INFRASTRUCTURE

MINING & METALS

NUCLEAR, SECURITY & ENVIRONMENTAL

OIL, GAS & CHEMICALS

Cybersecurity for Public Transportation Rail Systems

The Bechtel Approach

Table of Contents

I. Cybersecurity Challenges 1

II. Addressing the Cyber Challenge 1

III. Rail Risk Assessment and Management 2

IV. Industry References and Guidance to Support Transportation 4

Acronyms

APTA	American Public Transportation Association
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
BART	Bay Area Rapid Transit
CBTC	Communications-Based Train Control
CCTV	Closed Circuit Television
DHS	Department of Homeland Security
ETCS	European Train Control System
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISA	International Society of Automation
NIST	National Institute of Standards and Technology
PA	Public Address
SCADA	Supervisory Control and Data Acquisition

Cybersecurity for Public Transportation Rail Systems

I. Cybersecurity Challenges

The rail mass transit sector has many unique cybersecurity challenges. Modern rail systems include a wide range of complex and interconnected subsystems, including both wired and wireless communications between train, trackside, station, and command centers.

Critical subsystems such as fire suppression, life safety, and train control and signaling systems have high availability and reliability requirements. Internet-facing subsystems must also be addressed, such as real-time point of sale systems, real-time schedules, customer fare systems, and a web presence. Railway systems rely on industrial control systems (ICS) to keep them moving. Therefore, a comprehensive cyber security plan is crucial to integrate the various subsystems.

These systems are used daily by thousands of people, and visibility and public awareness are high. As more components are digitized and networked, the exposure has grown and new threats are coming to light. This evolution makes cybersecurity an important concern.

Over the last few years, the cyber security threats for rail systems have grown significantly. Examples include:

- **January 2008.** In the city of Lodz, Poland, a teenager hacked the trams signaling system, taking control of the trains. As a result, four vehicles were derailed injuring twelve people.
- **November 2016.** A ransomware attack on the San Francisco Bay Area Rapid Transit (BART) ticketing machines resulted in passengers being unable to purchase tickets over Thanksgiving weekend.
- **May 2017.** WannaCry infected German train stations, and passenger information monitors were seen displaying the ransom window.

The cyber threat to these systems is real. Nation states, cybercriminals, hacktivists, cyber-terrorists, malicious insiders, and even unscrupulous operators all have their motives. The consequences of a successful cyber-attack on rail infrastructure could be catastrophic. Not only financial loss is at stake; public safety can be at risk, with consequential loss of reputation. Meeting the cybersecurity requirements of such a complex system requires a design and implementation approach that integrates risk management and security into each phase of the project lifecycle.

Cybersecurity is **critical** to the transportation sector, making risk assessments and management increasingly important to the safety of rail systems.

Integrating cybersecurity throughout the system design process is the best approach to **minimize risk and cost.** Bechtel leverages engineering expertise to incorporate cybersecurity into **every phase** of project engineering methodology.

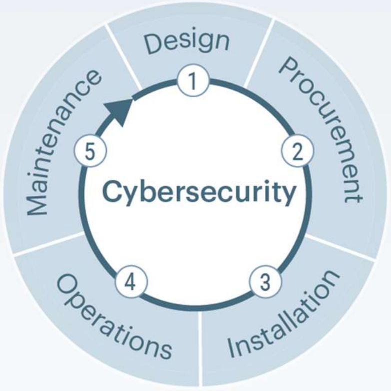


Figure 1: *Cybersecurity is integrated into the entire system design process.*

II. Addressing the Cyber Challenge

Integration of Security and Design

Integrating cybersecurity requirements into the entire system design process is considerably more effective than addressing cybersecurity at single points in the process. Bechtel incorporates cybersecurity into all phases of the control systems engineering project methodology. Our approach is “cybersecure by design.”

By addressing cybersecurity holistically via existing standard work processes, cybersecurity requirements are automatically flowed down to procurement processes, suppliers, and vendors. As shown in in **Figure 1**, cybersecurity is an integrated component from design to procurement to installation to operation to maintenance. This unified project execution process includes specific design reviews to assess physical protections for security but also reviews to assess the physical protection for cyber risk reduction.

For example, all acceptance testing includes specific cybersecurity testing to ensure attack surface concerns are addressed. Equipment from other subsystem suppliers are incorporated into acceptance tests to ensure strong cybersecurity resiliency. Policies and procedures are addressed by integrating security considerations with the programmatic elements of the project. This approach provides the appropriate layers of protection to meet the project specific risk requirements.

III. Rail Risk Assessment and Management

The threat landscape for rail mass transit applications is changing. It is critical to have a clear understanding of what level of risk is acceptable to our client early in the project execution. It is crucial to decide when to conduct an assessment and which risk model to apply.

When to Assess a System

Proactively integrating cybersecurity requirements leads to a cohesive and layered approach, which is more cost effective and robust. Risk assessment will be conducted throughout the project life cycle, and should be reviewed periodically after the system is commissioned. Most projects begin with a high-level assessment, with more detailed assessments and gap analysis preformed as appropriate as the project matures. It is important for the client to be heavily involved in the risk assessment process. Ultimately the project cybersecurity program needs to be consistent with our client’s cybersecurity requirements.

Risk assessments also need to be performed for existing systems and during significant upgrades. Although less efficient and often costlier than designing in cybersecurity from the beginning, existing systems can be retrofitted to significantly improve their cybersecurity posture. This can occur as a standalone activity, or along with any required system upgrades. A system upgrade, such as implementing Positive Train Control or European Train Control System (ETCS), should trigger an assessment of cybersecurity.

Risk Assessment Model

The risk assessment model chosen for rail and mass transit projects must address the geographical and functional diversity of these systems. The ISA99/ IEC 62443 approach, based on equipment zones or locations, and equipment conduits or communication paths is commonly used. This method provides mechanisms for grouping subsystems into zones with similar technical requirements and risk profiles, and developing risk reducing controls for each individual zone. This ensures that the physical and cyber controls are appropriately tailored for the specific subsystem risk levels.

The following elements are recommended for all risk assessments, regardless of the types of risks being assessed:

- Identify the hazards
- Identify the assets in scope
- Identify any control measures
- Evaluate the risk
- Implement appropriate control measures
- Document assessment
- Conduct Periodic Reviews

As identified by the APTA, **Table 1** below provides an example zone segregation for a rail transit system, with each zone having its own subsystems and requirements. Following the assessment of risk, consultation with the client will lead to management of risk using, for example, the ISA 4T risk management model (treat, transfer, terminate, tolerate), in the most cost-effective manner.

Table 1: *Logical System Grouping for Cybersecurity Zones*

Critical Safety Level	Fire and Life Safety Systems	Operational Critical Controls	Enterprise Level
Vital Signalling ATP	Gas Detection	Dispatch ATS	Access Control System
Vital CBTC	Mass Notification PA	Electrical Controller interfaces	Advertising
Platform Gate Control	Seismic Monitoring	Non-Emergency Voice Communications	CCTV
Crossing Gates	Status Displays	PA System – Passenger Info Display	Credit Card Processing
	Emergency Communications	SCADA	Fare Sales Collection
	Emergency Management Panel	Traction Power	Intrusion Detection
	Emergency Ventilation Systems and Control	Traffic Controller Interfaces	Logging
	Fire Alarm & Suppression Annunciator Systems	Tunnel pumping/draining	Passenger Information System
	Fire Detectors / Alarms Suppression Systems	Vertical Lift Devices	
	Safety Critical Physical Intrusion Detection		
	Traction Power Emergency Cut-off		
	Traction Power Protection Relaying		
	Tunnel Ventilation		

III. Bechtel-Specific Advantages

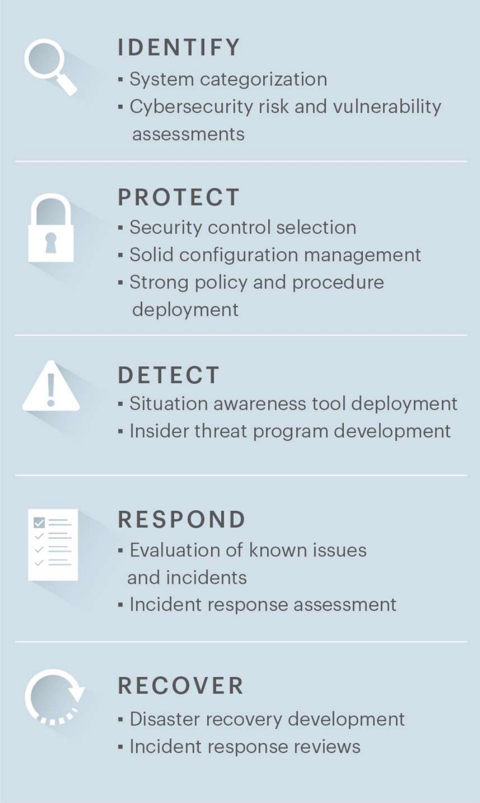
Bechtel has built rail system all over the world in the last sixty years, but also has extensive experience in the nuclear, defense and government sectors. Our view across multiple business sectors provides insight into all aspects of cyber security. We understand the unique needs of the rail industry, and are familiar with cyber security challenges. Bechtel has created a dedicated Industrial Control System (ICS) Cybersecurity Technical Centre to address security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.

The Technical Centre has a cross-function team, consisting of control systems engineers and IT professionals. The goal is to leverage our experience in various industrial sectors and create tighter integration between IT and ICS systems to address cyber security concerns.

The Technical Centre and the functional engineering group can help identify, protect, detect, respond, and recover from threats as necessary to support the contract, as described in **Figure 2**.

Our control system design experience in delivering rail projects globally creates a distinct understanding of ICS cybersecurity vulnerabilities. Our ICS Centre works with our clients to assess risk, implement measures to protect valuable assets, and provide recommendations to reduce the risk on existing and new networks.

By integrating physical and cybersecurity into the entire project lifecycle, we can deliver an integrated rail system that meets the client's needs and is resilient enough to support the client's overall lifecycle program.



IDENTIFY
- System categorization
- Cybersecurity risk and vulnerability assessments

PROTECT
- Security control selection
- Solid configuration management
- Strong policy and procedure deployment

DETECT
- Situation awareness tool deployment
- Insider threat program development

RESPOND
- Evaluation of known issues and incidents
- Incident response assessment

RECOVER
- Disaster recovery development
- Incident response reviews

Figure 2: *Bechtel's cybersecurity threat capabilities*

IV. Industry References and Guidance to Support Transportation

American Public Transportation Association (APTA), an industry association

- APTA SS-ECS-RP-001-14 Recommended Practice: Cybersecurity Considerations for Public Transit
- APTA SS-CCS-004-16 Securing Control and Communications System in Rail Transit Environments Part IIIb: Protecting the Operationally Critical Security Zone
- APTA SS-CCS-RP-001-10 Recommended Practice: Securing Control and Communications Systems in Transit Environments Part1: Elements, Organization and Risk Assessment/Management

U.S. Computer Emergency Readiness Team (US-CERT), a government body

- Transportation ICS Cybersecurity Standards Strategy DHS 2013
- ISA/IEC 62443(-2-4) Requirements for IACS Solution Suppliers
- NIST 800 series

Rail Cybersecurity Guidance to Industry Department for Transportation

- RSSB - UK Railway Safety and Standards Board standards
- RISSB - Australia Rail Industry Safety and Standards Board standards
- ENISA - European Union Agency for Network and Information Security railway recommendations

Industry Specific Guidance

- EN50126 (RAMS) -Railway Applications
- EN50128 (Rail Control and Protection) Safety Critical Development
- EN50129 (Rail Safety Related) Safety Related Communication for Signalling
- EN50159 (Rail Safety Related Communications) Communication, Signalling