The adequacy of communication diagnostics for High Speed Rail

Nicholas DiSaia

Joe Greco

<Title>

October 14, 2018

BOMBARDIER

Bio: Nicholas DiSaia, Manager Networks and Cyber Security Bombardier Transportation, Rail Control Solutions, USA

- **13 years working in both Communications Engineering and Automatic Train Supervision.**
- **Responsible for project deliveries of the wired network and radio system.**
- **Manages R&D and product development efforts for Radios, Networks, and Communications Software.**
- **Principal Software Engineer and architect of Bombardier's Network Monitoring System products.**

Bio: Joseph A. Greco, Manager Technical Solutions Bombardier Transportation, Rail Control Solutions, USA

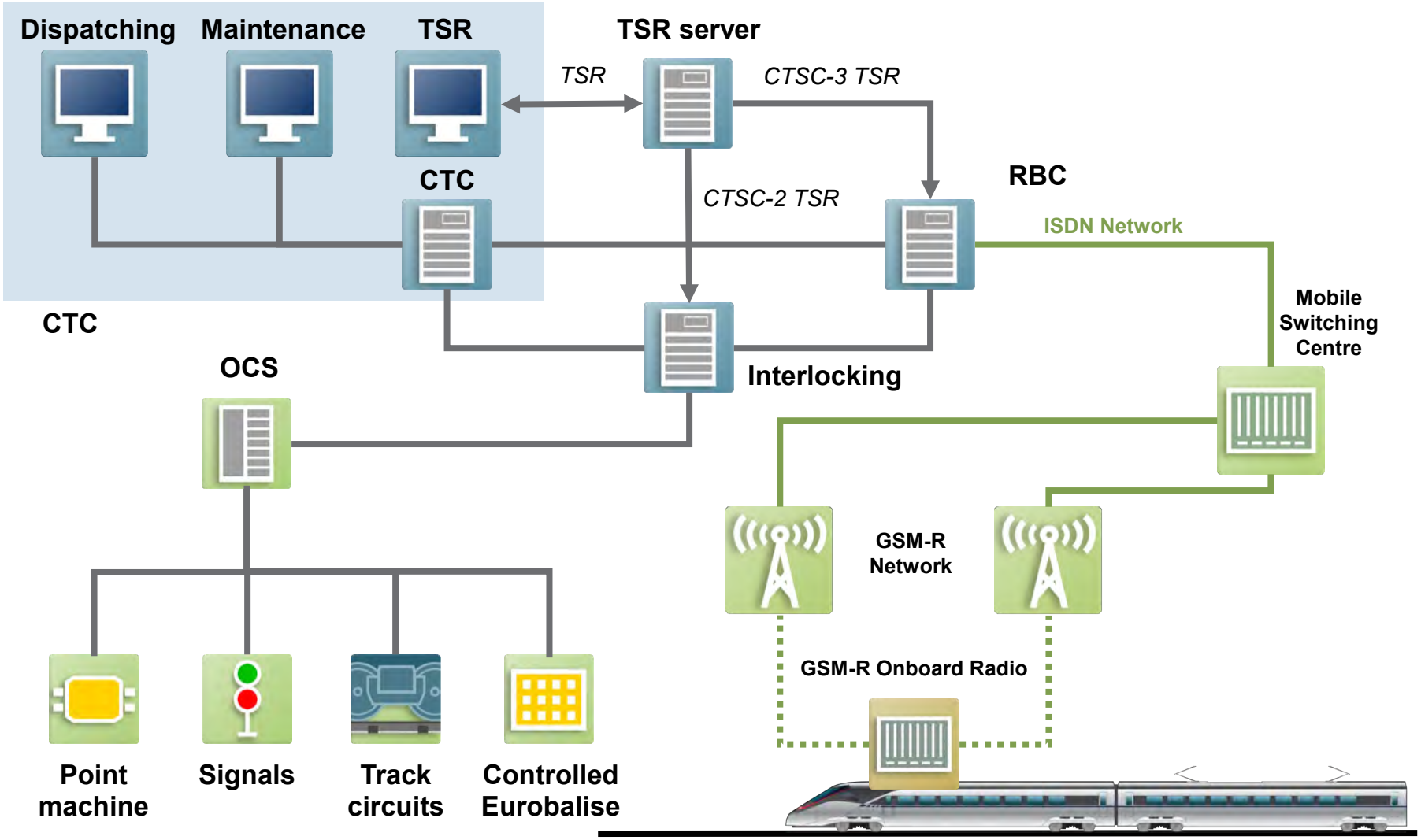
- **Over thirty years of experience in Train Control applications with a focus on Unattended Transit Systems and Communication Based Train Control.**
- **Led the wayside development of Bombardier's Communication Based Train Control System in the 1990s and holds a patent for the positioning system for a moving block system.**
- **Team member for the development of Bombardier's Network Radio System.**
- **For 10 years managed the CBTC software development teams for both wayside and on-board and is currently manager of Technical Solutions in Pittsburgh.**

High Speed Rail Train Control and Communication Systems

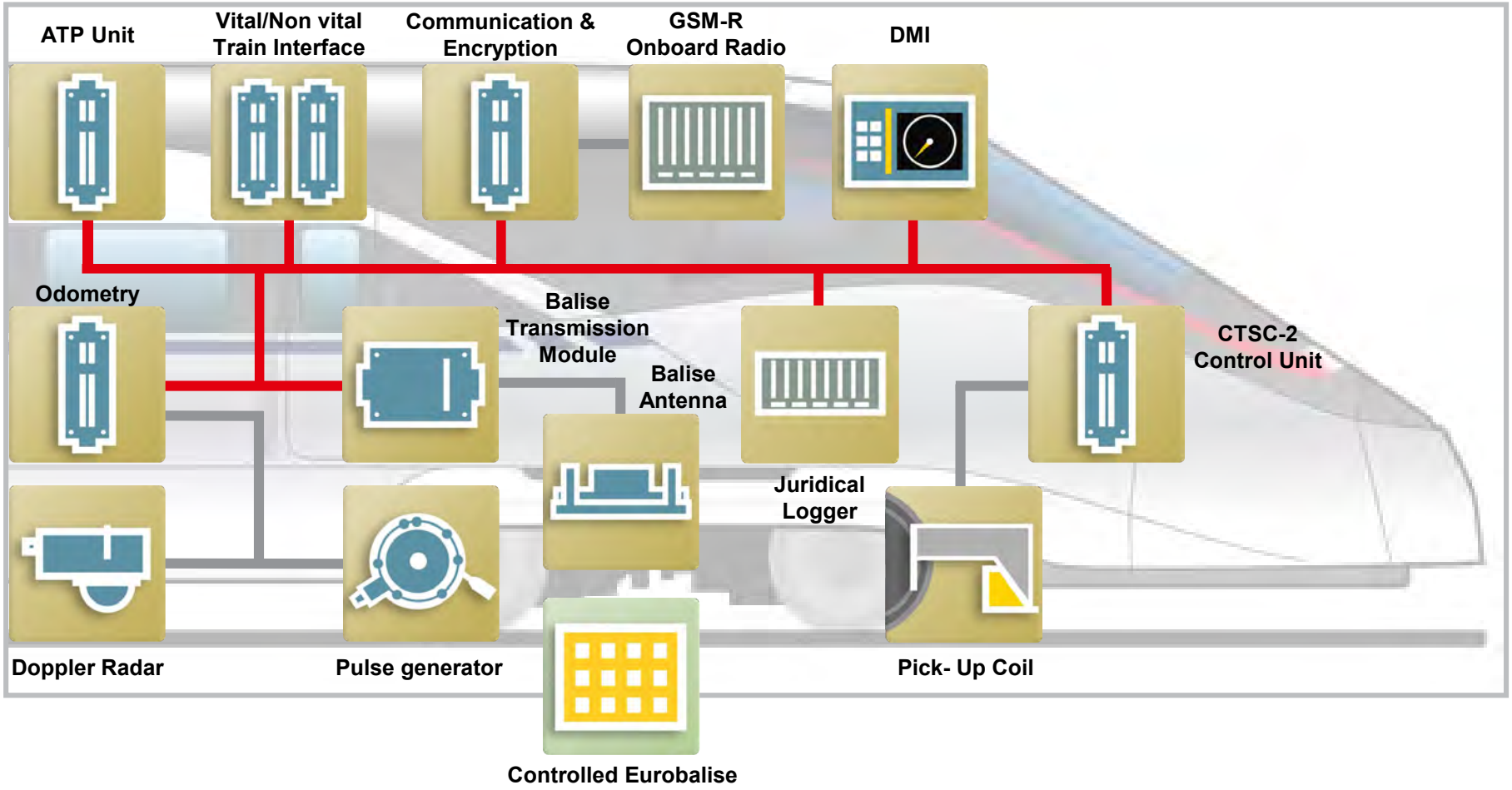
Communication Systems in High Speed Rail

- Communication Infrastructure - Wired and Wireless
- Industry diagnostics for communication Systems
- Enhanced diagnostics for wired and wireless systems
- Safety and Cyber-Security

Signaling System Components



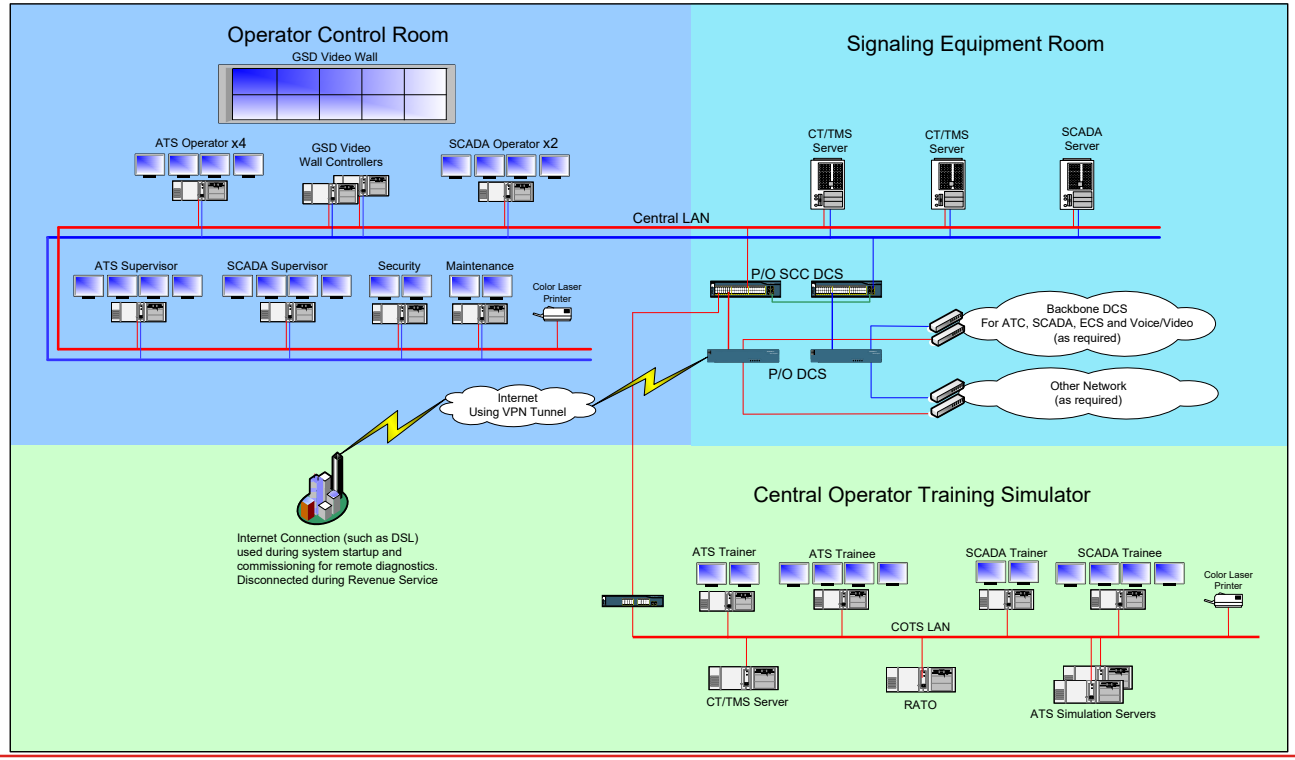
WuGuang DPL ATP Onboard - System Components



BOMBARDIER

High Speed Rail Train Control and Communication Systems – Supervisory Control and Data Acquisition

- **Central Command will have the ability to control the following functions:**
  - Signaling Operations and Passenger Communication – Includes telephones, Closed Circuit Television (CCTV), Public Addressing, Passenger Information Systems, and Emergency Passenger Communications



BOMBARDIER

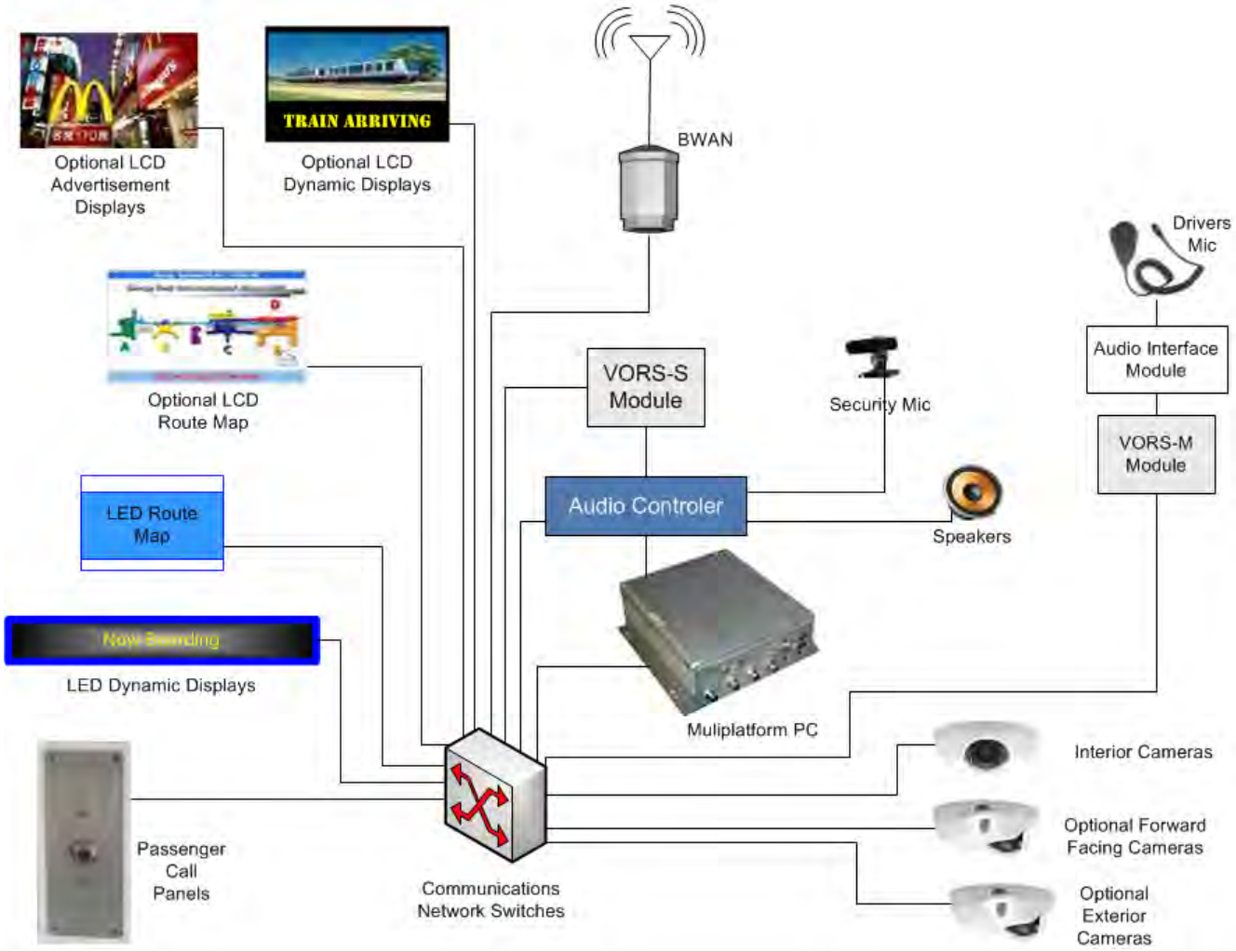
High Speed Rail Train Control and Communication Systems – Supervisory Control and Data Acquisition

SCADA –

- **The SCADA system provides aggregation and processing of field device signals and alarms as well as providing the ability to send control requests to field devices.**
- **Standard SCADA functionality may be required such as alarm evaluation, alarm acknowledgement, data logging, visualization of data as well as functionality beyond that of a typical SCADA system such as the integration of Communications functionality.**
- **Sub-system interfaces to the SCADA system:**
  - Power Distribution System, Primary (Traction Power) and Secondary Power Sources
  - Access Control/Intrusion Detection
  - Fare Collection
  - Fire Detection, Ventilation Systems
  - Signaling Alarms and Events

High Speed Rail Train Control and Communication Systems – Data Acquisition & Passenger Information

- **Onboard the Train**



BOMBARDIER

High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems

- Summary of Communication System Services
- A. Signaling
- B. Central Control System
- C. CCTV
- D. Passenger Signs and Infotainment
- E. PA System, Telephone System
- F. Intrusion Detection
- G. Possible WiFi Access

To supply all the services listed above, a communication Network is defined

High Speed Rail Train Control and Communication Systems

- Communication Systems in High Speed Rail
- **Communication Infrastructure - Wired and Wireless**
- Industry diagnostics for communication Systems
- Enhanced diagnostics for wired and wireless systems
- Safety and Cyber-Security

High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems

- **Key elements in the communication network design.**
  - What types of networks are required?
    - Signaling train to wayside for High Speed Rail
      - GSM-R
      - Tetra
      - GPRS
      - LTE
    - Wayside Infrastructure
      - Wired network with fiber along full alignment
      - Leased Lines
      - Wireless network between wayside objects
    - Train to Wayside for non-signaling functions (for ex. Operational Radio & diagnostics)
      - GSM – voice
      - Tetra
      - LTE
      - Wireless Mobile Network

High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems

- **Functional Operation**
  - Single Network Architecture with all services included
  - Separate networks for signaling and non-signaling functions

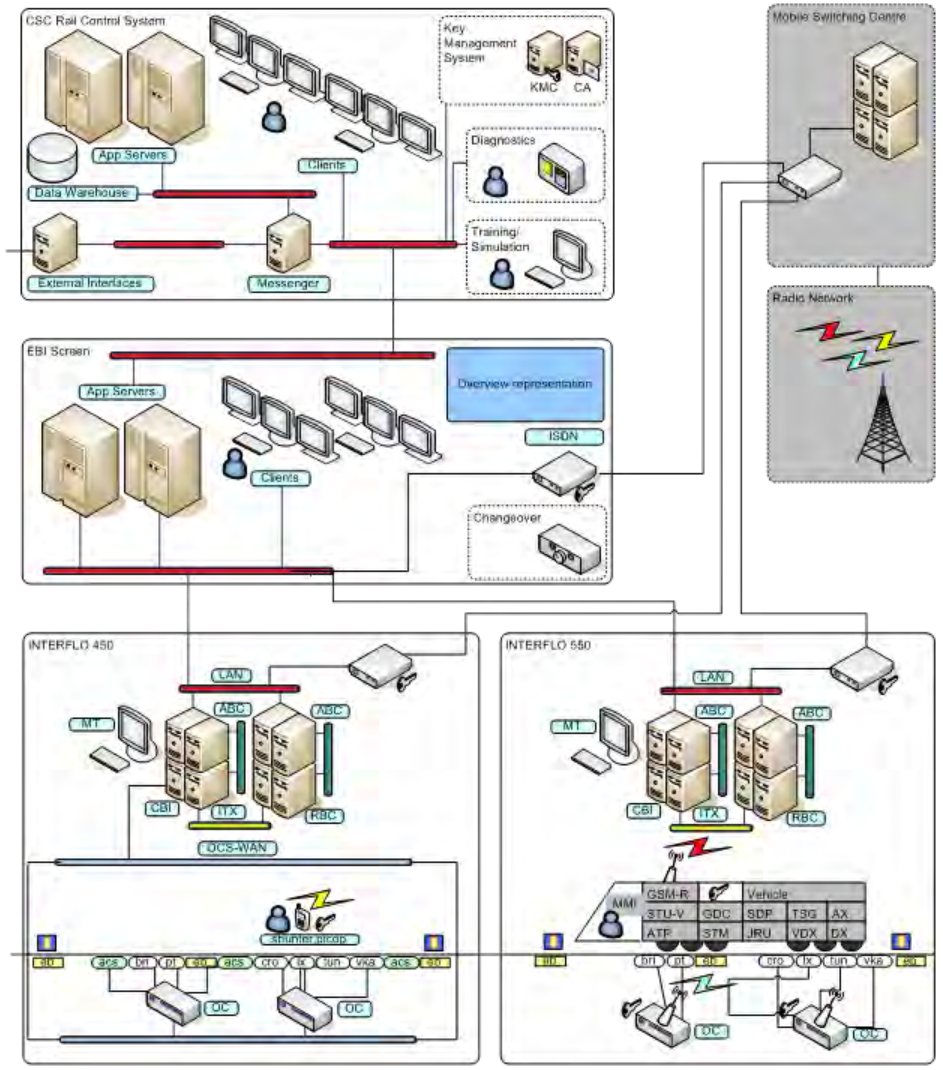
- **Performance**
  - Size of wired network
  - Bandwidth of wireless data from train to wayside
  - Quality of Service

High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems

Layer 3: CSC Rail Control System
(Advanced TMS)

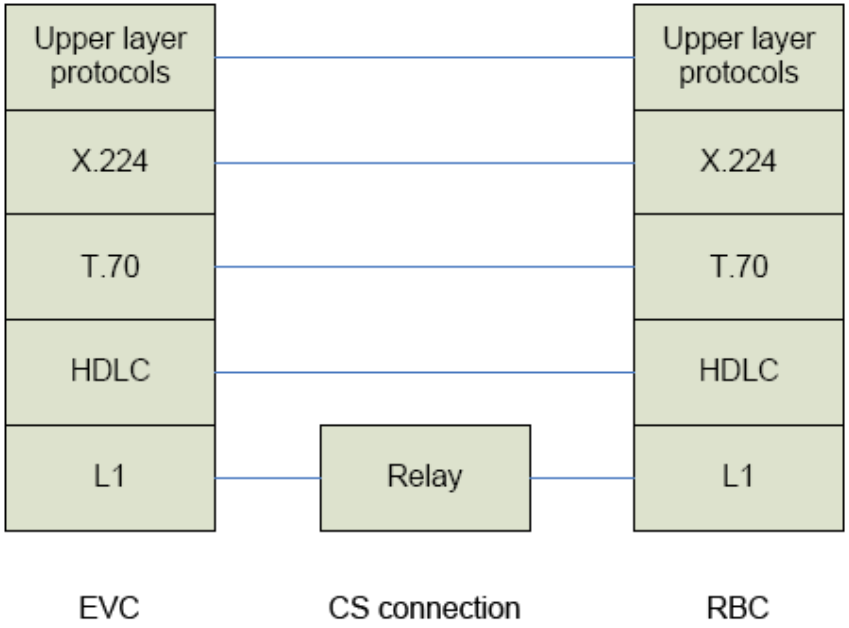
Layer 2: *EBI* Screen
(Basic TMS)

Layer 1: *INTERFLO* 450 or 550
(ERTMS Level 2/Regional)



BOMBARDIER

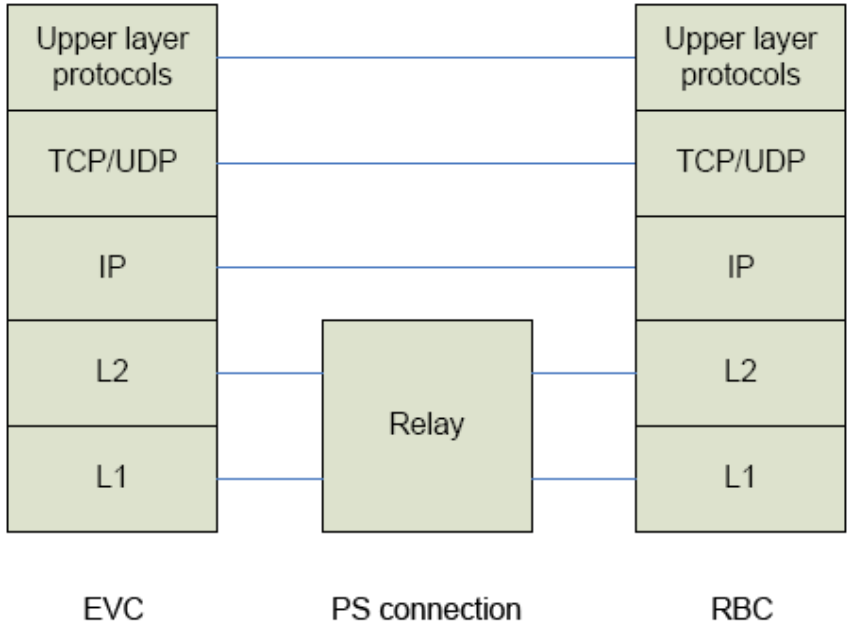
High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems



The protocol architecture according to the existing ERTMS specifications

The protocol architecture according to the future ERTMS specification.

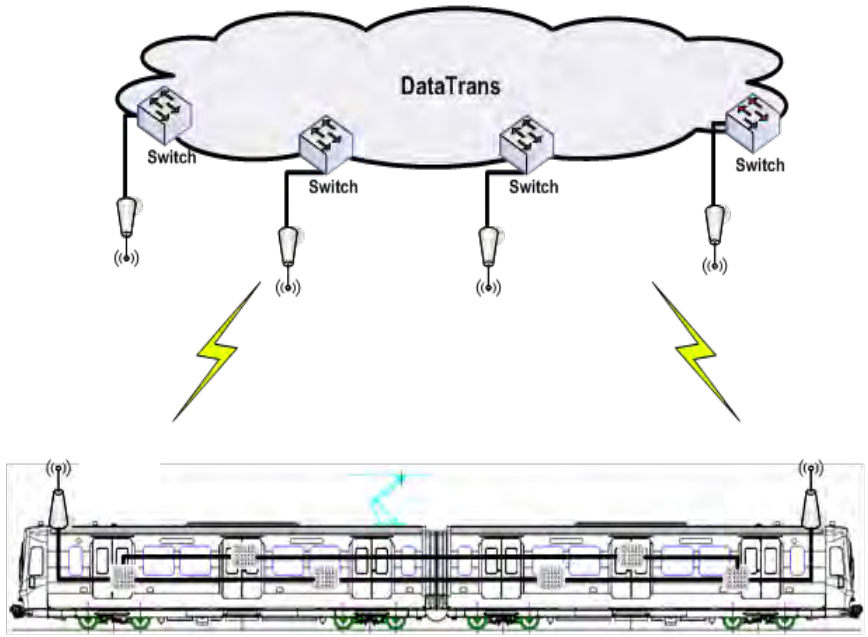
The future is now.



BOMBARDIER

High Speed Rail Train Control and Communication Systems – Wired and Wireless Data Transport Systems

- **Non-signaling Services**
  - Passenger Information Systems
  - Telephone
  - CCTV
  - Worker Protection Devices
  - Passenger Announcements
  - Operational Radio



High Speed Rail Train Control and Communication Systems

- Communication Systems in High Speed Rail
- Communication Infrastructure - Wired and Wireless
- **Industry diagnostics for communication Systems**
- Enhanced diagnostics for wired and wireless systems
- Safety and Cyber-Security

High Speed Rail Train Control and Communication Systems – Industry Diagnostics for Communications

Overview

- Industry Diagnostics for Communication Systems
  - Rail Industry Comparison
  - Communication Failures and Root-Causes
- Enhanced Diagnostics
  - Integrated NMS systems
  - Long-term Maintenance
- Safety and Cyber Security
  - Current State of Affairs
  - Normative Standards
  - Risk Tolerance, Avoidance, and Maintenance

High Speed Rail Train Control and Communication Systems – Industry Diagnostics for Communications

	Rail Industry	Commercial IT Networks
Design Life	30+ years	Variable –tends to follow market trends and favors increases in capacity.
Network Flux	Rare	Frequent
Feature Set	Narrow	Wide
Product Changes	Variable Vendors unlikely to commit to project schedules	Rare
Change Management	Structured baselines/releases of configuration. Limit untested changes to live system.	Auto-discovery of new devices. Live updates of configuration. Many cases changes are non-critical.
Network Commissioning	Strict Online, available, and built to spec -> Good	Relatively Lenient Online & available -> Good
Licensing	Fixed or preferably none	Per node, per interface, per sensor, per feature, consumption based, annual service fees, etc. May require internet access for validation. Move toward SaaS.

High Speed Rail Train Control and Communication Systems – Industry Diagnostics for Communications

What is a Communication Failure?

- Depends on who is detecting the failure...

Root Causes

- Radio System Issues
  - AP failure vs Client radio failure
  - Interference/Jamming
  - Roaming problems
- RSSI Issues
  - Antenna alignment
  - Degradation of mechanical connections
  - Inline component failure
  - LoS Blockage
  - TX Power Amplifier and Low-Noise Amplifier
- Application Issues
  - Software stops sending messages
  - CRC issue
- Network Issues
  - Did a device fail?
  - Excessive errors on port/bad connections
  - Change of configuration or component
  - Routing & VLAN'ing
- Does the failure affect every train in an area or just a signal train? Limited to 1 vehicle or multiple vehicles?

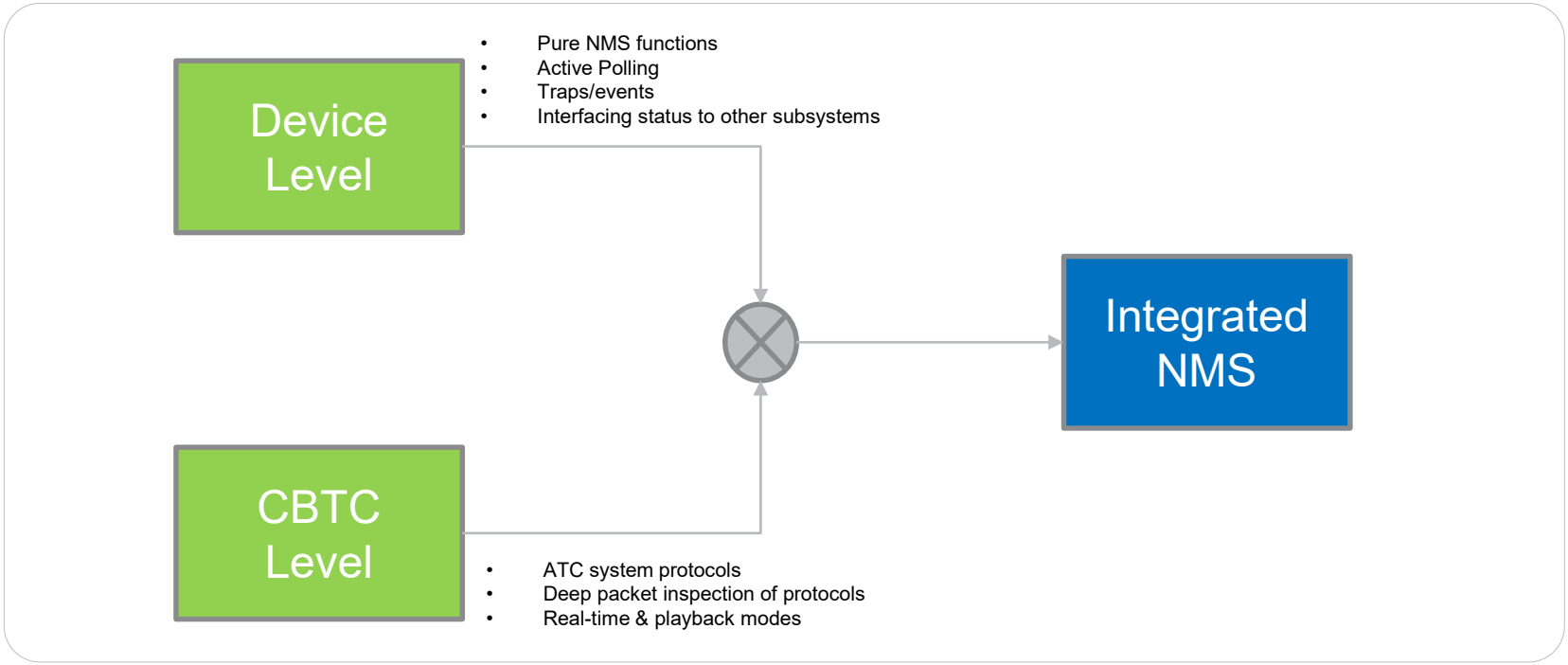
BOMBARDIER

High Speed Rail Train Control and Communication Systems

- Communication Systems in High Speed Rail
- Communication Infrastructure - Wired and Wireless
- Industry diagnostics for communication Systems
- **Enhanced diagnostics for wired and wireless systems**
- Safety and Cyber-Security

High Speed Rail Train Control and Communication Systems – Enhanced Diagnostics

Integrated Network Monitoring Systems

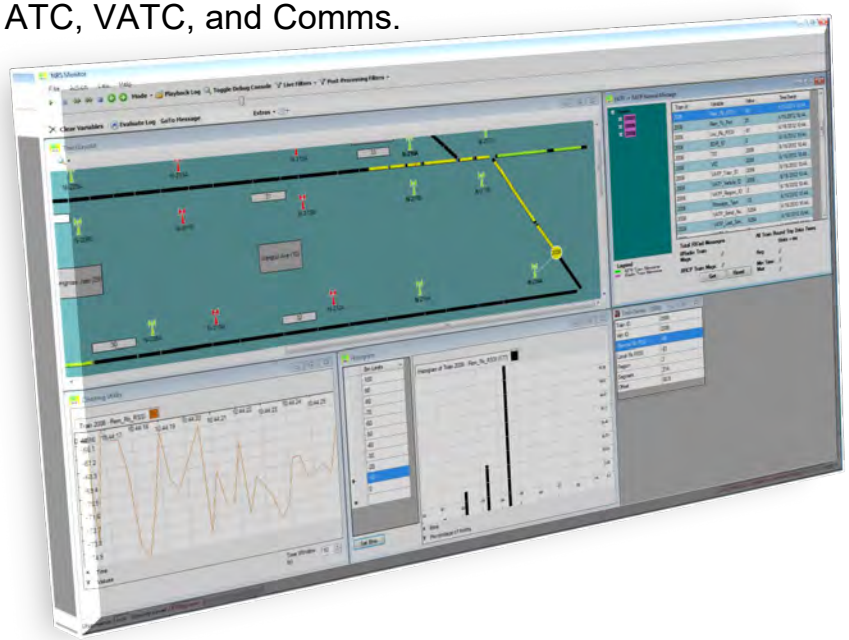


BOMBARDIER

High Speed Rail Train Control and Communication Systems – Enhanced Diagnostics

Key Features:

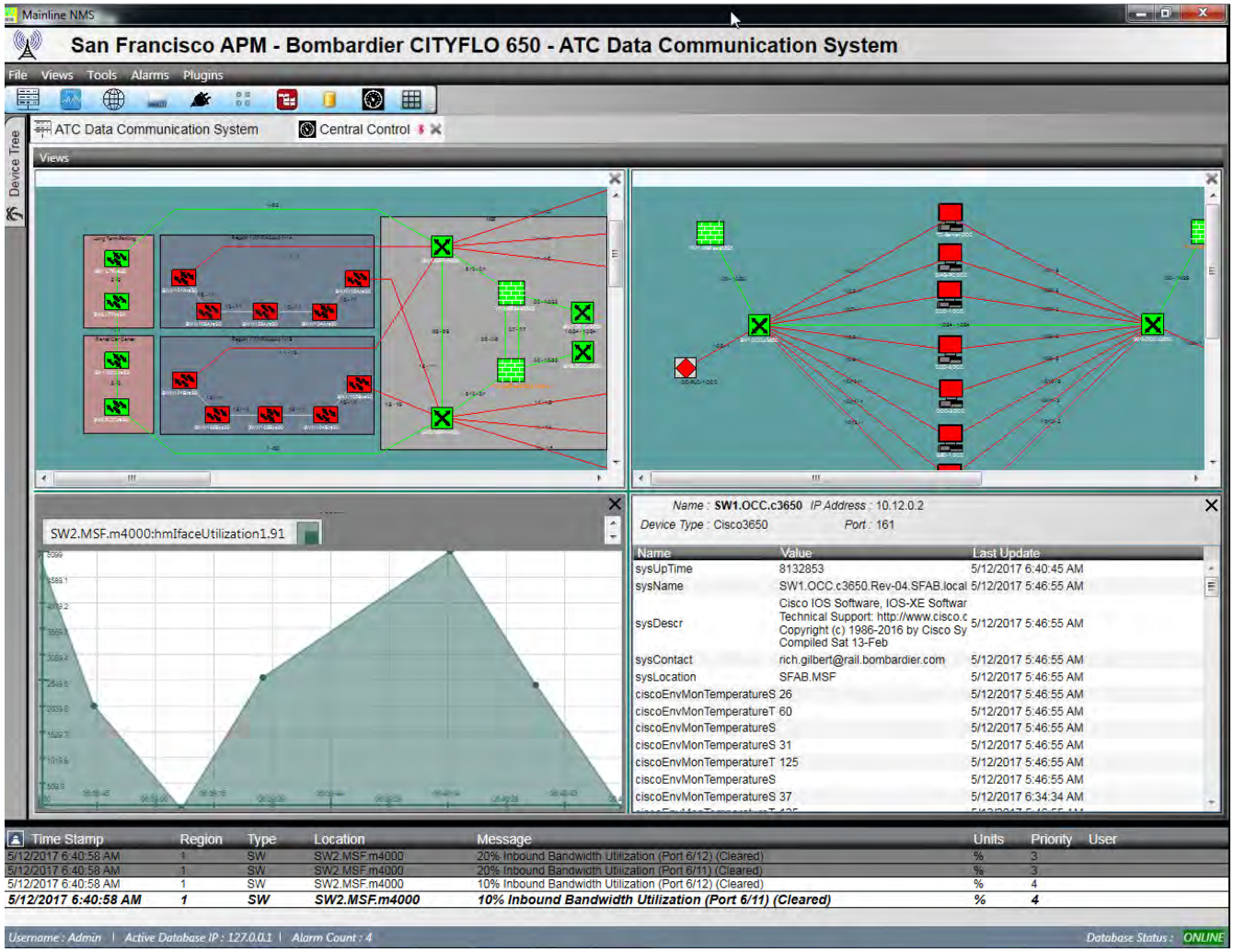
- SNMP (v1/v2c/v3) monitoring + other protocols
- Real-time analysis and playback of log files
- Online/Offline troubleshooting and diagnostics for ATC, VATC, and Comms.
- Normalized live data management
- Redundant operation
  - A/B pairing
  - Control Center Clustering
- User Security and Access Control
- Analysis
  - Statistics and charting tools
  - Visualization of the system
  - Alarm/Event filtering/sorting/preview
  - Heat Maps
- System commissioning tools



High Speed Rail Train Control and Communication Systems – Enhanced Diagnostics

BOMBARDIER

High Speed Rail Train Control and Communication Systems – Enhanced Diagnostics



BOMBARDIER

High Speed Rail Train Control and Communication Systems – Enhanced Diagnostics

Maintenance and Health Checks:

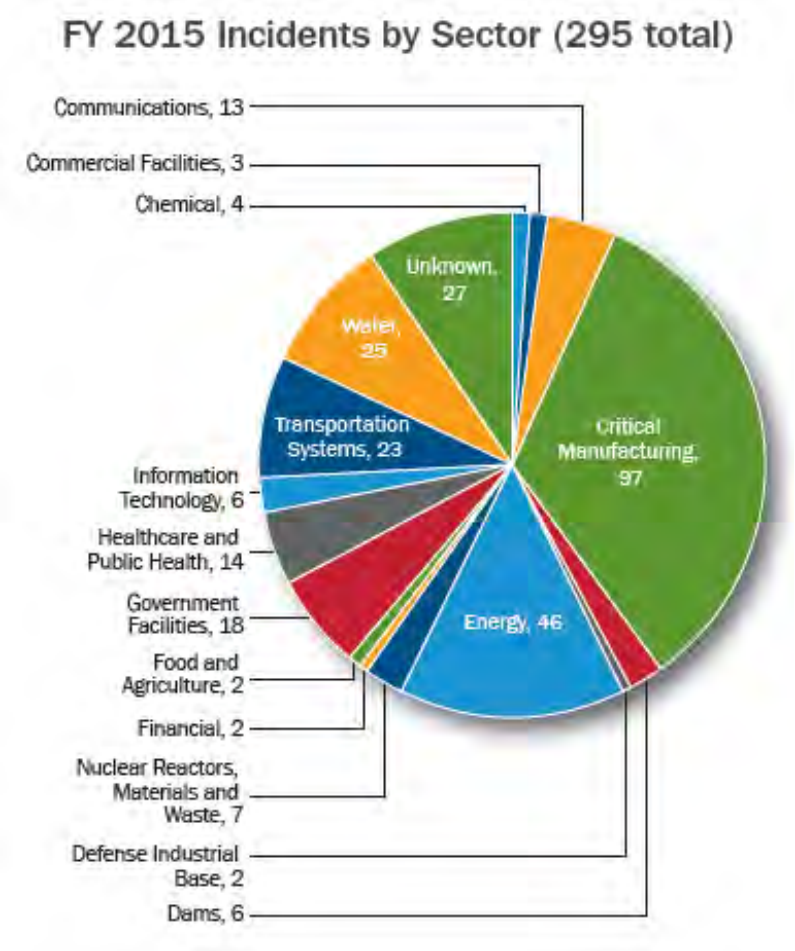
- Integration with higher-level systems for predictive and preventative maintenance
  - Dispatch the right people at the right time
- Remote Diagnostics
  - On-Demand Supplier support
- Health Checks
  - RF/TWC System
  - Network
  - Cyber Security
  - Onsite vs Remote Health Checks

High Speed Rail Train Control and Communication Systems

- Communication Systems in High Speed Rail
- Communication Infrastructure - Wired and Wireless
- Industry diagnostics for communication Systems
- Enhanced diagnostics for wired and wireless systems
- **Safety and Cyber-Security**

High Speed Rail Train Control and Communication Systems – Safety & Security

Transportation Sector – ICS-CERT 2015



23% of ICS Incidents have happened in the transportation Sector (USA)

Source: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

High Speed Rail Train Control and Communication Systems – Safety & Security

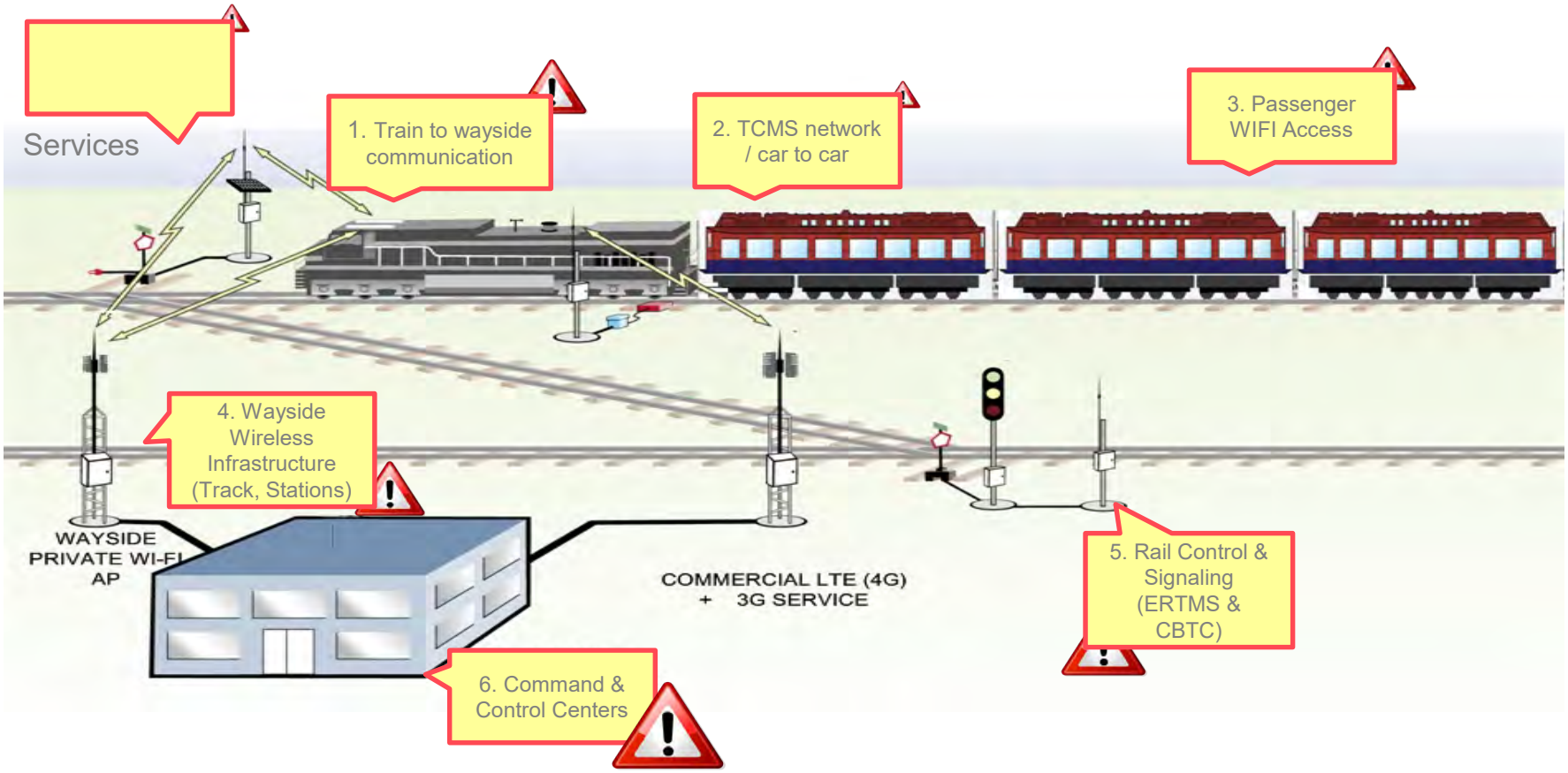
Why Rail Infrastructures became more vulnerable

REASONS

- Today Industrial Systems are **monitored and controlled** by IT technologies operating in open networks
- Establishing **standard protocols** make a wider range of devices vulnerable
- Coexistence of **Legacy** and **New systems**
- Utilization of **commercial of-the-shelf-products**, but lack of awareness to establish the necessary security tools and software updates
- **Wireless** and cellular communication

High Speed Rail Train Control and Communication Systems – Safety & Security

Attack Vectors and Intrusion Routes

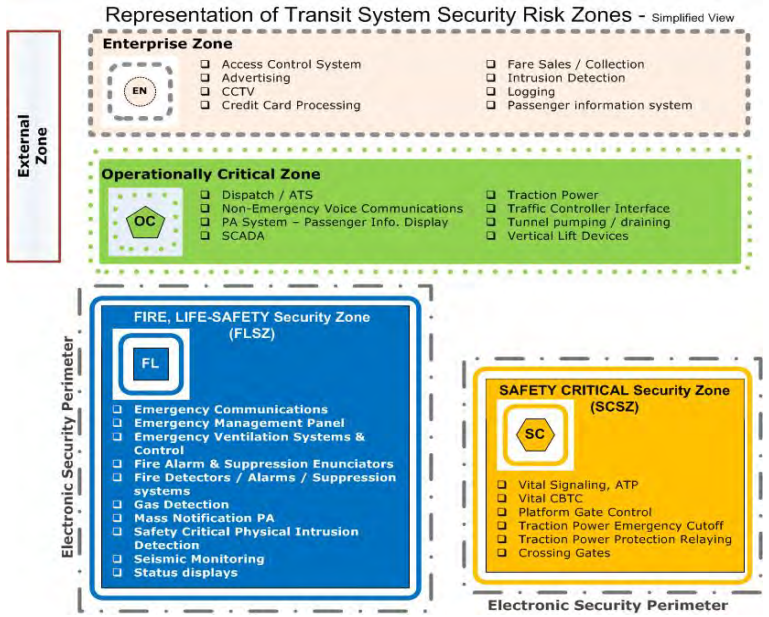


BOMBARDIER

High Speed Rail Train Control and Communication Systems – Safety & Security

Typical Standards

- ISO 27001
- APTA SS-CCS-RP001-10
- APTA SS-CCS-RP-002-13
- NIST 800 series
- EN 50159
- IEC 62443



Methods for Compliance

- Physical Security Measures
- Firewalls/NIDS/HIDS
- Network segmentation, isolation, and ACLs
- Policies and Procedures
- Monitoring, reporting, and identification of problems
- Security Server functions
- Centralized authentication strategies
- Password policies
- Encrypted links

Source: APTA-SS-CCS-P-002-13: Securing Control and Communications Systems in Rail Transit Environments
APTA: American Public Transportation Association

BOMBARDIER

High Speed Rail Train Control and Communication Systems – Safety & Security

Risk Tolerance and Continued Improvement

What is secure today will not be secure tomorrow!

- Threat and Vulnerability Assessment
- Security Log
- Principle of Least Privilege (PoLP)
- Cyber Security Health Check & Pen Testing

Thank You!

Questions?