Train Control System and Cyber Security

Ali Edraki **MASc, P.Eng, PMP**

Vice President Assurance and Systems

Immanuel Triea, **CISM, CISA, CRISC, CISSP**

Sr. Director of Information Security

Gannett Fleming

Gannett Fleming

Excellence Delivered As Promised

Rail Conference

APTA

Train Control System and Cyber Security

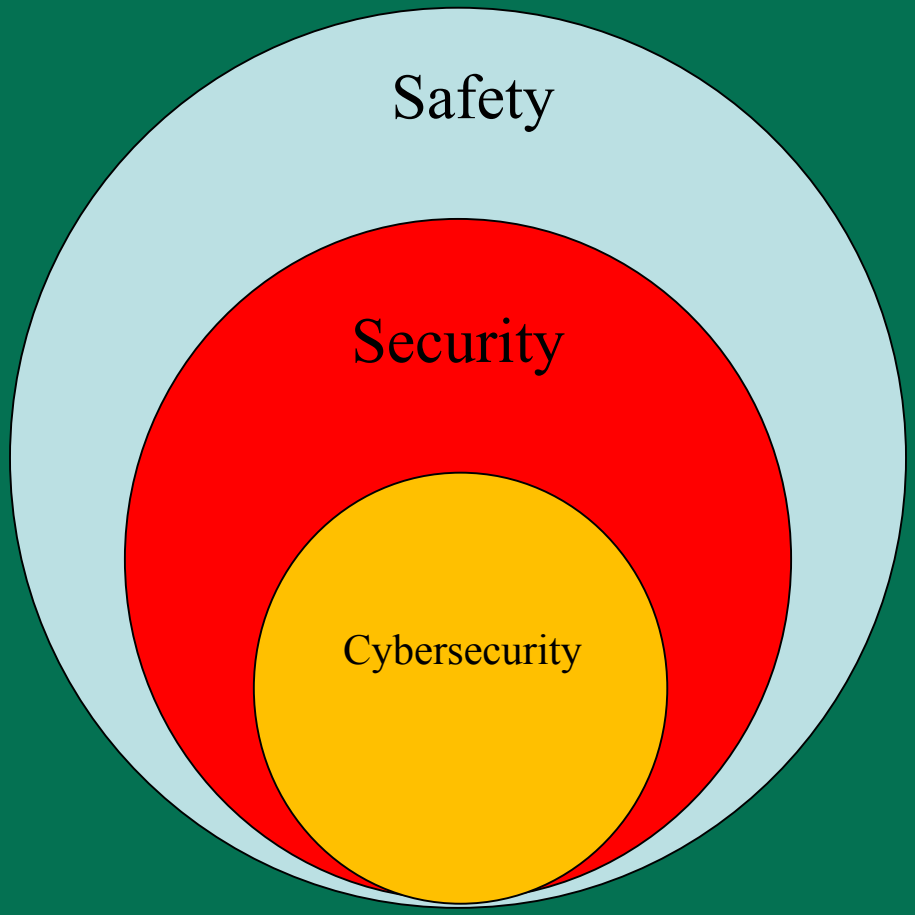
- Introduction
- Safety vs Security vs Cybersecurity
- Train Control System
- Threats
- Impacts
- Typical Cyber Security Defense Methods
- Conclusion

Gannett Fleming

Excellence Delivered As Promised


YOU HAVE
BEEN HACKED

Safety vs Security vs Cybersecurity

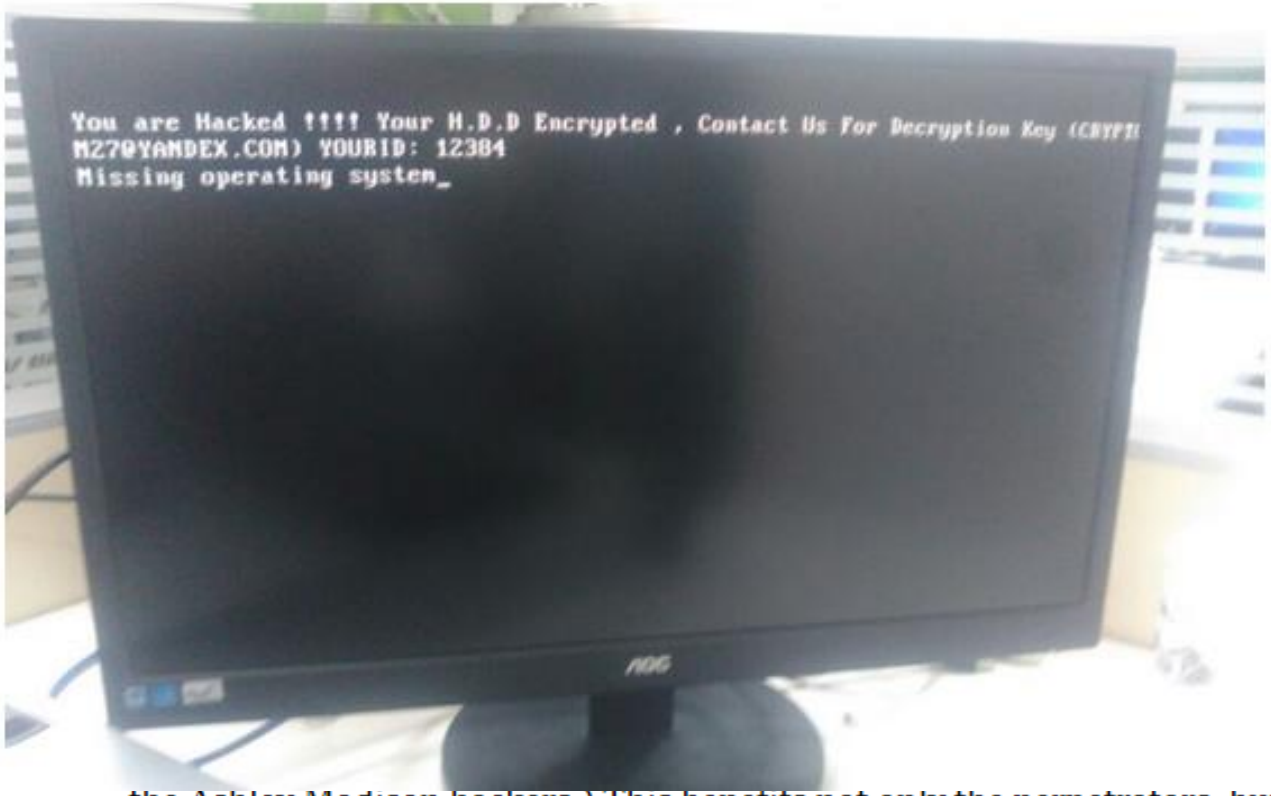


Gannett Fleming
Excellence Delivered As Promised

29 San Francisco Rail System Hacker Hacked

NOV 16

The **San Francisco Municipal Transportation Agency** (SFMTA) was hit with a ransomware attack on Friday, causing fare station terminals to carry the message, "You are Hacked. ALL Data Encrypted." Turns out, the miscreant behind this extortion attempt got hacked himself this past weekend, revealing details about other victims as well as tantalizing clues about his identity and location.

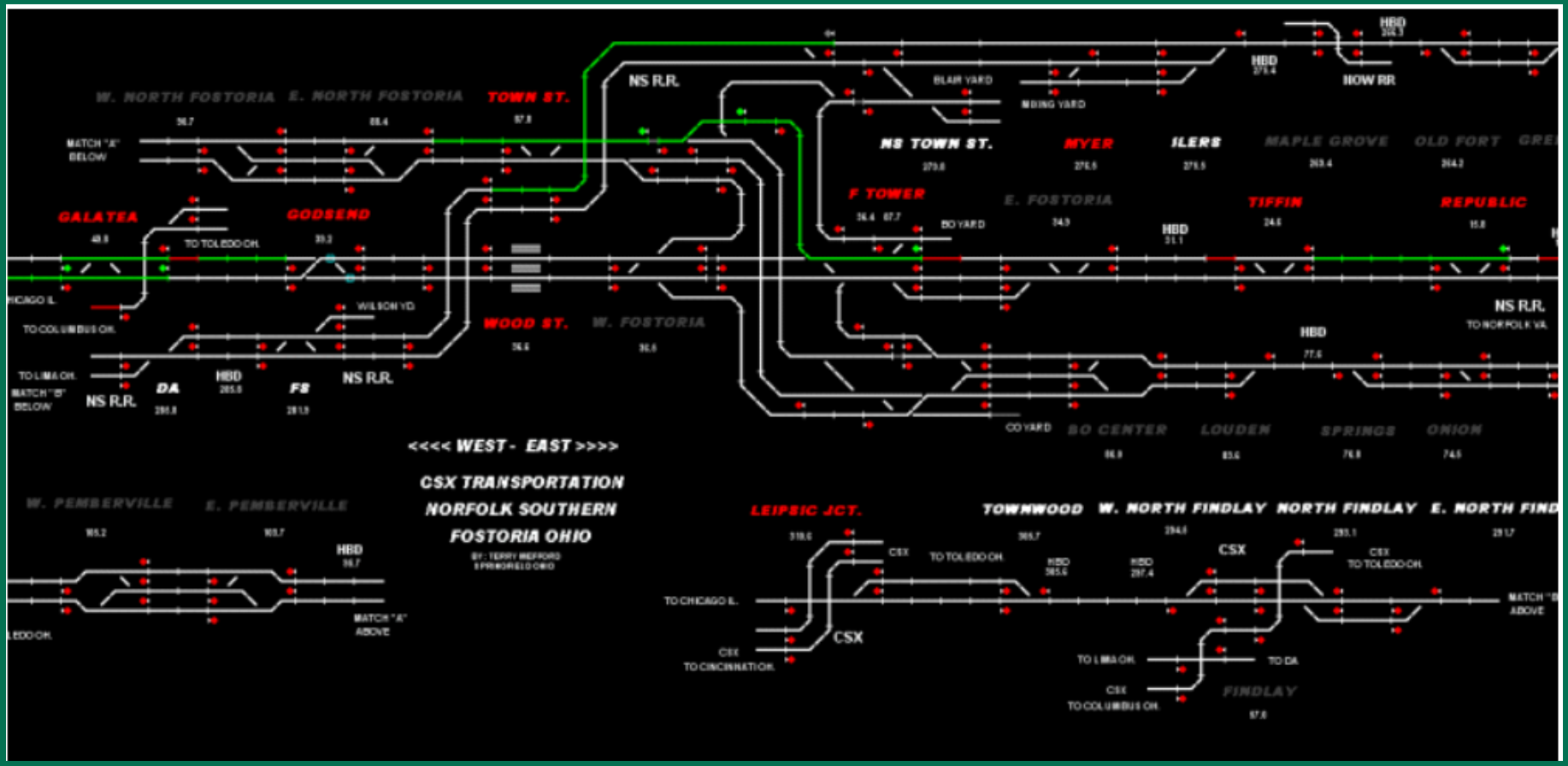


aph: Mark Dries

lar
nem,
n sets of
e
ted by

the Ashley Madison hackers.) This benefits not only the perpetrators, but also their

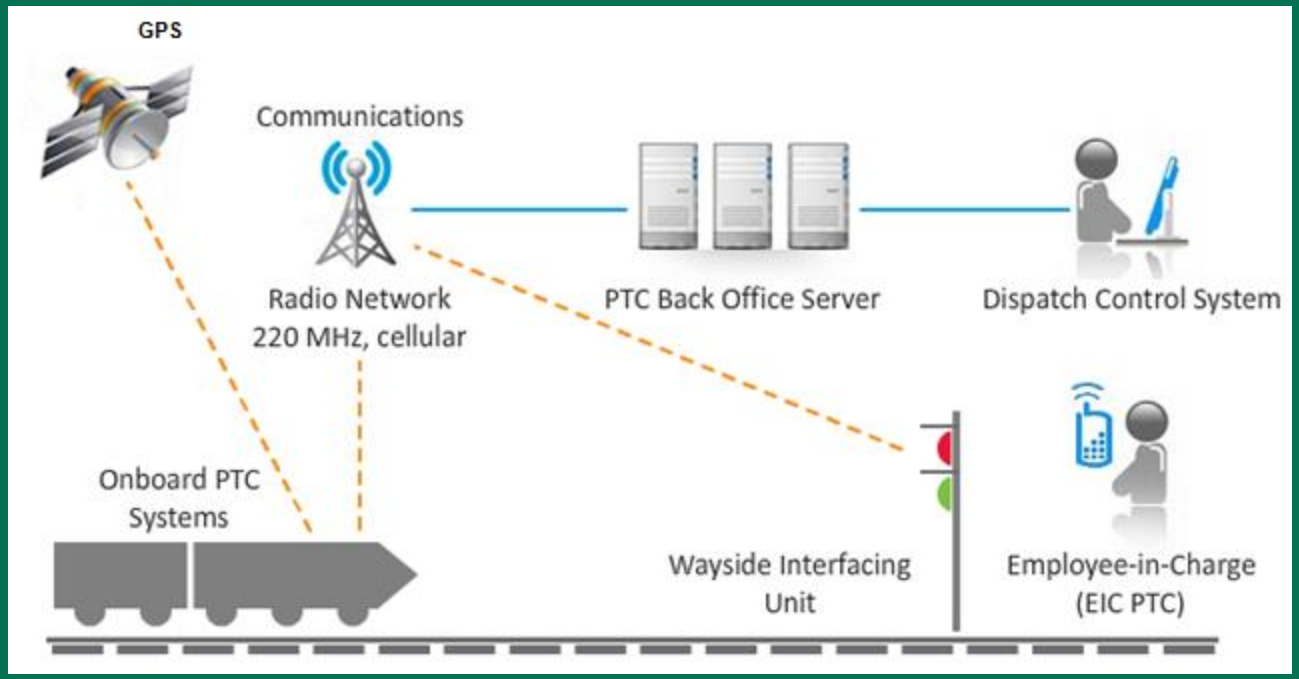
Train Control System



Gannett Fleming

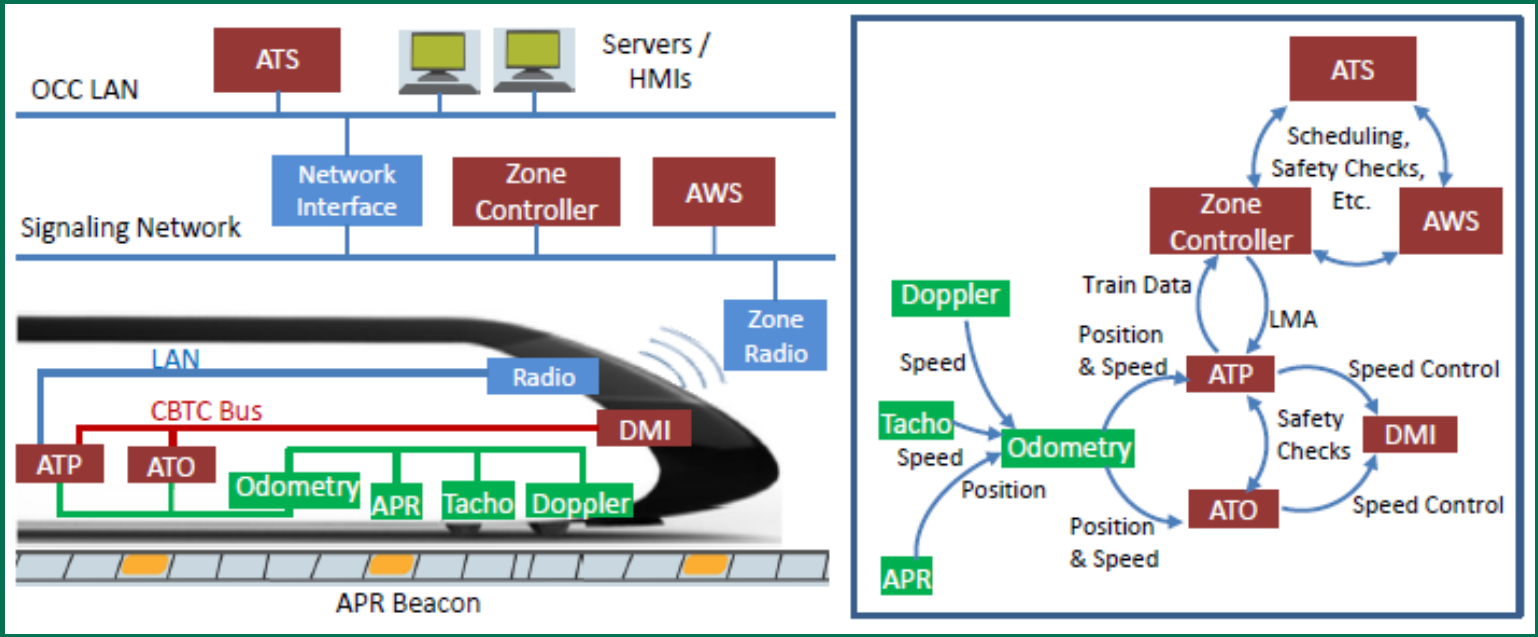
Excellence Delivered As Promised

Positive Train Control System - PTC



Gannett Fleming
Excellence Delivered As Promised

Communication Base Train Control System - CBTC



Gannett Fleming
Excellence Delivered As Promised

The Modes of Attack – in Rail

- Remotely
- At close hand
- Locally

Threats – Train Control Systems

- Breaches of train movement safety
- Breaches of functional safety and reliability
- Reduced efficiency

The Impacts

- Threats to safety (Injury, Death)
- Disruption to the rail network/services
- Economic loss
- Reputational damage
- Socioeconomical (Mental)

Typical Cyber Security Defense Methods

- Train Control Systems should be designed to secure against threats that can have an impact on safety and operations.
  - The communication networks over which they operate should be designed using defense-in-depth techniques.

Gannett Fleming
Excellence Delivered As Promised

Typical Cyber Security Defense Methods

- Risk Assessment and Penetration Testing
  - Define system assets
  - Identify threats and vulnerabilities and map to each asset
  - Review existing and planned controls
  - Estimate and rank risks
  - Perform penetration tests
  - Develop and implement Mitigation Plans

Gannett Fleming
Excellence Delivered As Promised

Typical Cyber Security Defense Methods

- Establish Cyber Security Design Essentials
  - Multiple layers of defense
  - Mechanisms to detect and recover from attacks
  - Security controls based on threat and risk assessments
  - Establish security zones

Typical Cyber Security Defense Methods

- Establish A Strong Perimeter
  - System-level authentication and application filtering
  - Defenses against common web attacks
  - Remote user authentication
  - Multi-layer firewalls
  - Secure Virtual Private Network (VPN) gateways

Typical Cyber Security Defense Methods

- Implement System and Detection/Recovery Controls
  - Logging and monitoring services
  - Threat detection and prevention
  - Centralized antivirus solution

Typical Cyber Security Defense Methods

- Utilize Cyber Security Standards
  - APTA Guidelines
  - NIST Series
  - ISA/IEC 62433 Standards
  - ISO 27001/2
  - NERC CIP Standards
  - FIPS

Gannett Fleming
Excellence Delivered As Promised

Typical Cyber Security Defense Methods

- Maintain Operational Conditions
  - Use a security operational controls check list to ensure the security posture of the system is maintained
    - Day-to-day activities
    - Proper policies
    - User access management
    - Auditing of policies

Typical Cyber Security Defense Methods

- Include Cyber Security in the Lifecycle
  - All projects involving Train Control Systems should include cyber security at every step
    - Bid process
    - Design and planning phase
    - Testing process
    - Technology upgrade

Gannett Fleming
Excellence Delivered As Promised

Key Presentation Take-Aways

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

Gannett Fleming
Excellence Delivered As Promised

Conclusion

Cyber security cannot be “bolted-on” at the end of the design process for Train Control Systems. To be effective, cyber security functionality needs to be designed in to systems from the earliest stage if it is to be successful in protecting the systems and be cost-effective.

Gannett Fleming

Excellence Delivered As Promised

Gannett Fleming

Excellence Delivered As Promised

Typical Cyber Security Defense Methods

- Require Safety Protection
  - Implement message integrity and safety controls to protect against any unauthorized message or malicious software on the network
  - Ensure protocols are based on One-Channel-Safe principles
    - Include internal cyclic redundancy checks (CRC)