 Configuration management, audit trail

Ref #	Version	Aud.	When	TITLE: Configuration management, audit trail
6	1.0	TA	Now	
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 SCSZ and FLSZ hardware and software with logs of the changes, including the purpose/rationale for the changes.		

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.

Discussion

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

Configuration change control includes changes to components of the SCSZ and FLSZ 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.

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 the approved level.
- An audit can quickly identify when a network device's software is *not* the approved level.

Examples

- **Acceptable:**
 - A documented change management procedure
- **Not acceptable:**

4.3.7 Security in procurement

Ref #	Version	Aud.	When	TITLE: Security in procurement
7	1.0	TA	Now	
Reference: SP 800-53 Primary: SA-1 SA-4 PM-9		CONTROL: Procurement documents to specify default hardening specification for SCSZ and FLSZ equipment, closing non-essential ports and services.		

Reason for control

SCSZ and FLSZ control and communications equipment is best delivered from the vendor with security pre-configured in at delivery time. TA purchasing needs a procurement process that includes language that will ensure that.

Discussion

Transit agency procurement documents should include requirements for vendors to:

- supply SCSZ and FLSZ 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 "Cyber Security Procurement Language for Control Systems" as revised (Revision 4, October 8, 2009) may be used as a reference.

Measures of effectiveness

- Audit of "as-received" SCSZ and FLSZ equipment.

Examples

- **Acceptable:**
 - Adding a procurement security specification to RFP and Purchase agreements
- **Not acceptable:**
 - Leaving unnecessary ports and services activated as a default configuration.

4.3.8 Physical Security, Attachments

Ref #	Version	Aud.	When	TITLE: Physical security, attachments
8	1.0	TA	Now	
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 SCSZ and FLSZ devices and equipment. Single-factor cyber authentication should be used on permitted ports.		

Reason for control

A transit agency needs to prevent unauthorized connections to SCSZ 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.

Discussion

Security attacks are often done by connecting an infected device to a secure device or network. To prevent the attachment of unauthorized devices, you should eliminate the ability to attach the device if that port is unneeded. 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 consideration should be placed into device control mechanisms, mobile access control mechanisms and device encryption.

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.

Examples

- **Acceptable:**
 - Unneeded ports are blocked
- **Not acceptable:**
 -

4.3.9 Unauthorized devices, detection

Ref #	Version	Aud.	When	TITLE: Unauthorized devices, detection
9	1.0	TA	Now	
Reference: SP 800-53 Primary: AC-18 SI-4 AC-3 AC-18 IA-2 IA-3 IA-8 SI-4		CONTROL: Bimonthly sweep for rogue wired or wireless devices attached to SCSZ and FLSZ control/communications networks.		

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.

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 so 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 bimonthly scan 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 proven not to have negative an operational impact on the system.

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.

Examples

- **Acceptable:**
 - Check for unauthorized devices done considering possible negative responses of the control network to the scan or sweep method used
- **Not acceptable:**

4.3.10 Unauthorized Software, Compliance

Ref #	Version	Aud.	When	TITLE: Unauthorized software, compliance
10	1.0	TA	Now	
Reference: SP 800-53 Primary: AU-12 CM-5		CONTROL: Bimonthly check of SCSZ and FLSZ computers, network devices, and other devices that use software for software that is unauthorized or questionable.		

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.

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 bimonthly 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.

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;
 - remove software found to be unauthorized; and
 - find a way to mitigate the software in question, such as remove it to a less-sensitive portion of the network.

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.

4.3.11 Active malware protection

Ref #	Version	Aud.	When	TITLE: Active malware protection
11	1.0	TA	Now	
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 PC's that connect to SCSZ and FLSZ equipment.		

Reason for control

Cyber-attacks 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.

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.

Measures of effectiveness

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

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

4.3.12 Operations Control Center, Alternate

Ref #	Version	Aud.	When	TITLE: Operations control center, alternate
12	1.0	TA	Now	
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.		

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.

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 only partially operational through being fully operational. There may be unexpected communication paths between the primary and alternate OCCs.

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.

Examples

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

4.3.13 Patch management

Ref #	Version	Aud.	When	TITLE: Patch management
13	1.0	BOTH	Now	
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 SCSZ and FLSZ commercial off the shelf (COTS) or proprietary software and firmware.		

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 Commercial off the Shelf firmware and software that is part of the Vendor's supplied equipment.

Discussion

SCSZ and FLSZ systems have various components, some 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 SCSZ and FLSZ 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 an exploit 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.

Measures of effectiveness

- A patch management program exists for each vendor's SCSZ and FLSZ products.
- 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.

Examples

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

4.3.14 Security compliance, validation

Ref #	Version	Aud.	When	TITLE: Security compliance, validation
14	1.0	VEND	Now	
Reference: SP 800-53		CONTROL: A yearly passive vulnerability check should be performed by an outside authorized and qualified agency.		
Primary:				

Reason for control

A transit agency should have an outside agency assess, at least annually, its vulnerability to cyber-attack in the SCSZ and FLSZ. 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 signoff on the results of the assessment and put mitigations in place as necessary to keep the transit system safe and secure.

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 cyber-attack as can be done reasonably.

Measures of effectiveness

- A contract exists for this activity.

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.

4.3.15 Access Control, safety-critical equipment

Ref #	Version	Aud.	When	TITLE: Access Control, safety-critical equipment
15	1.0	BOTH	Now	
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 SCSZ and FLSZ equipment.		

Reason for control

Safety-critical equipment needs to be protected to a greater extent than other equipment. Restricting both physical and electronic access is important to safety and security.

Discussion

Whenever a SCSZ or FLSZ device is being accessed, it should be done in-person. This may be accomplished by using two-factor authentication to access the physical space where the device is located, followed by at least single-factor cyber authentication to modify the SCSZ equipment.

Measures of effectiveness

- Audit

Examples

- **Acceptable:**
 - On-site physical presence.
- **Not acceptable:**
 - Remote change of safety-critical executable files from a distance using a web interface or telephone modem.

4.3.16 Audit and Accountability, logs

Ref #	Version	Aud.	When	TITLE: Audit and accountability, Logs
16	1.0	TA	To Be Dev	
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. (to be developed)		

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.

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.

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.

Examples

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

4.3.17 Responsibility, vendor product management

Ref #	Version	Aud.	When	TITLE: Responsibility, vendor product management
17	1.0	VEND	Now	
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 control and communications security activities for each SCSZ and FLSZ product used by transit.		

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.

Discussion

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

Measures of effectiveness

- Transit agency customer satisfaction.

Examples

- Acceptable:**
 - Control and communications security knowledgeable experts at vendor customer service locations who know both the equipment in question *and* cyber security.
- 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.

4.3.18 Communications, wireless security

Ref #	Version	Aud.	When	TITLE: Wireless security
18	1.0	VEND	To Be Dev	
Reference: SP 800-53 Primary: SC-5 AC-18 SC-1 AC-1		CONTROL: Wireless communications security (to be developed)		

Reason for control

Safety-critical systems must be highly protected. Wireless communications that have direct access to a safety-critical system must also be highly protected. The best protection available today is a VPN, which itself uses encryption.

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.

There is a history of today's IEEE 802.11 Wi-Fi–acceptable protocols being unacceptable tomorrow. (e.g., Wired Equivalent Privacy [WEP]). The agency should determine which protocols are appropriate and use only those. If any equipment uses a now-compromised protocol, it must be replaced.

Other communications protocols that are available should be investigated to ensure that the procurement includes requirements to meet acceptable encryption guidelines and are capable of performing mutual authentication to ensure that the devices/users are authorized to connect to the system wirelessly.

Measures of effectiveness

- VPN definition exists.
- The intervening communication “pipes” are also protected from Man-in-the-Middle attacks.

Examples

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

4.3.19 Forensic device for SCSZ controller, audit trail

Ref #	Version	Aud.	When	TITLE: Forensic device for SCSZ controller, audit trail
19	1.0	VEND	To Be Dev	
Reference: SP 800-53 Primary: AU-9 AC-3 AC-6		CONTROL: A tamper-resistant/evident “black box” should be installed locally or at a distance for SCSZ controllers such as vital PLCs for forensic uses. “Black box” to indicate all electronic accesses and changes. (to be developed)		

Reason for control

Transit agencies need a way to know what happened in every situation, regardless of environmental problems or attempts to tamper with critical equipment, especially if that equipment cannot log and save an audit trail of changes made to it.

Discussion

This control is intended to provide an audit trail and recording of all changes made to vital PLCs and related equipment that do not usually have their own logging ability. The information will be/may be used to confirm changes made to the PLC, especially to determine if a violation or corruption occurred.

Measures of effectiveness

Examples

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

4.3.20 Validate PLC and controller integrity

Ref #	Version	Aud.	When	TITLE: Validate PLC and controller integrity
20	1.0	VEND	To Be Dev	
Reference: SP 800-53 Primary: SI-7 SI-1		CONTROL: Use host file integrity verification with cryptographic checksum on SCSZ and FLSZ controllers such as vital PLCs, where not precluded by large or complex file structures. (to be developed)		

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.

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 SCSZ 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.

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.

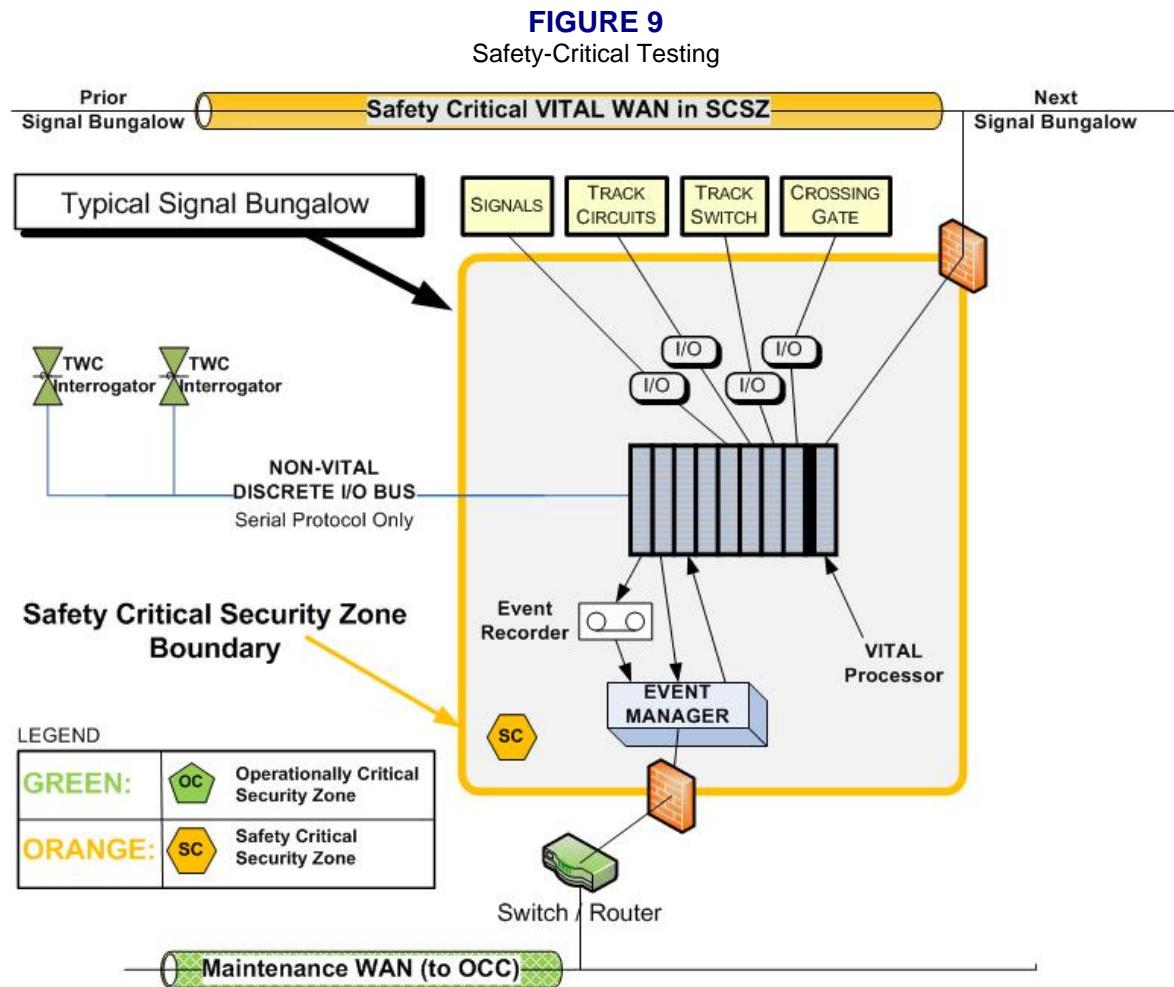
Examples

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

5. Applying security controls to zones

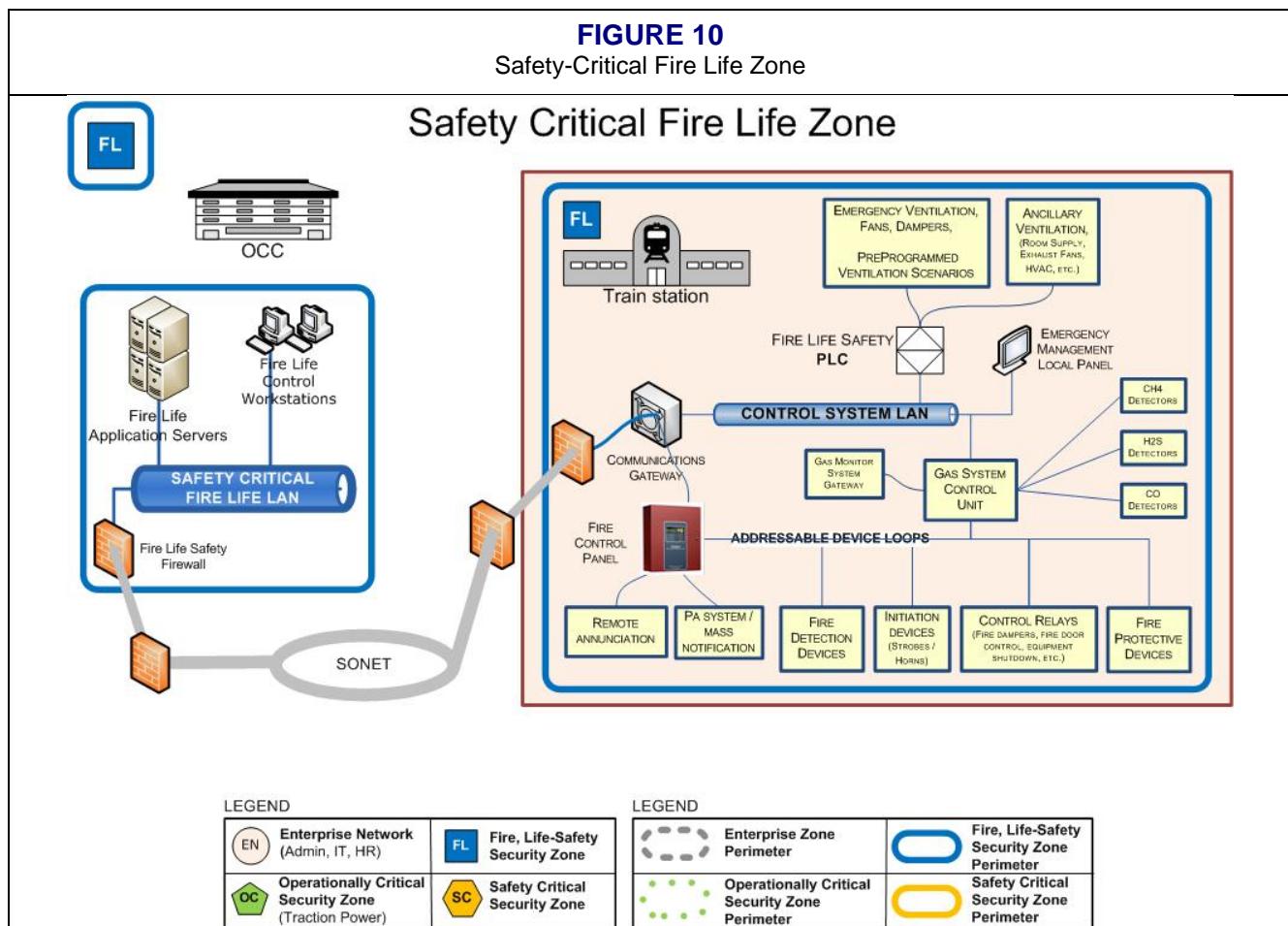
5.1 Safety-critical signaling

Figure 9 illustrates the application of SCSZ requirements to a generic signaling bungalow using a block signaling approach. Note that the network connections are consistent with **Figure 8**. Note also that the firewalls (isolation devices, per Section 4.2.2) are protecting the routable network connections.



5.2 Safety-critical Fire Life Safety

Figure 10 illustrates the application of Part II security controls to a generic FLSZ. Note the electronic security perimeter around the fire, life-safety LANs in the OCC and the train stations, and that they are both protected with firewalls (isolation devices, per Section 4.2.2).



6. Preview of the Recommended Practice series, Part III

Section 1.2 gives the breakdown of the three parts of the APTA *Recommended Practice* series “Securing Control and Communications Systems in Transit Environments.” This section gives a preview of topics that will be covered in Part III of the series. The main topics will be the following:

- Protecting the OCSZ
- Securing the train line control and communications systems
- Applying attack modeling for rail transit control and communications systems

6.1 Protecting the OCSZ

Per Sections 3.7.2 and 3.7.3, the OCSZ covers systems needed to run and maintain normal revenue operations, but excludes the safety-critical and fire-life safety systems in the SCSZ and FLSZ. Referring to **Figure 6**, this includes systems in the control room and train stations, such as dispatch, SCADA, ATS, traction-power SCADA, etc. These systems need cyber-protection. A failure of these systems normally results in stopped trains or a non-operational railway. The cyber-protection requirements for this zone are generally less strict than the protection for the SCSZ or the FLSZ. The zone does, however, need control and communications security measures, such as zone isolation and protection.

6.2 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:

- 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 in advance how the above systems will be segmented into security zones in Part III.

6.3 Attack modeling for transit control and communications systems

Attack modeling is a relatively new discipline within the area of control system security. It was popularized as a necessary step in Microsoft's 2006 manual for its Software Development Life Cycle (SDLC) under the name "Threat Modeling". There are a variety of methods to do attack modeling today, using procedures known as STRIDE; Confidentiality, Integrity, and Availability (CIA); and DREAD.

The procedure developed by APTA for rail transit attack modeling has the following steps:

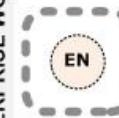
- Characterize the system assets and networked connections.
- Describe normal and intermittent sequence of operations of the system, along with data flow diagrams (DFD).
- Decompose operations into sequence diagrams.
- Identify the range of attacks (insider, outsider, accidental error).
- Build attack trees to describe and examine these attacks.
- Analyze vulnerabilities.
- Describe and rate the risks.
- Identify risk cutoff level.

The APTA attack-modeling procedure will be described in Part III, and an example given.

Appendix A: Control and communications system account worksheets

The following worksheets are to guide a transit agency in placing a functional area into the appropriate security zone.

Operations Control Center

Control & Communication System Worksheet - OCC		
OCC	Designated	Optional
EXTERNAL ZONE:  Enterprise Network (EN)	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
Enterprise Zone 	<input type="checkbox"/> Access Control System <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> Credit Card Processing <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> Logging <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
Operationally Critical Zone 	<input type="checkbox"/> Dispatch / ATS <input type="checkbox"/> Non-Emergency Voice Comm. <input type="checkbox"/> SCADA <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> CCTV monitoring of entrances / exits <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
Fire, Life-Safety Security Zone 	<input type="checkbox"/> Emergency Communications <input type="checkbox"/> Fire Alarm & Suppression <input type="checkbox"/> Enunciators <input type="checkbox"/> Emergency Ventilation Control <input type="checkbox"/> Status Displays <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
Safety Critical Security Zone 	<input type="checkbox"/> Vital CBTC <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

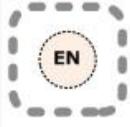
LEGEND

	Enterprise Network (Admin, IT, HR)		Fire, Life-Safety Security Zone
	Operationally Critical Security Zone (Traction Power)		Safety Critical Security Zone

LEGEND

	Enterprise Zone Perimeter		Fire, Life-Safety Security Zone Perimeter
	Operationally Critical Security Zone Perimeter		Safety Critical Security Zone Perimeter

Train station

Control & Communication System Worksheet - Station			
		Designated	Optional
 Train station APTA ENTERPRISE WORK GROUP EXTERNAL ZONE:	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
 Enterprise Zone APTA CONTROL & COMMUNICATION SECURITY WORK GROUP	<input type="checkbox"/> Access Control <input type="checkbox"/> Intrusion Detection <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> PA System <input type="checkbox"/> Passenger Information Displays <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
 Operationally Critical Zone APTA CONTROL & COMMUNICATION SECURITY WORK GROUP	<input type="checkbox"/> Traction Power <input type="checkbox"/> PA-Passenger Information Display <input type="checkbox"/> Vertical Lift Devices <input type="checkbox"/> Tunnel Pumping / Draining <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
 Fire, Life-Safety Security Zone APTA CONTROL & COMMUNICATION SECURITY WORK GROUP	<input type="checkbox"/> Emergency Ventilation Systems <input type="checkbox"/> Emergency Management Panel <input type="checkbox"/> Fire Detectors/Alarms/Suppression <input type="checkbox"/> Gas Detection <input type="checkbox"/> Mass Notification P A <input type="checkbox"/> Safety Critical Physical Intrusion Detection <input type="checkbox"/> Seismic Monitoring <input type="checkbox"/> Traction Power Emergency Cutoff <input type="checkbox"/> Traction Power Protection Relaying <input type="checkbox"/> _____	<input type="checkbox"/> HVAC <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
 Safety Critical Security Zone APTA CONTROL & COMMUNICATION SECURITY WORK GROUP	<input type="checkbox"/> Vital Signaling, ATP <input type="checkbox"/> Platform Gate Control <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> N/A	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	
	<input type="checkbox"/> _____	<input type="checkbox"/> _____	

LEGEND

 EN	Enterprise Network (Admin, IT, HR)	 FL	Fire, Life-Safety Security Zone
 OC	Operationally Critical Security Zone (Traction Power)	 SC	Safety Critical Security Zone

LEGEND

	Enterprise Zone Perimeter		Fire, Life-Safety Security Zone Perimeter
	Operationally Critical Security Zone Perimeter		Safety Critical Security Zone Perimeter

Signal hut

Control & Communication System Worksheet – Signal Bungalow

		Designated	Optional
SIGNAL BUNGALOW			
APTA ENTERPRISE WORK GROUP	EXTERNAL ZONE:	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A
	Enterprise Zone	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A
APTA CONTROL & COMMUNICATION SECURITY WORK GROUP	Operationally Critical Zone	<input type="checkbox"/> Traffic Controller Interface <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> N/A
	Fire, Life-Safety Security Zone	<input type="checkbox"/> Safety Critical Physical Intrusion Detection <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> N/A
	Safety Critical Security Zone	<input type="checkbox"/> Vital Signaling, ATP <input type="checkbox"/> Crossing Gates <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	<input type="checkbox"/> N/A

LEGEND

	Enterprise Network (Admin, IT, HR)		Fire, Life-Safety Security Zone
	Operationally Critical Security Zone (Traction Power)		Safety Critical Security Zone

LEGEND

	Enterprise Zone Perimeter		Fire, Life-Safety Security Zone Perimeter
	Operational Critical Security Zone Perimeter		Safety Critical Security Zone Perimeter

Appendix B: Out-of-Scope Item Discussion

This appendix gives guidance for two topics that are out-of-scope for this RP and are of interest to transit agencies and vendors:

B.1 How to Approach Security Retrofits for Legacy Systems

[Reference Section: 1.2.2 - Defining a Security Zone Architecture and Protecting the Safety-Critical Zone]

B.1.1 Preliminary suggestions and selected references

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:

- B.1.1.1 Extra protection around the perimeter of these devices, such as insulating these devices from external connections
- B.1.1.2 Increased use of personnel or physical security measures as compensating or mitigating controls

B.2 Security Control – How to provide isolation

[Reference: Section 4.2.2 - 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”

B.2.1 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 4.3.5), use of antivirus or whitelisting software (Section 4.3.10), and detecting unauthorized software (Section 4.3.10).

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:

- B.2.1.1 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
- B.2.1.2 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

References

- American Public Transportation Association *Recommended Practice*, “Securing Control and Communications Systems in Transit Environments,” APTA RP-CCS-1-RT-001-10, July 2010.
<http://www.aptastandards.com/Documents/PublishedStandards/Security/tabcid/329/language/en-US/Default.aspx>
- CENELEC standard EN 50159 “Railway Applications - Communication, Signalling 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,” ANSI/ISA Standard 99.00.01, 2007.
- International Society of Automation, “Security for Industrial Automation and Control Systems: Part 2: Integrating Security into the Manufacturing and Control Systems Environment,” ANSI/ISA Standard 99.00.02, 2007.
- International Society of Automation, “Security Technologies for Industrial Automation and Control Systems,” ANSI/ISA Technical Report TR99.00.01, 2007.
- National Institute of Standards and Technology (NIST), “Risk Management Guide for Information Technology Systems,” July 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- National Institute of Standards and Technology (NIST), “Recommended Security Controls for Federal Information Systems and Organizations,” Revision 3, August 2009, includes updates from May 1, 2010.
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>
- Also see: [sp800-53-rev3-updated-errata_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-updated-errata_05-01-2010.pdf)
- 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,” final, June 2011. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- 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

APTA-SS-CCS-RP-002-13 Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

U.S. Department of Homeland Security National Cyber Security Division, “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” October 2009. http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf

U.S. Department of Homeland Security National Cyber Security Division “Recommended Practice for Patch Management of Control Systems”, December 2008 http://www.us-cert.gov/control_systems/practices/documents/PatchManagementRecommendedPractice_Final.pdf

Definitions

automatic train protection (ATP): A wayside and/or on-board 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 of 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.

DREAD: A Microsoft risk-assessment technique that categorizes a threat by evaluating it in each of five categories: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. The sum of all of the ratings is used as the overall rating of the threat. The highest numbers indicate the highest threats.

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, 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 cyber-attack 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 notification, 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.

Recommended Practice: An APTA Recommended Practice represents a common viewpoint of those parties concerned with its provisions. The application of a Recommended Practice is voluntary.

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.

STRIDE: Defines a Microsoft method to classify computer security threats. The acronym stands for Spoofing of an id, Tampering with data, Repudiation, Information disclosure (breach), Denial of service, and Elevation of privilege.

track circuit: An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.

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.

vector (for cyber-attack): The path an attacker takes to attack a network. (This term is borrowed from biology, where disease is traced from its origin through the various carriers and paths taken to infect the victim).

virtual local area network (VLAN): A method to connect devices, at ISO Layer 2, that communicate on a network as if they were on a separate network segment, much as what a router would provide at Layer 3. It is most commonly implemented using IEEE 802.1Q.

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-programmable logic controller (vital-PLC): A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.

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
APTA	American Public Transportation Association
ATP	automatic train protection
ATS	automatic train supervision
CBT	Computer Based Training
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
CO₂	carbon dioxide
COTS	commercial-off-the-shelf
CRC	cyclic redundancy check
CSSP	Control Systems Security Program
DHS	U.S. Department of Homeland Security
DWDM	dense wave division multiplexing
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
NSA	U.S. National Security Administration
NERC	North American Electric Reliability Corporation
NERC-CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
OCC	operations control center
OCSZ	Operationally Critical Security Zone
PC	personal computer
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
WDM	wave-division multiplexing
WEP	Wired Equivalent Privacy