Securing Control and Communications in Rail Transit

Control & Communications Security Working Group

ICSJWG
Long Beach, CA
October 2011

Dave Teumim, CISSP
Teumim Technical, LLC

Annie McIntyre
Ardua Strategies Inc.

AMERICAN PUBLIC TRANSPORTATION ASSOCIATION

APTA Standards Development Program
Lead the Way

Topics of Discussion

APTA Standards Development Program
Lead the Way

- Overview of APTA Cyber Security Efforts
- The Control and Communications Security Working Group
- Threats and Consequences with Rail Transit
- Defining Safety/Security Critical Zones in Other Sectors
- Defining Safety/Security Critical Zones for Rail
- Assembling Recommended Practice ,Part 2

www.apta.com

APTA Standards Development Program
Lead the Way

American Public Transportation Association

Search

Home | About Us | Published Documents | Standards Programs | Contact Us |

American Public Transportation Association Standards Development Program

A Program of the American Public Transportation Association

APTA is a nonprofit international association of over 1,500 public and private member organizations including transit systems and commuter rail operators; planning, design, construction and finance firms; product and service providers; academic institutions, transit associations and state departments of transportation. APTA members serve the public interest by providing safe, efficient and economical transit services and products. Over ninety percent of persons using public transportation in the United States and Canada are served by APTA members.

Standards have become an important program activity at APTA and in the public transportation industry. APTA, through its policy and planning committees, has played a major role in creating active working structures within the organization focused on the development of standards. Hundreds of industry volunteers serving on numerous working committees have developed standards for bus, rail transit and commuter rail operations, maintenance, procurement and ITS. These consensus based standards are making a real difference to the management and operations of these organizations. These standards are now being used to achieve operational efficiencies and safety improvements in services, facilities and vehicles.

Login

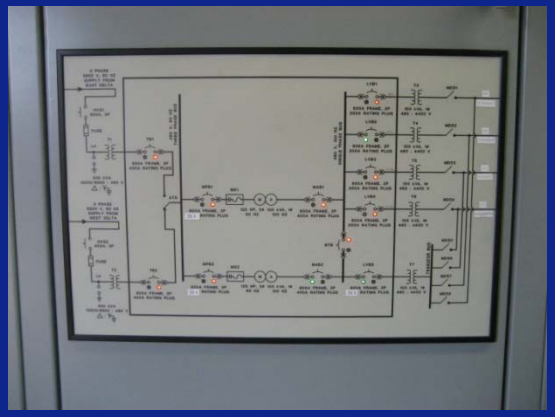
Join a Workgroup

Upcoming Events

Event Start	Title
1/10/2008 8:00 AM	Infrastructure Security WG - Newport Beach, CA (Infrastructure Security Calendar)
1/10/2008 8:30 AM	Call Center WG - Tampa (Paratransit Call Center Calendar)
1/17/2008 8:30 AM	Bus Op WG (Operator Training Calendar)

APTA Cybersecurity Working Groups

Control and Communications Security WG
Operational Systems (SCADA, Traction Power, Signaling, etc)
Established 2007



Enterprise Cyber Security WG (CIO/ IT Systems (business, revenue, and third party systems)
Established 2011

The APTA Control and Communications Security Working Group Members

- Transit Agencies
  - Toronto Transit
  - LA Metro
  - SEPTA
  - Miami-Dade
  - DART
- Government
  - Federal Railroad Administration
  - DHS CSSP
  - DHS TSA
  - Idaho National Labs
  - DOT Volpe Center
- Vendors
  - Ansaldo
  - Phoenix Contact
  - GE Transportation
  - Transdyn
  - Siemens
  - Horton Automation
  - Ruggedcom
- Consultants
  - NYRT
  - Teumim Technical, LLC
  - Weber Consulting

CCSWG Recommended Practice Part 1

- Issued July 2010
- RP Covers:
  - Introduction
  - Description of Control and Communications Systems
  - Getting organized for Control Security
  - Risk Assessment and Management
- Draws content from other standards, tailored for the rail transit industry

Typical Railway Systems

What's the Least that Could Happen ?

Hackers libel Canadian PM on train signs

By John Leyden "The Register" May 3, 2006

An unidentified ne'er-do-well broke into systems controlling electronic signs on Toronto's westbound Lakeshore GO Transit train to substitute transport updates for banners mocking the Canadian political leader.

What's the Worst That Could happen ?

Schoolboy hacks into city's tram system in Lodz, Poland with infra-red device

gazeta Łódź 14-latek wykolejał tramwaje
Fot. Sergiusz Pęczek / AG

From The Register, Jan 2008

Severity of Consequences

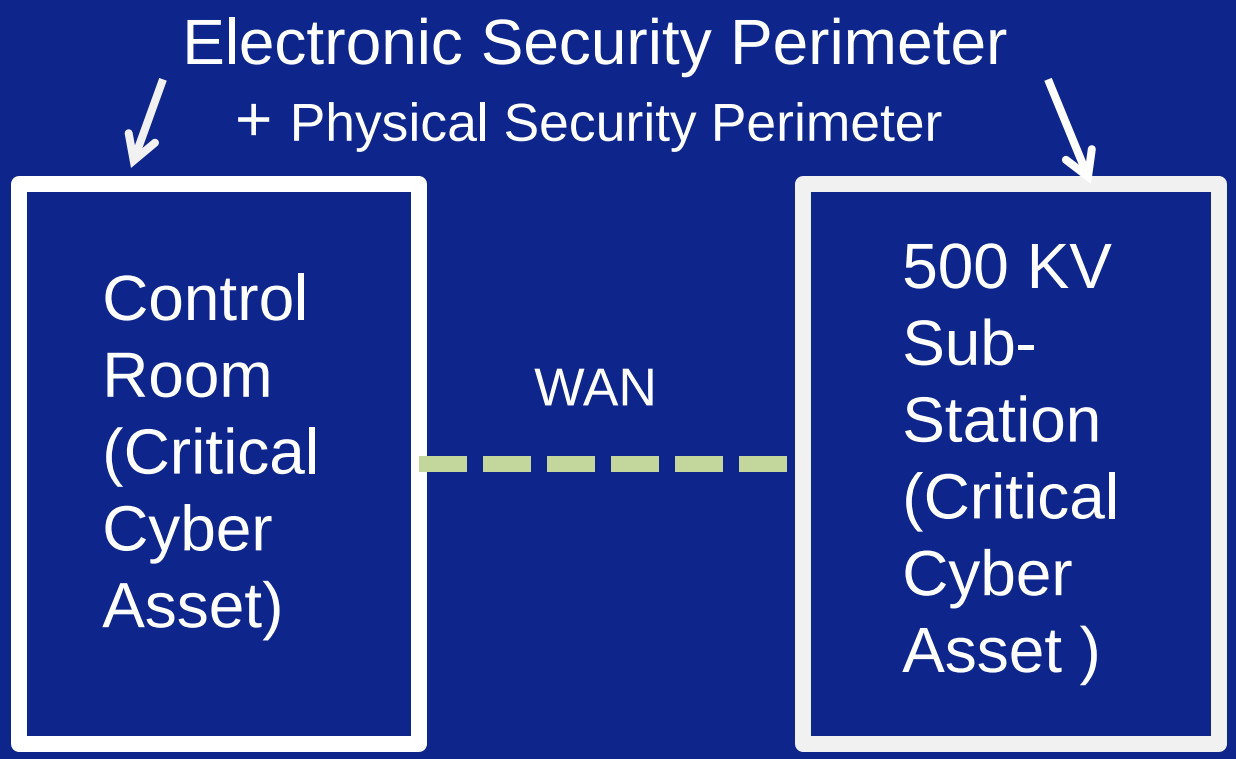
Severity of Consequences of Cyber Sabotage

- **Signaling, Interlocking and Fire/Life Safety**
  - Safety-Critical
- **SCADA, Traction Power, Fare Collection**
  - Operations-Critical
- **Passenger Information Display**
  - Passenger Convenience (Train Arrival Info)

Defining the Critical Zones (Safety/Security) in Other Sectors

- Electricity Generation, Transmission (NERC-CIP)
- Nuclear Generation (NRC Regulatory Guide 5.71)
- Pipeline/Oil & Gas Transport (in DOT High Consequence Areas)

Electric Sector (NERC – CIP)



Focus in on Transmission Grid Security

Nuclear Generation (NRC 5.71)

<u>Critical Digital Assets</u>
-Safety
-Security
-Emergency Prep
-Safety, Security
Support Systems

(Layer 4 Systems)

Boundary, with one way flow of information)

Pipeline/Oil & Gas Transportation Sector

Critical Zones:

- Control center
- Pump stations
- Field sites
- Ports
- Communication infrastructure
- High consequence distribution lines

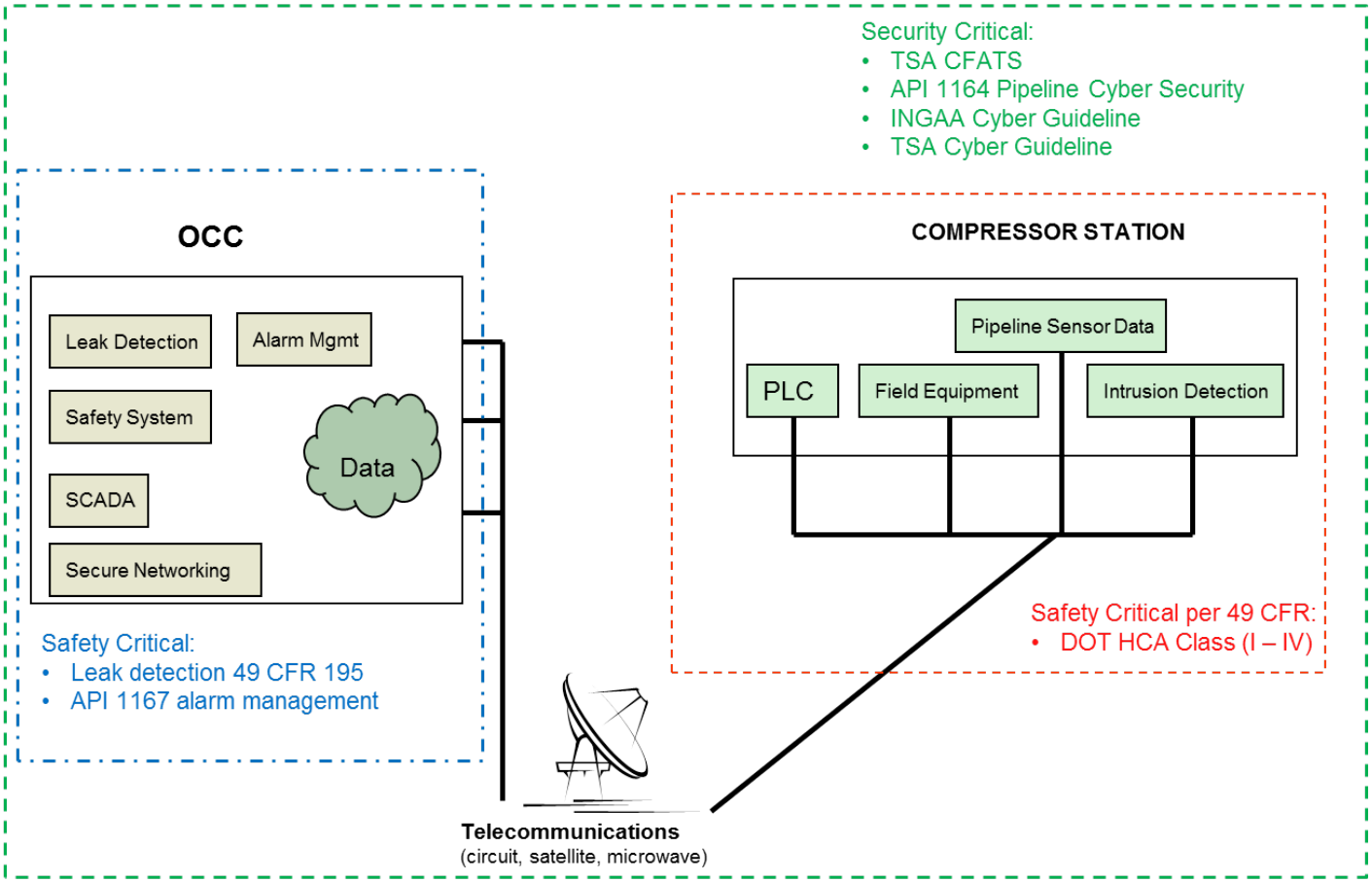
Approaches to Risk Mitigation:

- Blend of cyber and physical security
  - Geographic disparity presents challenges to security, yet large targets
  - Built-in security for new systems, bolt-on security for legacy systems
- Complex industry safety regulations exist
- Industry cyber standards and guidelines exist (API, INGAA, NIST), but cyber security is not yet regulated.

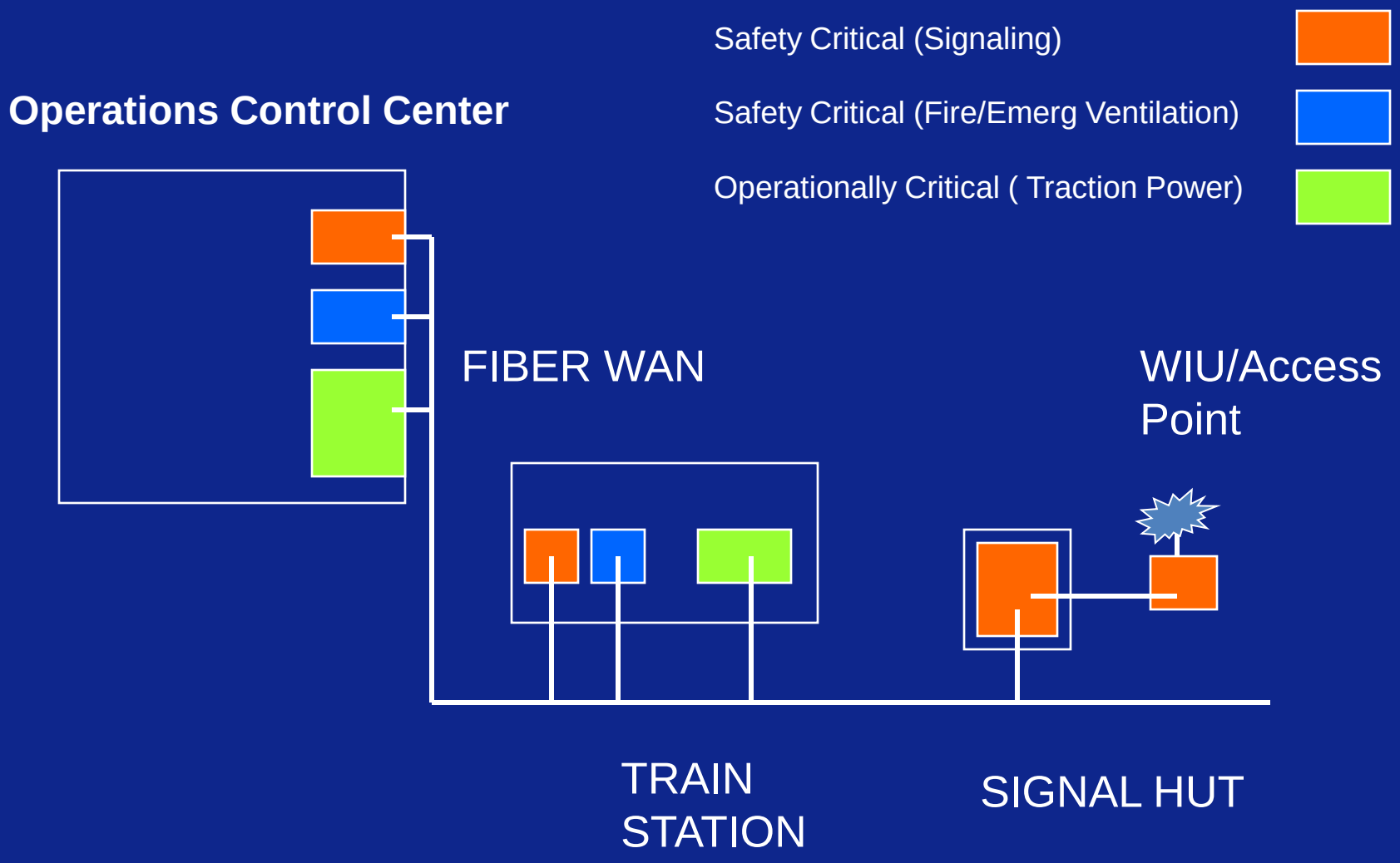
Pipeline/Oil & Gas Transport

Pipeline Example:
Gas Pipeline Compressor Station

Safety-Critical: leak detection, PLC, data integrity
Operationally Critical: sensors, field equip, SCADA, telecom



Defining the Critical Zones for Rail Transit



Strategy for Rail Transit

- Highest safety zone (safety-critical) already defined.
- Overlay the electronic security perimeter over this safety-critical zone
- Similarly overlay the physical security perimeter over the safety-critical zone
- Existing standards to be considered
  - FRA – Signaling
  - NFPA – Fire, emergency
  - IEEE - Trainline
  - AREMA

Typical Light Rail Signal Hut

Safety-Critical Zone
Electronic Security Perimeter
Physical Security Perimeter

It’s not always this easy !

Assembling RP Part 2

- Define safety-critical zone and boundary
- Define inter-zone communication controls
- Define within –the-zone security controls
- Relate controls to generic network diagrams
- Add explanatory text, glossary, etc.

Thank you!

Dave Teumim, Teumim Technical, LLC
dave431@enter.net

Annie McIntyre, Ardua Strategies Inc.
amcintyre@arduastrategies.com