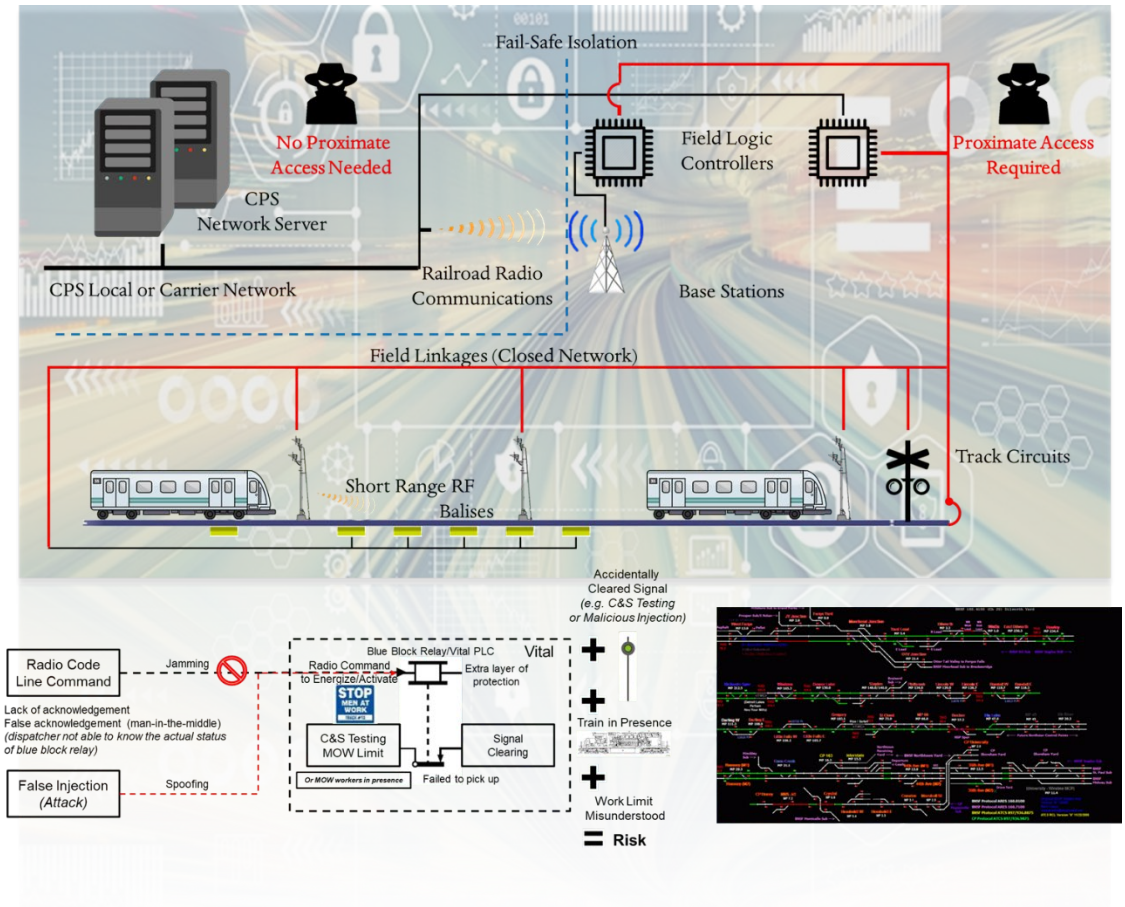
U.S. Department
of Transportation
Federal Railroad
Administration

Office of Research,
Development and Technology
Washington, DC 20590

Cyber Security Risk Management for Connected Railroads



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2020	Technical Report, Sept. 2017–Jan. 2020

4. TITLE AND SUBTITLE
Cyber Security Risk Management for Connected Railroads

5. FUNDING NUMBERS

6. AUTHOR(S)
Xiang Liu[1] https://orcid.org/0000-0002-4348-7432
Duminda Wijesekera[2] https://orcid.org/0000-0002-7122-3055
Zezhou Wang[1] https://orcid.org/0000-0003-4292-7341
Matthew Jablonski[2] https://orcid.org/0000-0002-6960-0181
Yongxin Wang[2] https://orcid.org/0000-0001-8343-4557
Chaitanya Yavvari[2] https://orcid.org/0000-0002-7002-9314
Keith Holt[3] https://orcid.org/0000-0002-1366-9497
Brian Sykes[4] https://orcid.org/0000-0002-2618-1968

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
1. Rutgers, The State University of New Jersey, New Brunswick, NJ
2. George Mason University, Fairfax, VA
3. HNTB Corporation, Philadelphia, PA
4. Pearce Services LLC, Paso Robles, CA

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Research, Development and Technology
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT/FRA/ORD-20/25

11. SUPPLEMENTARY NOTES
COR: Francesco Bedini Jacobini

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the FRA eLibrary.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This research develops a cyber security risk analysis methodology for communications-based connected railroad technologies. The methodology can be tailored to specific use cases and system designs. By implementing the methodological framework, the study can identify potential cyber attack threats, vulnerabilities, and consequences for each case, and thus assess the risk and recommend risk mitigation strategies. The selected connected railroad technology use cases in this project include a radio code line application of the Advanced Train Control System; a remotely controlled movable bridge; and a cyber security risk literature review on Positive Train Control systems. In each case study, the analysis summarized the cyber risk profiles and provided practical recommendations for cyber security improvement. Finally, the report discusses possible directions for rail-centric cyber security risk management in the future.

14. SUBJECT TERMS
Cyber security, communications, risk, connected railroad

15. NUMBER OF PAGES
167

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXIMATE)

1 inch (in)	=	2.5 centimeters (cm)
1 foot (ft)	=	30 centimeters (cm)
1 yard (yd)	=	0.9 meter (m)
1 mile (mi)	=	1.6 kilometers (km)

AREA (APPROXIMATE)

1 square inch (sq in, in^2)	=	6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2)	=	0.09 square meter (m^2)
1 square yard (sq yd, yd^2)	=	0.8 square meter (m^2)
1 square mile (sq mi, mi^2)	=	2.6 square kilometers (km^2)
1 acre = 0.4 hectare (he)	=	4,000 square meters (m^2)

MASS - WEIGHT (APPROXIMATE)

1 ounce (oz)	=	28 grams (gm)
1 pound (lb)	=	0.45 kilogram (kg)
1 short ton = 2,000 pounds (lb)	=	0.9 tonne (t)

VOLUME (APPROXIMATE)

1 teaspoon (tsp)	=	5 milliliters (ml)
1 tablespoon (tbsp)	=	15 milliliters (ml)
1 fluid ounce (fl oz)	=	30 milliliters (ml)
1 cup (c)	=	0.24 liter (l)
1 pint (pt)	=	0.47 liter (l)
1 quart (qt)	=	0.96 liter (l)
1 gallon (gal)	=	3.8 liters (l)
1 cubic foot (cu ft, ft^3)	=	0.03 cubic meter (m^3)
1 cubic yard (cu yd, yd^3)	=	0.76 cubic meter (m^3)

TEMPERATURE (EXACT)

[(x-32)(5/9)] °F = y °C

METRIC TO ENGLISH

LENGTH (APPROXIMATE)

1 millimeter (mm)	=	0.04 inch (in)
1 centimeter (cm)	=	0.4 inch (in)
1 meter (m)	=	3.3 feet (ft)
1 meter (m)	=	1.1 yards (yd)
1 kilometer (km)	=	0.6 mile (mi)

AREA (APPROXIMATE)

1 square centimeter (cm^2)	=	0.16 square inch (sq in, in^2)
1 square meter (m^2)	=	1.2 square yards (sq yd, yd^2)
1 square kilometer (km^2)	=	0.4 square mile (sq mi, mi^2)
10,000 square meters (m^2)	=	1 hectare (ha) = 2.5 acres

MASS - WEIGHT (APPROXIMATE)

1 gram (gm)	=	0.036 ounce (oz)
1 kilogram (kg)	=	2.2 pounds (lb)
1 tonne (t)	=	1,000 kilograms (kg)
	=	1.1 short tons

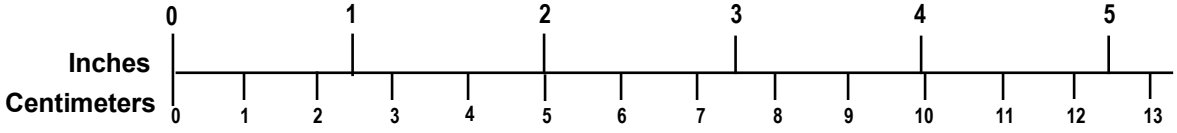
VOLUME (APPROXIMATE)

1 milliliter (ml)	=	0.03 fluid ounce (fl oz)
1 liter (l)	=	2.1 pints (pt)
1 liter (l)	=	1.06 quarts (qt)
1 liter (l)	=	0.26 gallon (gal)
1 cubic meter (m^3)	=	36 cubic feet (cu ft, ft^3)
1 cubic meter (m^3)	=	1.3 cubic yards (cu yd, yd^3)

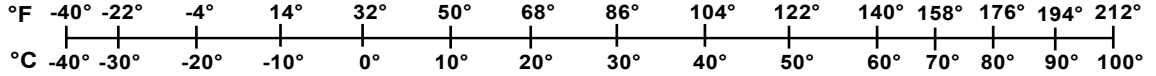
TEMPERATURE (EXACT)

[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSIO



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50
SD Catalog No. C13 10286

Updated 6/17/98

Acknowledgements

The U.S. Department of Transportation, Federal Railroad Administration (FRA) Office of Research, Development and Technology sponsored the work leading to this report. The authors would like to thank Francesco Bedini Jacobini, Program Manager, FRA, for his guidance during the development of this project and report.

The authors of this report thank all other students and staff from Rutgers University and George Mason University, who were involved in this project.

We also appreciate the kind support from the following individuals during this research. Nonetheless, the authors of this report are responsible for all views, analyses, and possible errors.

- Sam Alibrahim, P.E.
- Jared Withers
- Mark Hartong
- David Thurston
- Rui Silva and Robert Baylor
- Jared Hopewell
- Atousa Vali
- Nick Chodorow and Chris Murphy
- Patrick Guest
- Greg Gadomski
- Alison Suffield

Contents

Illustrations

Tables

Executive Summary

The purpose of this research is to develop a cyber security risk analysis methodology for communications-based connected railroad technologies. The methodology can be tailored to specific use cases and system designs. The use-case-specific implementation of the methodology can identify potential cyber attack threats, system vulnerabilities, and consequences of the attack – with risk assessment and identification of promising risk mitigation strategies.

The research team first conducted a literature review of existing or emerging connected railroad technologies, summarizing their commonalities and application scenarios. According to literature review results and identified areas of interests, the team designed an industrial survey distributed to various U.S. railroads to understand their thoughts and concerns for connected railroad cyber risks. After that, the team developed a general risk management methodology as well as the criteria for use case selection. Given the time limit and scope of the project, three representative use cases of connected railroad technology were chosen for a more detailed cyber security analysis: 1) a radio code line application of the Advanced Train Control System (ATCS); 2) a remotely controlled movable bridge; 3) a literature review on cyber security of Positive Train Control (PTC) systems. In each use case, the analysis summarized their cyber risk profile and provided practical risk mitigation recommendations. The primary findings include:

1) ATCS Radio Code Line Use Case: The ATCS radio code line system is widely adopted over North American railroads. The multi-layer, fail-safe design over the ATCS-related systems can prevent most unsafe train movements and thus catastrophic collisions. However, this research identified one potential safety risk case over the ATCS radio code line system, as explained in the Blue Block case scenario. Such risk is minimized by safeguards that are currently incorporated into the design of ATCS communications between the base station and wayside locations, and further augmented by the fact that current designs provide visibility at the back office when unknown factors prevent normal ATCS communication interactions. Since the introduction to PTC technologies, upgrading the legacy ATCS network for better security is no longer deemed as cost-effective. Although the ATCS-targeted attack precedents were rare in the past and could be minimized by its original design, the authors still recommend attention to this potential risk source and ensure that multiple operational verifications are required besides the sole dependency on the ATCS system itself. As for denial-of-service (DoS) attacks (another identified non-safety risk), better resource allocation is needed for optimal counteractions, such as radio channel monitoring and protection, workforce of communication and signaling (C&S) maintenance, flexibility of operation plans, etc.
2) Remotely Controlled Movable Rail Bridge Use Case: An analysis of a fail-safe movable bridge system led to several general conclusions regarding its safety and security risks. A computer simulation model has been developed, which can support “what-if” scenario analysis, the identification of a critical fault path, and a security path. Also, the model could be used to probabilistically differentiate between a fault and a cyber attack if the cause is not immediately known. It is also noteworthy that bridge designs vary case-by-case. Provided with specific data, the model can quantify the risk depending on questions of interest.

3) PTC Cyber Security Literature Review: PTC has evolved over the last 15 years. Many railroads and suppliers are proposing or developing advanced technologies to further secure current PTC systems. One potential future research area on this subject is pointed out: considering the migration from the PTC signaling systems into 5G-based communication systems (as being considered in the vehicle-to-everything, i.e., V2X systems). This will address the limitations of the allocated bandwidth for PTC. The disadvantage of this approach is that the prototyped radio system will need to replace existing QPSK-based modulations with GFDM modulations.

Due to proprietary information over specific system designs and implementation, railroad cyber security knowledge gaps still exist. It is practically impossible to draw a universal conclusion over cyber security vulnerability and profile for all possible systems in the U.S. Instead, use-case-specific risk analysis built upon a consistent methodological framework could be helpful for government, academia, and industry to work collaboratively to manage the cyber security risk associated with connected railroad technologies.

1. Introduction

The increasing use of both information technologies[1] and operational technologies[2] by railroads in the U.S. and elsewhere in the world is increasing their efficiency, safety, and productivity. However, this increased reliance by the railroads on these technologies introduces higher potentials for financial loss, operational disruption, or damage, from the technology failures employed for railroad informational and/or operational functions. These risks arise from unauthorized access, use, disclosure, disruption, modification, or destruction of such technologies. Identifying and mitigating against these require a new understanding of potential cyber security (also written as *cybersecurity*, *cyber-security)* risks for railroad.

Under the auspices of the Federal Railroad Administration (FRA), a research team led by Rutgers University, in collaboration with George Mason University, HNTB Corporation, and Pearce Services LLC, conducted research to better understand the cyber security risks of "connected railroad" technologies, especially in the area of wireless communications.[3] The study results presented in this report include:

- A simplified cyber security risk analysis methodology based on the best practices documented by the U.S. National Institute of Standards and Technology (NIST) tailored for railroads' use
- An illustration of the application to specific use case examples on American railroads
- A specific security risk assessment and risk mitigation strategies for each case study

The presented risk methodology can allow non-cyber specialists in the railroad industry to identify potential cyber attack threats, system vulnerabilities, and consequences of the attack – with risk assessment and identification of promising risk mitigation strategies. Adoption of this methodology by the railroad industry will allow railroad domain experts to be involved with the acquisition, design, development, deployment, testing, operation, and maintenance of the communications-based connected railroad technologies to identify potential security issues associated with these systems, and to facilitate the communication between railroad domain experts and cyber security specialists.

---

[1] Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by the enterprise. Source: FIPS Publication 200 "Minimum Security Requirements for Federal Information and Information Systems" (Ross *et al.*, 2006).

[2] Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Source: NISTIR 8183 NISTIR 8183 Cybersecurity Framework Manufacturing Profile (Stouffer *et al.*, 2017).

[3] See, for example "Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways" (Fraga-Lamas *et al.*, 2017).

1.1 Background

Railroads are adopting various digital technologies to achieve higher efficiency, better safety, and more connectivity. These implementations are regarded as elements of a "digital railway," including but not limited to: remote interoperability, information and configuration management systems, PTC-based signaling systems, distributed power control systems, and various advanced monitoring and detection systems. Increasing connectivity is drawing numerous connections among railroad components to form an information network of rail transportation, referred to as the "rail internet of things" (RIoT) in this study.

Railroads are one element of the critical infrastructure of the United States.[1] Railroad operation involves train equipment movements, various types of freight loads, train passengers as well as the general public that are close to railroad property. Railroads are also essential for both the national economy and its security. National objectives for protecting critical infrastructure include:

- Identify and assure the protection of those assets, systems, and functions deemed most critical in nature, particularly in a national or major regional context.
- Assure the protection of infrastructure and assets that face a specific, imminent threat.
- Pursue collaborative measures and initiatives to assure the protection of other potential targets that may become attractive over time.

Hence, the evolving RIoT demands more active consideration by the railroad management, engineering, and operating personnel toward the cyber-based risks associated with the uses of railroad-owned or commercially tenanted communication networks that support various RIoT applications. While there is a large pool of literature available for systematically identifying and mitigating these risks, much of it requires a level of expertise in cyber security engineering that the majority of railroad personnel do not possess. Therefore, this project aims to assist the industry to further understand:

- Connected railroad/RIoT technologies and their pertinent cyber risks (focusing on communication networks)
- Cyber attack threats, system vulnerabilities, and possible attack consequences
- Possible cyber security risk mitigation strategies

1.2 Objectives and Overall Approach

The primary objective of this research is to develop a cyber security risk analysis methodology for communications-based, connected railroad technologies that can be used by railroad personnel who are not cyber security specialists. Secondary objectives of this research are:

1) Demonstrate the application and usefulness of this simplified methodology and,
2) Evaluate and identify risks and associated mitigation strategies of RIoT elements that rely extensively on communication technologies.

---

[1] See "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," (Washington, DC: Government Printing Office, 2005).

The emphasis was on evaluating both safety and operational efficiency risks that may arise from the exploitation of cyber vulnerabilities in both currently adopted and emerging RIoT technologies.

1.3 Scope

The project assumes that the intended audience of railroad personnel involved in the acquisition, design, and deployment of operational technologies have no, or limited, experience in cyber security engineering. During the use case selection, it further considers RIoT technologies currently in use or being adopted by U.S. railroads only. However, while this research focuses on the technologies used by the railroads within FRA's regulatory governance (both freight railroads and commuter passenger rail), the methodology may be adapted to other similar technologies used in rail systems under Federal Transit Administration (FTA) jurisdiction.

1.4 Organization of the Report

- Section 2 is the literature review and industrial survey. The literature review provides the research results based on academic papers and industrial reports related to connected railroad technologies. The industrial survey was distributed to various railroads or agencies; the results are summarized following the literature review.
- Section 3 provides a simplified risk analysis methodology and use case identification for the connected railroad technologies on American railroads. Several connected railroad technologies subject to potential cyber attacks are listed.
- Section 4, 5, and 6 provide the applications of the risk analysis methodology in Section 3 to three selected use cases. For each use case, the risk assessment and mitigation strategies are provided.
- Section 7 provides a concluding summary of this research. The organization of this report is illustrated as Figure 1.4-1:

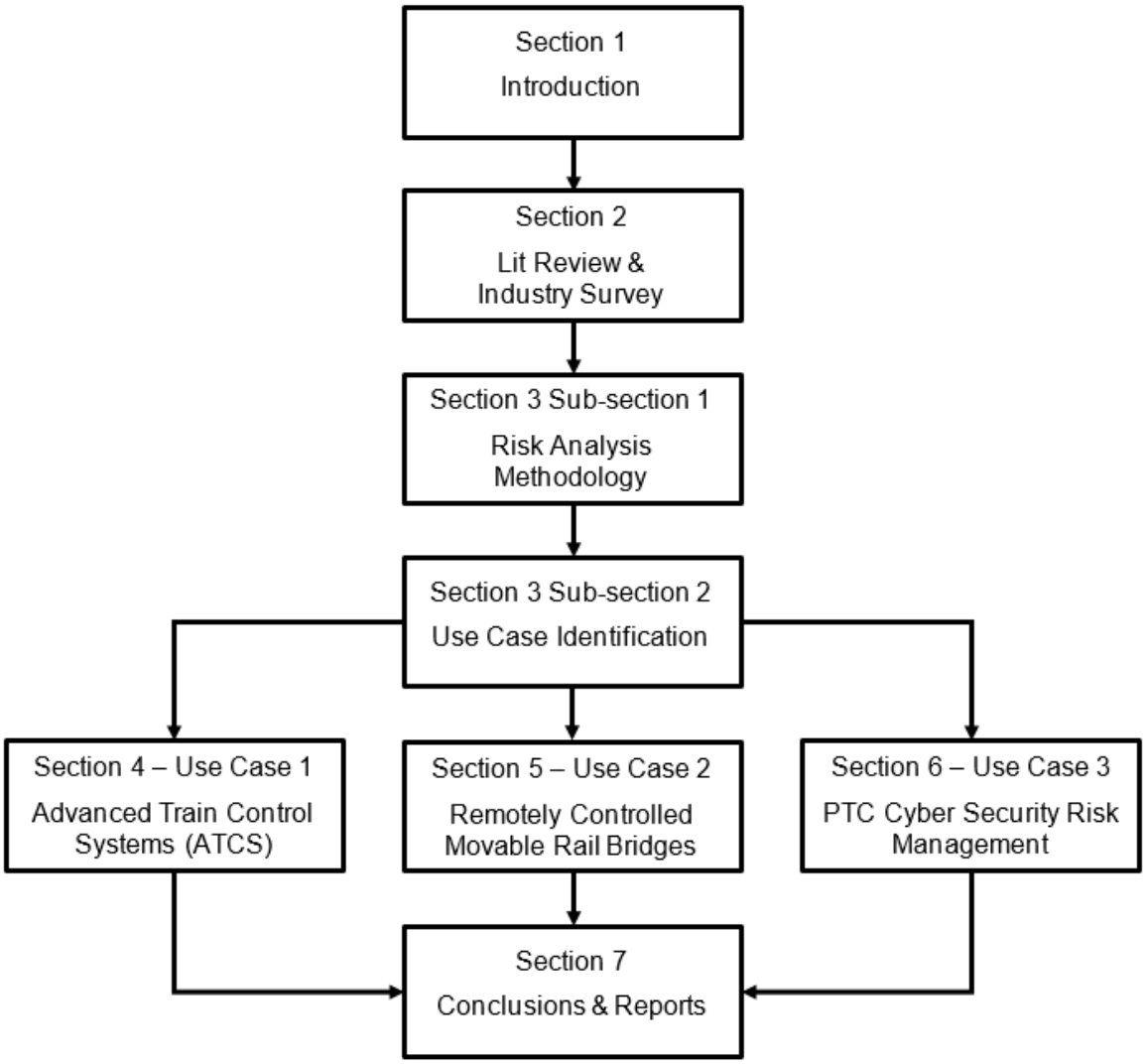


Figure 1.4-1 Report Organization

2. Literature Review and Industrial Survey

The rollout of the internet of things (IoT) and increased use of data-driven and intelligent, interconnected, cyber-based systems occurring in other industries is also occurring globally in the rail industry. This is creating a new era of a "rail internet of things" (RIoT). The RIoT consists of a wide array of communication, information, and automation technologies that comprise all the major elements in the railroad industry (e.g., track, rolling stock, electrification systems). It involves digital communication links upon both wired and wireless networks, communications-based train control (CBTC) systems, distributed power and energy management systems, remote control locomotives, and various advanced defect detection and sensor-based warning systems. Such increasing connectivity and interoperability introduce new safety and security vulnerabilities. For example, in 2008, a Polish teenager used a wireless remote controller to change a track switch, derailing multiple trains and injuring 12 people (Baker, 2019); in 2011, in the U.S. Pacific Northwest, computers in the signaling system were remotely attacked, and a malfunction of train signals lasted for 2 days, causing large-scale service disruptions (Masson & Gransart, 2017); in 2016, Darktrace, a British cyber defense firm, reported that the UK railway network was beset by at least four major cyber attacks (McGoogan & Willgress, 2016); on the U.S. West Coast, the ticketing system of the Bay Area Rapid Transit (BART) in San Francisco was attacked by ransomware that encrypted the hard disk of the ticket machines (Masson & Gransart, 2017). All these examples demonstrated the vulnerabilities of modern rail systems to potential cyber attacks using different techniques.

In addition to the traditional cyber vulnerabilities associated with modern digital devices, the introduction of extensive communication networks[1] to connect these devices requires a systematic approach to enable the railroad administration to identify and understand cyber security vulnerabilities, risks, and their potential impacts on railroad operational safety and efficiency, which justifies an up-to-date overview for technologies, methodologies, and applications.

This section provides a summary literature review of the most widely used and adopted RIoT deployments. To bound the scope of the review, the research team also designed and distributed a cyber risk-oriented industrial survey for several North American railroads, and gathered the results related to cyber security practices and questions of interest. As a whole, the review and industrial survey results serve as a basis for selecting use cases to demonstrate the application of the risk review methodology. This methodology will be explained in more detail in Section 3 of this report, and its applications will be illustrated in Sections 4, 5, and 6. The literature review of this section also provides a summary of published practices of cyber security risks management, the associated analytic models, and corresponding technologies.

2.1 Literature Review

Topics covered include:

- Identification of previous significant cyber rail research efforts

[1] These communication networks include railroad-owned and commercial internet service provider's services, in the forms of both hardwired and radio frequency.

- Identification of cyber characteristics in RIoT systems: the cyber commonalities shared by various RIoT systems
- Identification of known RIoT system cyber vulnerabilities and corresponding cyber attack scenarios
- Identification of methods for estimating the chance of a successful cyber attack and the impact of the attack
- Identification of documented cyber security risk mitigation practices and available recommendations

2.1.1 Previous Cyber Rail Research

Rail cyber security risk management has attracted increasing interest among academia, industries, and government agencies. Several important projects for rail cyber risk reduction were funded or implemented in Europe, such as SECurity of Railways against Electromagnetic aTtacks (SECRET) (SECRET, 2015), SECured URban Transportation – European Demonstration (SECUR-ED) (SECUR-ED, 2014), and European Union Agency for Network and Information Security (Now EU Agency for Cybersecurity) (ENISA, 2004). In recent years, increasing research has been conducted to assess cyber security risk or to develop countermeasures to reduce the cyber security risk for railroad RIoT systems.

There also exist many related literature reviews summarizing cyber research efforts with cyber-physical infrastructure systems. For example, Cherdantseva *et al.* (2016) and Henrie (2013) respectively reviewed the methods of cyber security assessment and management for supervisory control and data acquisition (SCADA) systems. Cheminod *et al.* (2018) reviewed security issues in general industrial network control systems of similar critical infrastructure systems. Baumeister (2010), Lu *et al.* (2010), Wang and Lu (2013), and Yan *et al.* (2012) investigated cyber security in the smart grid electrical systems. However, none of them specifically covered cyber attack risk management in the rail transportation domain, which has its own unique operational and physical characteristics. Additionally, the identified and reviewed security literature also lacks a holistic approach to address security risks associated with concurrent, connected railroad systems. In fact, the research team has only identified limited prior research on the development of a comprehensive cyber risk management methodology tailored to the rail transportation sector. These past studies focused on security-related safety vulnerabilities of individual components, and did not consider the entire rail transportation system.

2.1.2 Cyber Characteristics of RIoT Systems

As expected, Positive Train Control (PTC) was identified as the RIoT system of the most interest to U.S. industry. Successful rail operations are predicated on the control and management of safe and efficient movements of rail vehicles. This naturally makes train control applications, of which PTC is one type, the most safety-critical RIoT component.

PTC is a type of communications-based train control (CBTC) widely implemented in the U.S. CBTC is a system of systems comprised of various RIoT subsystems and components, so the results of the reviewed literature addressing cyber characteristics of PTC are generally applicable to other RIoT systems and components. Analyzing CBTC-related similarities among rail

infrastructure, equipment, business orientation, and safety scopes have made it possible to extract the common fundamental features of train control systems and then the cyber features of RIoT systems. The results of the literature survey summarized in this section are therefore directly applicable to understanding the cyber framework for connected railroad operations. This section enables the identification of cyber-related components that may be compromised and provides a logical framework for understanding the interrelationship among cyber-physical system security, rail operations, and safety.

Communications-Based Train Control (CBTC)

Any train control system's design principle guarantees safe train separation upon desired capacity and safety improvements. These systems have evolved with the introduction of proven, low-cost, and highly efficient communication technologies capable of delivering messages in a timely and correct way to a remote location. Over time, these communications technologies have evolved from simple analog voice communication systems to advanced analog and then digital systems with significant functionality enhancements. These advanced systems are known as CBTC systems. According to IEEE Standard 1474.1-2004 (IEEE, 2005), these systems must provide:

1. High-resolution train location determination, independent of track circuits
2. Continuous, high-capacity, bi-directional train-to-wayside data communications
3. Train-borne and wayside processors performing vital[1] functions

Generally, the term CBTC is associated with rail transit passenger operations, but is usually not associated with general freight rail operations. This is because transit systems operate in an environment that allows for accurate train location determination independent of track circuits. This is not the case for current freight rail operators in the U.S.: the freight rail industry, due to a number of operational, regulatory, and commercial reasons, has been reluctant to get rid of track circuits because of various safety concerns (e.g., broken rail detection by track circuits). Eliminating the requirement for train location determination independent of track circuits, the remaining CBTC system functional requirements are naturally the pivotal and fundamental component of RIoT train control applications because all the functionalities are built upon cyber networks and wireless communication technologies. For the purposes of deriving the common cyber characteristics of RIoT systems, the research team thereby regards any RIoT applications qualified for any part of the IEEE 1474 standard as "CBTC" systems.

CBTC systems use communication technologies to achieve heterogeneous sub-functions to support the safe and efficient operational requirements. These common subcomponents and associated functionalities include, but are not limited to:

- Centralized traffic control (CTC) functions for efficient traffic management and safe train separation, providing both manual and automated train routing or scheduling capabilities while avoiding logic conflicts, and supporting higher traffic efficiency and flexibility.

[1] "Vital" has a very specific meaning – "fail-safe." See 1483-2000 – IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

- Essential communication links delivering messages to and from moving trains and miscellaneous wayside units to the office.
- CTC-associated wayside and onboard signaling and messaging systems to deliver the traffic commands to trains by traditional visual, audio or coded circuit signals, and/or varied forms of advancing transceivers towards onboard computers.
- The infrastructure items that directly involve train control actions, such as wayside control points and associated switches or derails, interlockings, grade crossings, movable bridges, miscellaneous yard components, etc.
- Location monitoring or positioning systems for trains and other involved vehicles to guarantee the accuracy and safety for the awareness of both CTC office and onboard forces.
- Onboard vital computer systems and their associated human interface to conduct the execution and/or enforcement for traffic dispatching commands.
- The SCADA system that controls overhead or third-rail traction power supply (where electrification is applicable) to support the normal operation and responsive fault handling.

The following three CBTC examples were selected and studied in more detail to define and generalize the cyber characteristics of RIoT:

- PTC developed in the U.S.
- European Train Control System (ETCS) and its derivatives
- ATACS version of Japanese Automatic Train Control (ATC) systems

These examples are briefly described and compared in the following sections.

PTC in the U.S.

The most widely implemented PTC systems in the U.S. are the Advanced Civil Speed Enforcement System (ACSES II, hereafter referred to simply as ACSES)[1] and the Interoperable Train Management System (I-ETMS).[2] Figure 2.1-1 illustrates the functionalities and the system structure of the current ACSES with optional wayside worker monitoring and protection. As one specific development of the PTC family, ACSES has been deployed mostly in the Northeast Corridor of the U.S. and operated mostly by Amtrak.

[1] A transponder-based system, originally put into use on the Northeast Corridor by the specific requirements of an Order of Particular Applicability.

[2] A GPS- and communications-based system adopted by the Class I railroads (and various passenger/commuter railroads) derived from the earlier Electronic Train Management System of BNSF Railway.

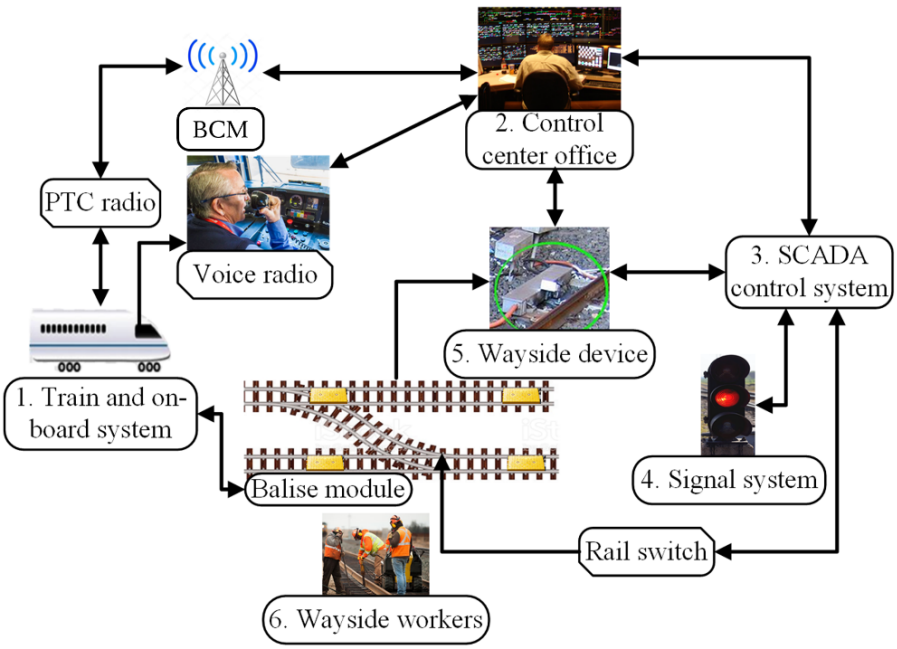


Figure 2.1-1 Architecture of U.S. PTC System – ACSES II

In the ACSES implementation, the control center office delivers the traffic controlling messages, or movement authorities (MA), through the PTC wireless radio links established between the onboard integrated module and the wayside base communication managers (BCM) using leased commercial carrier networks and/or dedicated private networks. In the initial design, the positioning data and permanent infrastructure speed limits are permanently preloaded into the passive transponder modules providing referencing information to the onboard system for adaptive braking calculation[1] at critical locations. The MA limits would further be transmitted downstream through active transponders using the radio links of the backhaul network. Such transponders and broadcasting wayside units are located at interlocking and control point locations to protect critical wayside units such as switches and home signals. Voice radios and visual signals also serve as a human-intervening methods in downgraded cases or special operation scenarios.

In the research scope, the PTC radio links and transponder-train communication links in this system are used by railroads, and would then introduce the rail-exclusive cyber features into the CBTC/RIoT applications. Except from the PTC radio links, the other backhaul network components such as railroad-owned voice radio links, signaling, and SCADA systems are also the research objects for railroad cyber integrity.

Another key system of the PTC family in the U.S. is the Interoperable Electronic Train Management System (I-ETMS). I-ETMS was developed by Wabtec Corporation and has been adopted by PTC-220 member railroads, including the major U.S. freight operators, to comply with a Congressional mandate.[2] The I-ETMS uses the same railroad-owned radio frequency as

[1] This is a limitation that is being addressed in the subsequent designs of ACSES, allowing the transponder information to be updated remotely using a combination of wired and wireless communication networks.

[2] Rail Safety Improvement Act of 2008 [DOCID: f:publ432.110], Public Law 110-432.

ACSES for wireless links. However, it uses completely different methods for modulation, data encoding, and channel access protocols. In addition, I-ETMS utilizes GPS plus dead-reckoning by the wheel odometer to track train location in lieu of transponders. Peer-to-peer communication technologies are also integrated into the system for interoperability and operational flexibility outside of base station coverage. While there are other nuances that exist, the functional structure and cyber components of I-ETMS could also be referred and formulated into the architecture described in Figure 2.1-1.

ETCS in Europe and China

In the 1990s, the major national European railways created the European Railway Traffic Management System (ERTMS) user group. This group, in conjunction with the major train control solution vendors, developed a unified train control system, ETCS, to resolve the interoperability issues of through-traffic among European countries. Interoperable railroad movements in the EU were complex, as some national rail authorities had already developed their own train control systems (for example: Germany and France, each with its own proprietary standards)[1], while other national rail authorities had no mature proprietary train control systems in place. These problems impeded efficient through-border rail traffic, especially for passenger services. To date, ETCS has successfully been developed into three different levels (0, 1, and 2); Level 2 (ETCS-2) is the most applied version in many countries. Meanwhile, Level 3 is still under development.[2] Because ETCS Level 2 is the most widely deployed system worldwide, the team chose ETCS-2 for further study.[3]

Figure 2.1-2 below shows the architecture of the ETCS-2/CTCS-3 system, where the lineside equipment unit (LEU) is equivalent to the wayside devices in the U.S. PTC concept. With extensive use of active trackside balises[4] communicating with the train's onboard computer and radio links established by GSM-R, the ETCS systems enable two-way messaging delivery for movement authority and feedbacking, signaling status, and train positioning data. GSM-R is an international wireless communications standard for railway communication and applications. GSM-R is based on the Global System for Mobile Communications (GSM) standard that was customized for railways' use. GSM-R was deployed mainly in Europe and Asia. Different GSM-R users (countries) can have their GSM-R specifications, such as allocated radio channel, modulation and data encoding methods. These protocols are mainly derived from the ETCS open standards, and numerous tests are being developed over the world for other wireless communication technologies.

---

[1] Even within the countries, multiple standards exist. For example, in Germany the most commonly used systems were Punktförmige Zugbeeinflussun (PZB) and Linienzugbeeinflussung (LZB), while France implemented three common different systems-Le Crocodile, Contrôle de Vitesse par Balises (KVB), Transmission Voie-Machine (TVM).

[2] Visit http://www.ertms.net/ for more information.

[3] Note that Level 3 of the Chinese Train Control System (CTCS-3) that is widely adopted in China's high-speed rail system is a close variant of ETCS-2.

[4] These correspond to transponders in the U.S. ACSES system.

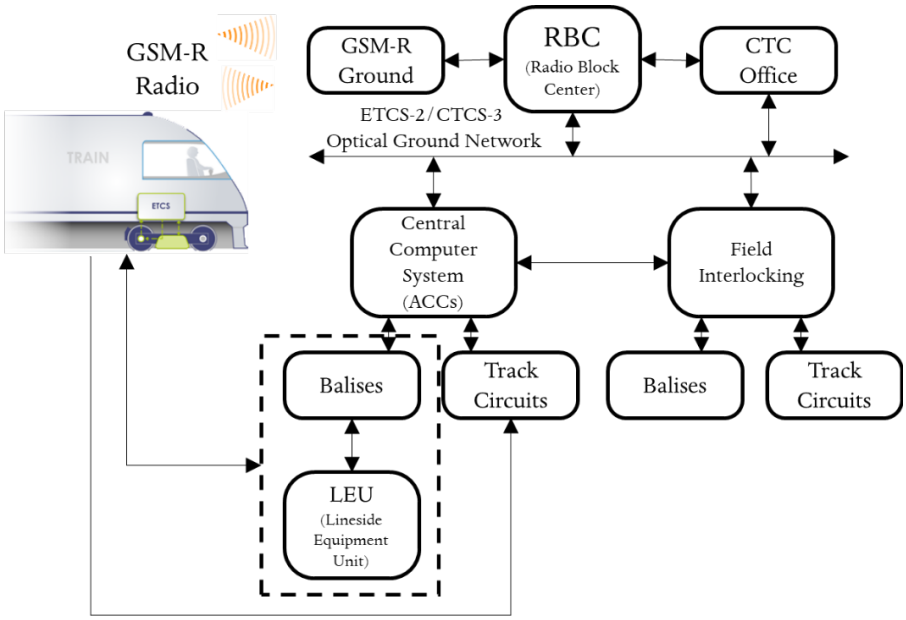


Figure 2.1-2 ETCS-2/CTCS-3 System Architecture

ATACS System in Japan

After the privatization of the Japan National Railway (JNR) in the 1980s, its successor operators developed individual train control systems based upon earlier JNR analog Automatic Train Control (ATC) developments. In principal, most of the conventional-line Japanese ATC systems or Shinkansen ATC systems are similar to different levels of ETCS, depending on the degree of digitization. Representative of these systems is the Advanced Train Administration and Communications System (ATACS). It was first developed by the East Japan Railway Company (JR-East)[1] since 1995 and put into operation on the JR-East Senseki Line as an ERTMS/ETCS Level 3 equivalent system in 2011. The ATACS train control method is fundamentally different from traditional signaling systems because train position detection is determined by onboard equipment rather than by track circuits.[2] Figure 2.1-3 below shows the system architecture for ATACS.

[1] See T. Kobayashi, O. Iba, H. Inage, and Y. Tateish, "ATACS (Advanced Train Administration and Communication System)," *Transactions on the Built Environment* vol. 18, 1996 WIT Press.

[2] See N. Miyaguchi, D. Uchiyama, I. Inada, Y. Baba, and N. Hiura, "The Radio-based Train Control System ATACS," *Transactions on the Built Environment* vol. 155, 2015 WIT Press.

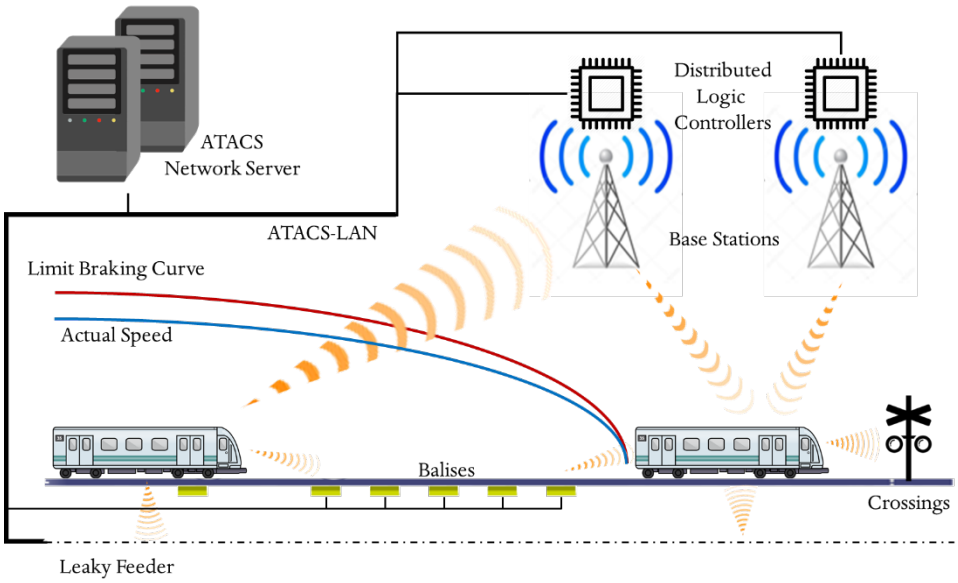


Figure 2.1-3 JR-East ATACS System Architecture

In the JR East ATACS implementation, the train control concept excludes track circuits but still maintains effective train detection and positioning with various approaches. Rather than solely depending on GSM-R (as in the case of ETCS Level 2 systems deployed in European and Chinese railroads systems), ATACS widely adopts leaky feeders (a.k.a. radiating cables) as well as active transponders in collaboration with GSM-like radio protocols (such as time-division multiple access [TDMA]) to achieve train-ground communication.

ATACS implements the concept of decentralized traffic control, where each distributed logic controller has its own vital jurisdiction to determine safe train separations, and coordinate with each other for moving authority issuing and interlocking logic processing. The train's onboard system coordinates with the ground network through transponders, leaky feeders or radio channels to dynamically adjust the braking curve with the accurate information exchange of train positions. This implements moving block traffic control[1] upon the decentralized traffic control schema. Distinctive from various transit CBTC systems customized for homogeneous traffic pattern, ATACS is designed for the upgrade of conventional rail lines in Japan's rail network that is compatible with mixed freight traffic with numerous grade crossings.

System Comparison

Table 2-1 compares the three preceding RIoT train control systems. Note that all systems require wireless communication integrity to support the system's safe and efficient operation. The six common train control functions critically supported by RIoT wireless communication are:

1. MA delivery and acknowledgement

[1] A moving block is a signaling block system where the blocks are defined in real time by computers as safe zones around each train. A moving block allows trains to run closer together, while maintaining required safety margins, thereby increasing the line's overall capacity.

2. Peer-to-peer communications among train, transponder/balise and wayside devices, field controllers, power supply units, base radio stations, etc.
3. Accurate and timely train positioning
4. System diagnosis for wayside devices and maintenance reporting
5. Wireless hand-over between adjacent regions, blocks, or different systems when trains are moving across
6. Fail-safe protections when wireless links become unreliable or under other special operation scenarios

These common traits form the basis of the literature review on vulnerabilities that may potentially compromise these functions.

Table 2-1 Lateral Comparison Among Selected RIoT Train Control Systems

	ACSES	I-ETMS	ETCS-2	CTCS-3	ATACS
Signaling	Cab+Wayside	Cab+Wayside	Cab+Wayside	Cab only	Cab only
Train-Ground Messaging Communication	Transponders +220 MHz Radio	220 MHz Radio	GSM-R Radio	GSM-R Radio	Balise+Leaky Feeder+TDMA Radio
Train Positioning	Transponders +Dead Reckoning	GPS+Dead Reckoning	Balise+Dead Reckoning	Balise+Dead Reckoning	Balise+Dead Reckoning
Traffic Blocking	Fixed	Fixed	Fixed (Virtual)	Fixed (Virtual)	Moving Block
Speed Enforcement	Responsive Penalty	Responsive Penalty	Automatic Train Protection (ATP)	Automatic Train Protection (ATP)	Preventive Dynamic

Note that while there are significant commonalities in functions, there are also significant operational considerations that will require further case-by-case analysis for their respective impacts on the cyber characteristics. These considerations include:

- Non-uniformity in rail operational conventions due to different operating practices[1]
- Varying degrees of interoperability between the independent railroad operators and lack of widely available consistent technical standards for RIoT technology[2]

[1] For example, in the U.S., operating practices are governed by two major sets of requirements – General Code of Operating Regulations (GCOR) and Northeast Operating Rules Advisory Committee (NORAC) Rules.

[2] In the U.S., the industry emphasis has established a significant degree of standardization in the areas of payload handing-over practices. For example, yard classification/marshalling exchange for carloads, locomotive exchange for passenger/unit trains, or container exchange for intermodal traffic are the common practices.

- Geographical differences of respective rail networks
- Various history backgrounds
- Various financial resources to implement RIoT technologies (different railroads have different financial profiles to support the cost of RIoT developments)
- Business protectionism among competitors

2.1.3 Identification of Attack Scenarios and Vulnerabilities

Railroad IoT systems and components consist of hardware devices, device drivers, and associated application programs. These all have individual vulnerabilities, which introduce various misuse cases that are potentially exploitable by attackers. Regardless of the motivations of the potential attackers, which are entirely speculative and outside the control of the railroad, the potential consequences of a successful attack shouldn't be out of the control. These consequences may include, but are not limited to, train derailment, train collision, fatalities of wayside workers hit by trains, and the disruption of train service. The following illustrates, in a non-comprehensive manner, one approach to identifying attack scenarios and vulnerabilities.

Attack Scenarios

The research team identified three common recurring attack scenarios, as shown in Figure 2.1-4:

1. Loss of train operation monitoring (unmonitored)
2. Malfunction of the signaling/SCADA systems or being under attacker's control
3. Malfunction of wayside devices (e.g., switch controllers) due to cyber attacks

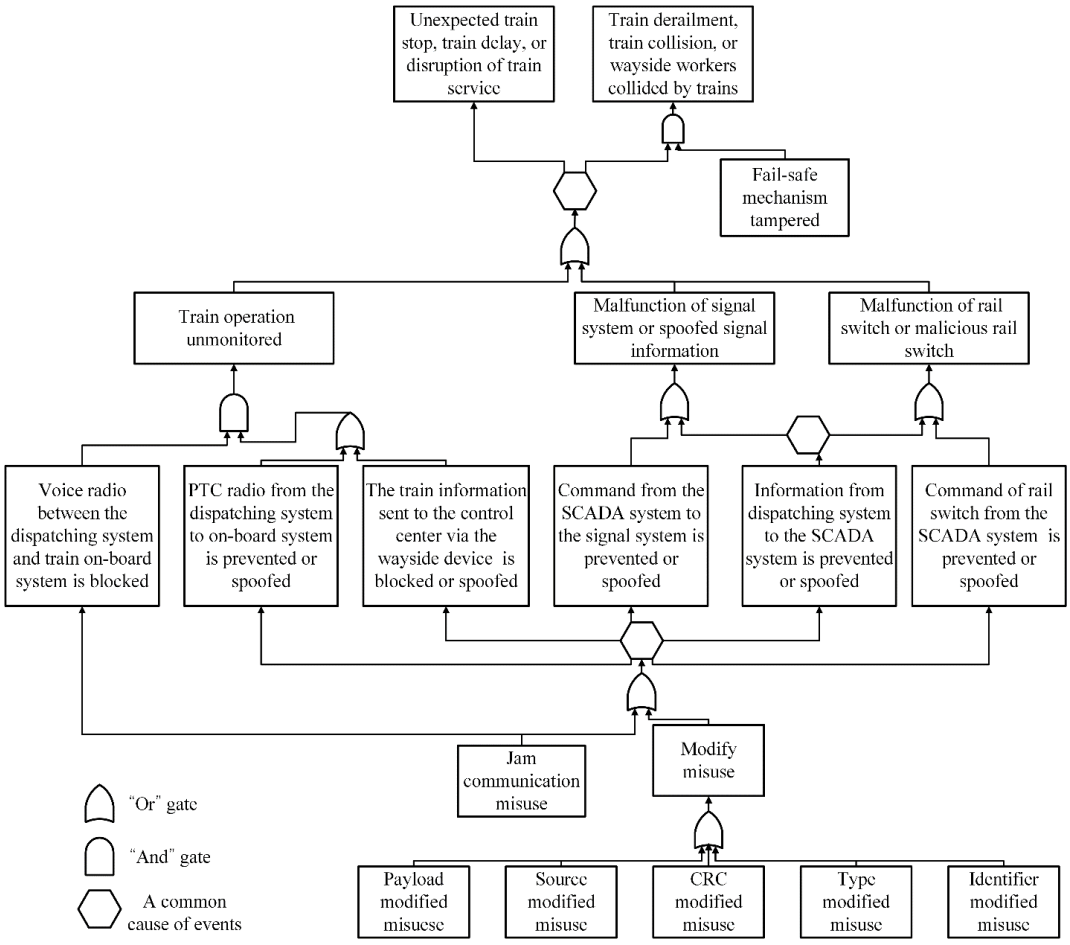


Figure 2.1-4 Misuse Cases of the RIoT/Connected Railroad Systems

Each of these three scenarios is discussed more fully in the following sections.

Loss of train operation monitoring (unmonitored):

Potentially compromised RIoT functions:

- MA delivery and acknowledgement
- Peer-to-peer communications among train, transponder/balise and wayside devices, field controllers, power supply units, base radio stations, etc.
- Accurate and timely train positioning
- Wireless handing-over between adjacent regions, cells, blocks, or different systems when trains are moving across

In most CBTC systems, the RIoT system determines train position based on data received from onboard sensors (e.g., tachometer readings, odometers, or GPS) or data from the absolute position reference (APR) transponders fixed on the track. Train speed is usually derived solely from onboard sensors. This data is used in conjunction with movement authority information (that may be exchanged via the radio links directly between the central office and moving trains) for critical functions, such as issuing moving authority, or taking preventive actions to enforce

moving authority. The scenario of an unmonitored train would occur if the CBTC system loses its ability to communicate with sensors or data internally or externally, or the train operation states cannot be accurately submitted to/received from the dispatching system.

For example, consider the case in the U.S. PTC ACSES system where radio messages used to deliver MA from the dispatching system to the onboard or wayside units are prevented (e.g., jammed) or spoofed (e.g., maliciously modified), so that radio links lose downstream efficacy, or when the train information sent from the onboard system to the control center is blocked or modified upstream. When any of these messages are spoofed or blocked, the moving train is unable to get the correct information for its MA limit, and the dispatching system is unable to get accurate information of train status. Consequently, the trains are left in an unmonitored state. Such a scenario leads the system to practice the various embedded fail-safe mechanisms.

Malfunction of the signaling/SCADA systems or being under attacker's control:

Potentially compromised RIoT functions:

- MA delivery and acknowledgement
- Peer-to-peer communications among train, transponder/balise and wayside devices, field controllers, power supply units, base radio stations, etc.
- Wireless handing-over between adjacent regions, blocks, or different systems when trains are moving across.

Some systems, such as the ETCS or ATACS, integrate the traditional signaling system functionality into the train control system. However, normal train operations in the U.S. still rely on a separate physical signaling system. Currently implemented PTC system in the U.S. acts as an additional safety overlay rather than as a replacement.[1]

Without a backup, the malfunction or external interference of such integrated signaling systems would lead to the disruption of train service. There are two typical message paths that convey the signaling information, both of which are vulnerable to cyber attacks when messages are prevented or spoofed:

1. Downstream information from dispatching system to the signaling system
2. The upstream command information communicating between the signaling system and the dispatching system[2]

While modern RIoT signaling/SCADA systems are often designed to allow maintenance mode or manual mode for special operations in the event of malfunctions (and could possibly be used

[1] Although not currently implemented, U.S. Federal regulations make provision for the use of PTC as the sole method of operation if the PTC system design can be demonstrated to be failsafe as described in 49 CFR 236 Appendix C.

[2] Although not directly related to the train control systems, a similar disruption to service can occur in electrified systems using communication-based SCADA systems for traction power supply control. Such traction power supply controlling SCADA systems (overhead catenary or third rail) may also have pair of links communicating with the center office and the signaling system, to establish logical signaling to prevent the hazards to traction power equipment. Disruption of any of these communications links can result in loss of service.

in situations arising from a cyber attack), such degraded state operations introduce new operational and safety risks.

Malfunction of wayside devices (e.g., switch controllers) due to cyber attacks:
Potentially compromised RIoT functions:

- Peer-to-peer communications among train, transponder/balise and wayside devices, field controllers, power supply units, base radio stations, etc.
- System diagnosis for wayside devices and maintenance reporting
- Fail-safe protections when wireless links become unreliable or under other special operation scenarios

Any failure or malfunction of their components could introduce operation hazards to train movements. A malfunction of a wayside device by itself, regardless of the cause, may not always result in catastrophic consequences such as derailments or train collision. However, such malfunctions would trigger designed downgraded states, stopping trains from entering the unsafe state, and causing service disruptions. The status of wayside devices is connected to the signaling system through multiple types of communication links[1], making the wayside devices and their vital logic accessible through wireless communication links or any wired forms of cyber connection.

The fail-safe mechanism, which is built in the field vital logic modules (where implemented), is the last protection layer preventing adverse safety consequences. Operational failures, such as a misaligned switch, gapped switch point position, or shorted track circuit, would also autonomously trigger a stop signal aspect in the signaling system thanks to the built-in fail-safe mechanism. Provided with the additional network connectivity to other regions, larger traffic disruptions can propagate due to embedded safety redundancy.

Communication Misuse

Communication timeliness and accuracy is essential to support the above-mentioned common train control functions. RIoT systems operate with stringent timing requirements and are dependent upon accurate messages. Common to all of the preceding attack scenarios is the misuse of the communications system. The research team classified communication misuses into two categories – radio jamming and data modification – both of which could affect the timeliness and accuracy of communications.

Radio Jamming Misuse
In the simplest form of jamming, the adversary transmits higher-powered radio signals in the same frequency band. Higher power levels than the original signal can overwhelm a receiver and then block communications.

More advanced forms of jamming are possible. There are several ways jammers can interfere with normal operations in a system. If remote access to the control center can be achieved, steering a receiving antenna, for example, to a null point can effectively silence a data link. In

[1] These include wired and wireless connections using a variety of both proprietary and open protocols.

addition to power- and frequency-based jamming, smart jammers are also a problem: there are designed techniques to disrupt wireless protocol operations instead of overwhelming the receiver with noise to achieve DoS.

Data Modification Misuse

Data modification misuse includes modification of one or multiple fields in a data packet. These include payload modification misuse (where the data content of the packets, such as the slow order messages containing temporary speed limit, is changed), source modified misuse (where the sender field is changed, such as from a wayside interface unit (WIU) to a signal point), cyclic redundancy check (CRC) modified misuse (modify the CRC bits contained in the message), type modified misuse (i.e., change the type of a message; for example, modifying from a keep-alive message to a speed restriction in some CBTC systems), and identifier modified misuse (where the message ID and/or the time stamp is changed).

Categorization of Reviewed Literature

There are numerous approaches to identification of attack scenarios and vulnerabilities. Table 2-2 provides a summary of literature reviewed that refers to cyber security in RIoT/connected railroad systems, categorized by identified attack scenarios.

Table 2-2 Applicable RIoT by Cyber Attack Scenarios

RIoT Systems	Attack Scenarios	References
General RIoT train control and signaling system (e.g., PTC, ETCS, various CBTC implementations, etc.)	Multiple attacks including electromagnetic interference, jamming, and, denial-of-service, message modification and unauthorized access, etc.	Bezzateev *et al.*, 2013; Bloomfield *et al.*, 2016; Bloomfield *et al.*, 2012; Chernov *et al.*, 2015; Craven, 2004; Flammini *et al.*, 2006; Hartong *et al.*, 2008a, 2008b; Hartong, 2009; Lopez & Aguado, 2015; Masson & Gransart, 2017; Pinedo *et al.*, 2016; Rodríguez-Piñeiro *et al.*, 2012
	Electromagnetic interference, jamming attack	Andre'B, 2014; Baldini *et al.*, 2010; Bandara, Kolli, *et al.*, 2017; Chang *et al.*, 2015; Heddebaut *et al.*, 2015; Heddebaut *et al.*, 2016; Heddebaut *et al.*, 2014; Mansson *et al.*, 2008; Mili *et al.*, 2015; Mili *et al.*, 2013; Sondi *et al.*, 2014; Xu & Zhu, 2017
	Brute force attacks, unauthorized access to the network, and message modification	Bantin & Siu, 2011; Chang *et al.*, 2016; Chen *et al.*, 2014; Chen *et al.*, 2011; Chothia *et al.*, 2017; de Ruiter *et al.*, 2016; Feuser & Peleska, 2010; Franekova & Chrtiansky, 2009; Franeková *et al.*, 2011; Franeková & Výrostko, 2012; Franekova *et al.*, 2013; Hartong *et al.*, 2006b; Koutsoukos *et al.*, 2016; Melaragno *et al.*, 2016; Nowakowski *et al.*, 2017; Temple *et al.*, 2016; Výrostko *et al.*, 2012
	Passive eavesdropping, active denial of control, and assumption of control	Hartong *et al.*, 2006a, 2006c, 2007, 2010
Transponder/balise data transmission	Compromise the availability or integrity of the balises' data, jamming, electromagnetic interference.	Harshan *et al.*, 2017; Lim *et al.*, 2017; Rodriguez *et al.*, 2016; Temple *et al.*, 2017; Wu *et al.*, 2017
Rail traction power supply & control systems	False data injection attacks, message modification, and unauthorized access to the network	Lakshminarayana *et al.*, 2017; Lakshminarayana *et al.*, 2016; Nguyen *et al.*, 2015; Teo *et al.*, 2016
Multiple types of human machine interface on RIoT	Multiple attacks including, DoS, message modification and unauthorized access, etc.	Bondavalli *et al.*, 2009; Grønbæk *et al.*, 2008
Public address or information display systems	Unauthorized intrusions	Chen *et al.*, 2014
Wayside devices	Both physical and cyber intrusion to lineside shelter protection system	Marrone *et al.*, 2015

In addition, the National Vulnerability Database at the National Institute of Standards and Technology (NIST) has provided a reference list of vulnerabilities with associated risk profiles and the systems known to have these risks.

Some researchers investigated vulnerabilities of RIoT systems based on a number of perspectives. These included the strength of defense, attacker effort, and achievable attack effects. Kohli (2016), for example, classified attacks and vulnerabilities by rail system target type (such as traffic management system, billing systems, telephony, remotely manageable infrastructure, confidential and safety information, corporate intranets, external websites and passenger information) that are vulnerable to cyber attacks. Tan and Ai (2011) categorized attacks and vulnerabilities from the perspective of cloud computing in high-speed rail systems such as abusing cloud computing, insecure interfaces, malicious insiders, shared technology issues, data loss or leakage, accounting services or hijacking, etc. Craven (2004) categorized attacks and vulnerabilities in terms of protocol vulnerabilities, dividing railroad wireless protocols into three groups: locomotive communications, wayside communications and train control communications. Chen *et al.* (2014) identified five attack scenarios in the CBTC systems. Bastow (2014) used some railroad cyber attack examples to identify the threats: computer viruses (e.g., Stuxnet, Trojan, etc.) collecting information, and then discovering vulnerabilities for subsequent analysis, followed by exploitation, and finally shutting down signaling or dispatch systems.

Other researchers have identified vulnerabilities in specific system technologies that are not necessarily related to rail operations. These include general complex cyber-physical industrial systems (Drago *et al.*, 2013; Marrone *et al.*, 2015), control systems (Mansson *et al.*, 2008; Wu *et al.*, 2017), signaling systems (Heddebaut *et al.*, 2016), communication systems (Chang *et al.*, 2015), etc.

One of the most interesting approaches to literature classification involves evaluating the applicability of specific attack scenarios from other critical infrastructure domains to the rail domain. Temple *et al.* (2016) translated attack scenarios identified by the National Electric Sector Cybersecurity Organization Resource (NESCOR) for the electric sector to the rail domain. Its work identified 123 attack scenarios in the electric domain that were applicable in the rail domain. Of the original electric power grid scenarios, for example, 64 (52 percent) were found to be applicable in the rail domain. The 64 scenarios were classified into 6 categories: message (spoofing, false data injection, or improper commands), malware, configuration (incorrect or compromised device or logical access control), inadequate access control, DoS, and absent or inadequate processes.

Regardless of the approach, of critical importance to note is that all of the efforts from the literature identified a large number of potential vulnerabilities and attacks that must be carefully considered by system designers/operators/owners to ensure that they have been considered and then mitigated. The potential vulnerabilities and attacks identified in the literature illustrate that industry efforts focusing on performance improvement may result in overlooking cyber security issues. Therefore, an increased focus on cyber security issues is crucial to develop safe and secure solutions.

2.1.4 Risk Assessment Reviewed for RIoT Cyber Security

Once cyber threat attacks and vulnerabilities have been identified, a risk assessment of the consequences of a successful attack and vulnerability exploitation is required to formulate the appropriate mitigations. Risk assessment is used for uncertain events that could have many outcomes and for which there could be significant consequences. Risk is a function of probability of an event (a particular hazard occurring) and the consequences given the event occurs. Probability refers to the likelihood that a hazard will occur. There are a number of different approaches to conducting the risk assessment that have been identified in the literature (see Table 2-3). Qualitative, probability, and consequence-based assessment approaches are discussed more comprehensively in subsequent sections.

Table 2-3 Literatures on Cyber Security Risk Assessment Methodologies

Cyber security risk assessment			No.	References
Qualitative assessment			12	Adin *et al.*, 2012; Andre'B, 2014; Bloomfield *et al.*, 2016; Bloomfield *et al.*, 2012; Craven, 2004; Dablain, 2017; Hartong *et al.*, 2006a, 2010; Kertis & Prochazkova, 2017; Lopez & Aguado, 2015; Rodríguez-Piñeiro *et al.*, 2012; Steen & Aven, 2011
Probability-based assessment	Simple probability analysis		3	Chothia *et al.*, 2017; de Ruiter *et al.*, 2016; Franekova & Chrtiansky, 2009
	Network-based models	Bayesian network	3	Drago *et al.*, 2013; Flammini *et al.*, 2006; Marrone *et al.*, 2015
		Tree-based models (e.g., fault tree, attack tree)	5	Bezzateev *et al.*, 2013; Chen *et al.*, 2014; Flammini *et al.*, 2006; Hartong *et al.*, 2006c; Temple *et al.*, 2016
		Petri Net	2	Drago *et al.*, 2013; Marrone *et al.*, 2015
	FMVEA		1	Chen *et al.*, 2014
Consequence-based assessment	Simulation		10	Chang *et al.*, 2015; Lakshminarayana *et al.*, 2017; Lakshminarayana *et al.*, 2016; Nguyen *et al.*, 2015; Rodriguez *et al.*, 2016; Sondi *et al.*, 2014; Temple *et al.*, 2016; Temple *et al.*, 2017; Teo *et al.*, 2016; Wu *et al.*, 2017
	Physical models		6	Lakshminarayana *et al.*, 2017; Lakshminarayana *et al.*, 2016; Lim *et al.*, 2017; Mansson *et al.*, 2008; Nguyen *et al.*, 2015; Wu *et al.*, 2017
	FMVEA		1	Chen *et al.*, 2014

Qualitative Risk Assessment

In a qualitative assessment, probability and consequence are not numerically estimated, but are evaluated using qualifiers like high likelihood, low likelihood, etc. Qualitative assessments are good for screening level assessments when comparing/screening multiple alternatives, or for when sufficient data is not available to support numerical probability or consequence estimates. Once numbers are inserted into the analysis (either by quantifying the likelihood of a hazard or quantifying the consequences), the analysis transitions to a semi-quantitative or quantitative risk assessment.

The most commonly used methods of qualitative risk assessment are description, stratification, and grading. Description-based methods qualitatively depict the formation process (likelihood) or the physical consequence of a cyber attack to the RIoT systems (Andre'B, 2014; Kertis & Prochazkova, 2017; Steen & Aven, 2011). Stratification provides different levels (e.g., low, medium, and high) to measure the likelihood or severity of cyber attacks to the RIoT systems (Bloomfield *et al.*, 2016; Bloomfield *et al.*, 2012; Lopez & Aguado, 2015). Grading approach assigns a score (usually from 0 to 1) to attack types to represent the likelihood of a successful cyber attack or the severity of attack consequences (Conklin, 2006; Fink *et al.*, 2013). These methods are used in general cyber security research and not specific to rail systems.

Probability-Based Assessment

Probability-based approaches support the model of a multi-stage attack process to demonstrate potential attack paths. Probability assessment methods can be classified into two categories, simple probability analysis and attack formation probability analysis. Simple probabilistic analysis estimates the probability of a single attack (e.g., brute-force key-guessing attacks) (Chothia *et al.*, 2017; de Ruiter *et al.*, 2016; Franekova & Chrtiansky, 2009). Attack formation probability analysis, including failure mode vulnerabilities and effects analysis (FMVEA) and network-based models, investigates the probability that the attack scenario is realized by analyzing precursor attack events and paths.

Simple Probabilistic Analysis

Simple probabilistic analysis estimates the probability of a single-step attack. For the example of a brute-force key-guessing attack, a simple probabilistic analysis calculates the total number of combinations of keys and then obtains the probability of correct attempts (Apostol, 2012; Cho *et al.*, 2011; Tsudik, 1992). Together with calculating the probability of a correct attempt, researchers also calculate the computational complexity of a successful attack by enumerating all keys to achieve successful attacks. However, simple probabilistic analysis only focuses on single-step attacks, and is not suitable for other more complex attacks (Chothia *et al.*, 2017; Franekova & Chrtiansky, 2009), and they cannot quantify the severity/consequences of the impact.

FMVEA

FMVEA is a qualitative analysis method, but can be made quantitative when mathematical failure models are used based on statistical data (Gürcan *et al.*, 2015). FMVEA has been widely applied to cyber security risk assessment (Gürcan *et al.*, 2015; Petit & Shladover, 2015; Schmittner *et al.*, 2015; Silva *et al.*, 2014). FMVEA is a highly structured and systematic technique for failure analysis that can help analysts identify vulnerabilities or attack scenarios, can be easily extended to estimate the impact (e.g., consequences), and can study potential causes in an element-by-element manner. However, because FMVEA divides the system into elements, it cannot provide the information about interactive effects of attacks and the joint threat to the overall system when multiple elements of the system are subject to a multi-stage cross-domain attack. Also, it is difficult for FMVEA to capture complex failure modes involving multiple failures within a subsystem (Lipol & Haq, 2011).

Network-based Models

Network-based models include tree-based models, Bayesian networks, and Petri nets. Tree-based tools (e.g., attack trees, fault trees) can model complex multi-step attacks by investigating a series of possible precursor events (Fovino *et al.*, 2009; Roy *et al.*, 2010; Xie *et al.*, 2013). The top node of the tree represents the attack goal. Each branch is the method (path) to achieve the ultimate goal by obtaining a series of precursor sub-goals. The leaves of the tree are individual attack activities that contribute to the sub-goals through the logic “AND” or “OR” gates (Bayuk & Mostashari, 2011). Tree-based models account for possible paths to achieve an attack scenario and thus enable decision makers to optimally deploy countermeasures to prevent the attack by cutting potential attack paths.

A Bayesian network is a graphical formulation of a series of variables and their causal relationships. Nodes in a Bayesian network represent the studied variables and the links are the causal relationships among these variables. The degree of causal relationships is determined by the conditional probabilities. Bayesian networks have been used for cyber security risk analysis in multiple transportation fields, but very few in RIoT cyber systems (Drago *et al.*, 2013; Marrone *et al.*, 2015).

A Petri net is a directed bipartite graph in which the nodes represent transitions (i.e., events that may occur, represented by bars) and places (i.e., conditions, represented by circles). The directed arcs describe which places are pre- and/or post-conditions for which transitions (signified by arrows). Tokens, denoted by black dots within places, specify the state evolution via the firing rule (Marrone *et al.*, 2015).

Network-based models are powerful tools for real-time cyber security analysis (Xie *et al.*, 2010). However, it is difficult to capture three types of uncertainty in network-based models:

1. Uncertainties of potential attack paths. Sometimes it is difficult to determine if two events have direct causal relationships, and thus the attack structure may be uncertain. In addition, uncertainties of the attack structures are also shown in the difficulty to investigate the exponentially increasing paths of potential attacks. Lastly, they do not easily address unexpected attack scenarios such as "zero day" attacks (AlEroud & Karabatis, 2012; Bilge & Dumitras, 2012).
2. Uncertainties associated with the probabilities of attacker actions. The probability that the attackers executing a particular attack is generally difficult to estimate.
3. Uncertainties of conditional probabilities on successful attacking events. After the casual relationship among events are determined, the conditional probabilities of these events are uncertain because of the lack of knowledge in various occasions.

Therefore, it is necessary to develop tools integrated with network-based models that enable analysts to model the physical consequences of cyber attacks to RIoT systems. For example, event trees can be used to analyze a chronological series of subsequent physical events or consequences caused by a successful cyber attack. However, to the best knowledge of the team, no research has combined such tools (e.g., event tree and simulation) with the attack tree or attack-defense tree to formulate the causes of a cyber attack as well as the consequence of a successful cyber attack to RIoT systems.

Consequence-Based Assessment

From the perspective of the system operator, consequence-based assessments provide the most meaningful way to evaluate the attack impact on railroad operations and best support both prioritization of mitigation actions and the effectiveness of those actions. Once a cyber attack occurs, compromised systems may trigger cascading effects to RIoT systems and their functions. For example, an attacker may introduce malware into a processor embedded into a signal system component to cause the malfunction of a signal. While compromise of a single embedded processor may not be of significant concern, the cascading consequences of such a compromise may be. The compromised processor may cause the signal system to function in a fail-safe manner. This in turn may result in a single train stoppage and delay, which in turn may create problems for dispatchers to meet train timetables, which in turn could adversely impact customer

service commitments resulting in adverse financial impacts on the railroad. Malicious changes to a track switch may give rise to probabilities of train derailments or collisions resulting in severe derivative consequences (e.g., fatalities and hazmat release).

Consequence-based assessments also support cyber resilience engineering of the systems. Cyber resilience engineering is based on the concept that successful detection and prevention of the all cyber attacks is highly improbable. System designs and mitigations should reflect this assumption, and be implemented in a way to minimize the adverse consequences while optimizing the remaining system performance. Researchers have shown growing interest in mitigating the consequence of a cyber attack in order to improve the resiliency of rail transportation systems (Heddebaut *et al.*, 2014; Pinedo *et al.*, 2016). Table 2-4 below lists the references that studied consequences of cyber attacks on RIoT systems.

Table 2-4 Literatures on Cyber-Attack Consequences on RIoT Systems

References	The RIoT systems studied	Attack scenarios	Consequences
Teo *et al.*, 2016	Urban train control system	Attackers remotely control the train to stop.	Train delay and passengers stranded
		False data injection (FDI) attacks on train-borne sensor measurements	Extra power consumption and rail voltage exceeding safety limits.
Temple *et al.*, 2017	Automatic train stop	Attackers compromise the availability or integrity of the balises' data.	The trains stop dozens of meters away from the right position, disrupting train service.
Chang *et al.*, 2015	Communications-based train control system	Jamming the leaky waveguide communications	Jamming the waveguide causes direct damage to the communication systems.
Rodriguez *et al.*, 2016	Balise-train communication system	Electromagnetic interferences	Unexpected train stop
Mansson *et al.*, 2008	GSM-R communication system	Intentional electromagnetic interferences	Direct damage to the communication systems
Lim *et al.*, 2017	Balise transmission modules	Data integrity threats to Balise transmission modules	Incorrect train stop position
Lakshminarayana *et al.*, 2017; Lakshminarayana *et al.*, 2016	Urban rail transit traction power systems	False data injection attacks	Extra power consumption and misleading trains' local voltages to exceed given safety-critical thresholds
Nguyen *et al.*, 2015	Rail feeder voltage control system	Signal delay attack, i.e.,, the timing information of voltage measurements is maliciously corrupted.	Unstable voltage output
Chen *et al.*, 2014	Communications-based train control system	Attackers compromise the train odometry and signaling network.	Train switches to fail-safe state due to lack of integrity and availability.
Wu *et al.*, 2017	Urban rail transit systems	Compromised human-machine interface sends malicious commands to devices, and SCADA systems suffer from DoS attacks.	Rail operation is disrupted, and control center loses sight of the status of devices and control center is unable to send commands to devices.

There are two broad approaches to consequence-based analysis: simulations and physical models.

Simulations

A simulation is a computer-based model of a real-world system operations. Researchers usually apply cyber-rail simulation (e.g., train motion simulation, traction power simulation, traffic control simulator, and network simulator etc. (Teo *et al.*, 2016)) to estimate the impact of cyber attacks to the RIoT systems, by comparing the simulation results with and without cyber attacks. Unlike analytical methodologies, simulation can assess the impact of attack scenarios in complex cyber rail systems (Chang *et al.*, 2015; Rodriguez *et al.*, 2016; Sondi *et al.*, 2014; Temple *et al.*, 2017; Teo *et al.*, 2016). Simulation is more flexible for cyber security risk analysis by allowing changes to the attack structure, probability, and consequences. However, similar to some

network-based models (e.g., a Bayesian network), knowledge of some of the required parameters in simulation are not known because of a lack of knowledge of a cyber attack in connected railroad systems cannot be expressed algorithmically, or the solutions are computationally complex (i.e., NP hard or beyond). Thus, uncertainty of input parameters of simulation should be considered when building reliable simulators.

Physical Models

Physical models study the consequences of cyber attacks on actual physical implementations of components of the rail systems, such as voltage control, train dynamics, traction power, movement trajectory, etc. Like computer-based simulations, researchers compare how these physical attributes change between "normal" (non-attack) and attack operations scenarios to estimate the impact of cyber attacks. For example, Nguyen *et al.* (2015) studied the cyber security risk of the traction power voltage control that regulates the voltage of rail power feeder substations. If the control system is attacked, the timing information of voltage measurement is corrupted so that the system uses the wrong measurements to make control decisions. Temple *et al.* (2016) used a physical model to study the impacts of balises' data alteration on the deceleration of a train and thus obtained the difference between a train's actual stop position and its required stop position. However, physical models are difficult to develop accounting for complex consequential paths and logical dependencies.

2.1.5 Mitigation Strategies Reviewed for RIoT Cyber Security Risks

General cyber security risk mitigation objectives are confidentiality, integrity, and availability. Confidentiality ensures that the data are not disclosed to unauthorized subjects. Integrity guarantees that information is not changed. Availability is the uninterrupted accessibility to the information and the system (Bloomfield *et al.*, 2016). According to Bloomfield *et al.* (2016), RIoT cyber security objectives come in the order of priority: integrity, then availability, and confidentiality. This is because loss of integrity may result in risks for accidents, loss of availability may cause delays and suspension of rail services, and loss of confidentiality may result in leaking of sensitive operational or financial information.

Several researchers have proposed mitigation strategies to reduce the cyber security risk of RIoT systems. Hartong *et al.* (2006a), for example, indicated that the preferred mitigation methods for passive attacks are access control and confidentiality, and the preferred mitigation methods against active attack include access control, availability, accountability, authentication, and integrity.

In this report, cyber security risk countermeasures are classified into two main categories – technical strategies and administrative strategies – that can and should be applied concurrently. Technical strategies focus on detection, prevention, and impact mitigations. Intrusion detection strategies (e.g., IDS) monitor the systems to detect malicious activities or policy violations. Prevention mechanisms (including authentication, authorization, access control, encryption, etc.) work to protect the system from attacks. Impact mitigations, also known as cyber resilience, are designed mechanisms that can decrease the negative consequences to the system if it is successfully attacked. Administrative strategies include training operation rules, improving awareness, configuration management (e.g., software patching and updating), and system maintenance. Table 2-5 summarizes previous studies for RIoT studies based on this countermeasure classification.

Table 2-5 Literature Review Summary of Cyber Security Risk Mitigation Strategies

Countermeasures	Ref.	Description of mitigation strategies or technologies
Detection techniques	(SECRET, 2015)	Developed a detection mechanism based on spectrum statistics, quadratic analysis and time characteristics
	Lakshminarayana *et al.*, 2017; Lakshminarayana *et al.*, 2016	Proposed intrusion detection systems (IDS) consisting of bad data detection and secondary attack detection mechanism
	Chernov *et al.*, 2015	Used a rough set of theory-based anomalies to detect abnormal activity
	Melaragno *et al.*, 2016	Designed a rail radio intrusion detection system for radio signaling
	Heddebaut *et al.*, 2015	Proposed a signal-jamming detection mechanism
	Baldini *et al.*, 2010	Proposed an early warning system for detecting GSM-R wireless interference
	Mili *et al.*, 2015	Developed a jamming detection system
	Mili *et al.*, 2013	Developed a pattern recognition-based intrusion detection mechanism
Prevention mechanisms	Hatzivasilis *et al.*, 2017	Proposed a real-time management of railway systems. The mechanism provides user authentication, agent actions authorization against agent permissions, and message signing and encryption.
	Tan & Ai, 2011	Proposed a cloud security reference framework with authentication, access management and encryption
	Koutsoukos *et al.*, 2016	Used hash-based message authentication system and firewalls
	Schlehuber *et al.*, 2017	The presented security concept includes monitoring and information systems as well as basic security building blocks such as cryptography and packet filtering.
	Zhu *et al.*, 2016	Proposed an authentication protocol referred as adaptive and lightweight protocol for both hop-by-hop and end-to-end authentications (ALPHA)
	Hartong *et al.*, 2008b	Designed a trust management system with online key exchanges
	Hartong *et al.*, 2006b	Proposed a cryptography based key management system (KMS). Analyzed transmitting delays resulting from preparing the data for transfer and decoding for block encryption algorithms and integrity
	Hartong *et al.*, 2006c, 2007	Proposed a distributed trust management system to enable PTC use cases and eliminate identified misuse cases
	Hartong, 2009	Integrated trust management with train scheduling
	Chen *et al.*, 2011	Recommended to improve communication protocol by (1) adding advanced scheme of establishment of safe connections, and (2) adding double serial numbers as replacements for time stamp
	Bondavalli *et al.*, 2009	Designed a safety architecture and wireless communication protocol for driver-machine interface
	Bantin & Siu, 2011	Designed security gateways consisting of authentications and proxies
	Harshan *et al.*, 2017	Proposed a new communication framework called cryptographic random fountains transmitting telegrams containing of random signals
	Franeková & Výrostko, 2012	Proposed a key management system using elliptic curve cryptography
	Franekova & Chrtiansky, 2009	Developed a key management system for ETCS
	Chang *et al.*, 2016	Developed a two-layer dynamic key update scheme
	Výrostko *et al.*, 2012	Developed multiple cryptographic techniques
	Feuser & Peleska, 2010	Combined open-source software and proprietary system-specific code, and virtualization mechanism of hardware
	Bandara, Kolli, *et al.*, 2017	Developed a mechanism of Secure Intelligent Radio for Trains (SIRT) to improve the reliability and security of the radio communication
	Grønbæk *et al.*, 2008	Proposed a secure communication protocol for the safety layer
	Hartong *et al.*, 2006a	Recommended to use access control and confidentiality to prevent passive attacks, and to use access control, availability, accountability, authentication, and integrity to prevent active attacks
	Zones, 2013	Defined a security zone architecture for rail transit to protect critical zones
	Temple *et al.*, 2017	Proposed software-only countermeasure using high-fidelity train braking models to minimize the stop position error
Impact mitigations	Xu & Zhu, 2017	Applied a multi-channel model to enhance the reliability of the communications and developed a zero-sum stochastic game to capture the interactions between a transmitter and a jammer
	Heddebaut *et al.*, 2014	Proposed a resilient communication architecture consisting of a detection system and a multipath communication system

Prevention mechanisms and detection techniques	Pinedo *et al.*, 2016	Proposed an adaptable communication resilience architecture consisting of three main blocks: an acquisition system, a detection system and a multipath communication system
	Lopez & Aguado, 2015	Provided four main recommendations: a robust cryptography based new key distribution scheme, a new key storage and a system integrity module and a set of countermeasures for avoiding radio jamming
	Wu *et al.*, 2017	Recommendations: detecting jamming attack, mitigating faking attack, defeating replay attack
Detection techniques and impact mitigations	Lim *et al.*, 2017	Device level: cryptographic solution; system level: secure hybrid train speed controller to mitigate the impact.
Prevention mechanisms and impact mitigations	Huang & Milius, 2016	Developed a set of human-factor-based operational rules
Administrative strategies include training operation rule, improving peoples' awareness, configuration management, and system maintenance.	Heddebaut *et al.*, 2016	Recommendations: increasing the base station (BS) radiated power, switching from the front to the rear train antenna system, using a high front-to-back train antenna to prevent jamming attacks
	Dablain, 2017	Recommendations: penetration testing of backdoors and services, employee training, equipment updates, putting the system on air gap networks
	Czescik & Siemianowski, 2014	Recommendations: education of institutions, adoption of permanent rules of law enforcement cooperation with private sector entities
	Kohli, 2016	Developed a cyber security asset management framework for railway system in UK
	Hartong *et al.*, 2008a	Appeal to collaborate with public, private and international organizations to address cyber threats to railway systems
	Bastow, 2014	Introduced three categories of countermeasures, technological (e.g., firewall and IDS), social (e.g., training and awareness) and procedural (e.g., maintenance and data logging).
Mixed administrative and technical strategies	Mansson *et al.*, 2008	Developed a framework for improving critical infrastructure cyber security with core functions of detection, protection, response, and recovery
	SS-CCS, 2010	Recommendation: protecting the operationally critical security zone by prevention of human error and detection of abnormal or unauthorized activity

Countermeasures to Railway Communications Cyber-Attacks

As previously indicated in the Section 2.1.3, RIoT/connected railroad systems are heavily dependent on wired and wireless communications. Countermeasures against attacks to wired communications are very similar to traditional communications security practices, where the uses of authentication (sometimes multi-factor), challenge response protocols, and hashing and encryption are common to ensure integrity and confidentiality. These techniques are also applicable for wireless protocols. However, due to the nature of common RIoT communication protocols, the limited bandwidth and strict timing requirements to deliver messages induce challenges for cost-effective methods to enhance cyber security in RIoT systems. Other aspects of wireless techniques such as dynamic modulation and scaling, frequency hopping (a.k.a. dynamic channel selection), and multiple protocols (such as proprietary, carrier-grade telecommunications backup, Wi-Fi, etc.) have been proposed (Bandara, Kolli*, et al.*, 2017; Bandara, Melaragno*, et al.*, 2017). The objective of these two works was to manage available limited bandwidth in a way that minimizes the impact on safety. These methods have been backed up using IDS solutions customized for U.S. PTC protocols (Bandara *et al.*, 2016; Kolli *et al.*, 2018).

Operation Research for Risk Management

Evaluating optimally effective countermeasure strategies is a problem in operation research. Cyber operation research optimally allocates available resources to mitigate cyber security risk. This subsection summarizes two commonly implemented operation research approaches to such optimizations: portfolio optimization and game-theoretic models.

Portfolio Optimization

Portfolio optimization is inspired by the knapsack problem (Chu & Beasley, 1998). The basic idea is to optimally select countermeasures to be implemented under a limited budget with the objective of mitigating the harmful impact of a cyber attack to the maximum extent or minimizing the potential losses from successful cyber attacks (Fielder *et al.*, 2016; Ojamaa *et al.*, 2008; Rakes *et al.*, 2012; Sawik, 2013; Srinidhi *et al.*, 2015). The selection of countermeasures is based on their effectiveness of preventing attacks, reducing the probability of potential attack scenarios, and mitigating the impact and consequence of the attack, as well as their implementation cost of countermeasures, etc. Portfolio optimization considers multiple mitigation strategies that can obtain the optimal combinations of possible options but does not consider the interactive relationship between defense and attack. To the authors' best knowledge, no researchers to date have applied portfolio optimization techniques in RIoT cyber security risk management.

Game-theoretic Models

Game theory is an effective tool that models the interactions between attackers and defenders. The basic idea of game-theoretic models is that the attacker aims to maximize the severity of the attack while the defender's objective is to minimize the impact of an attack. Game-theoretic models focus on the conflicting situations of participants (attackers and defenders) so that the participants' behaviors can be predicted. Most researchers seek the equilibrium state of attackers' and defenders' behaviors. Many references have applied game theory to study the interactive actions between attackers and defenders (Bhattacharya & Başar, 2010; Du *et al.*, 2014; Moayedi & Azgomi, 2012; Rao *et al.*, 2014; Rao *et al.*, 2016; Shiva *et al.*, 2010; Xu & Zhu, 2017). However, among all of these references, only Xu and Zhu (2017) focused on rail systems, which used game theory to model the interactions between the rail transmitters and a jammer.

2.2 Industrial Survey

The survey aims to identify the RIoT systems that have been adopted by U.S. railroads and the cyber security approaches that currently are or in the consideration of being adopted by U.S. railroad operators. To select the appropriate RIoT systems for further study, the research team communicated with several industrial practitioners in the U.S., via an online survey.

2.2.1 Survey Questions

The survey solicited industry information in four general areas:

1. What connected railroad systems are used?
2. What systems are possibly exposed to cyber attack or interference?
3. What security measures are being used?
4. What emerging communications-based, connected railroad technologies may be considered for cyber security risk management?

Table 2-6 below is the exact survey questionnaire the research team has distributed to the U.S. railroad practitioners:

Table 2-6 Survey Questions

1. Your name and your company?
2. What is your contact information, email and/or phone number?
3. What safety related systems do you have that use internet connections to pass data?
4. How do your dispatching systems communicate with wayside interlockings and control points? 4 (a). Is the communication path of your dispatching system through a dedicated closed network controlled by the railroad? 4 (b). Does your railroad dispatching system use leased lines for this purpose? 4 (c). Does your railroad dispatching system use a closed network? If yes, is there a way for an employee or contractor to access the system externally?
5. Does your railroad use a Supervisory Control and Data Acquisition (SCADA) system for traction control (electrified railroad) or for some other purpose? 5 (a). If so, how does your SCADA system communicate with devices in the field? Is the communication path through a dedicated closed network controlled by the railroad? 5 (b). Does your railroad SCADA system use leased lines for this purpose? 5 (c). Does your SCADA system use a closed network? If yes, is there a way for an employee or contractor to access the system externally?
6. Does your railroad use remote control of locomotives in train consists or in yards? 6 (a). If so, what security measures are in place to prevent someone else from taking control?
7. Does your railroad use radio code lines for control of switches and signals? 7 (a). If yes, what security measures has your railroad taken to prevent unauthorized control of these devices?
8 (a). What security measures is your railroad taking to safeguard the data radio system in Positive Train Control (PTC) system? 8 (b). What security measures is your railroad taking to safeguard the back office to back office communication system in PTC? 8 (c). What security measures is your railroad taking to safeguard other transmitting system of data or safety related information in PTC?
9. What safeguards are being implemented by your railroad to ensure the integrity of defect detectors?
10. What other systems (e.g., safety related systems, business systems, and systems involved in operation of trains) does your railroad use that are possibly exposed to cyber attack or interference?
11. Does your railroad have a plan in place to identify and mitigate cyber security risks?
12. Is there a specific area of cyber security risk that you feel needs closer attention, industry collaboration or research to help the industry mitigate the risk?
13. In addition to the above-mentioned technologies, what are other existing or future communications-based, connected railroad technologies that your company implements or considers?
14. What would this research project benefit your railroad or what are additional areas of interest to your company? Please list them.

2.2.2 Industrial Survey Responses

Nine railroads responded to the survey.[1] Researchers found that the most mentioned connected railroad system in the U.S. was the PTC system. Besides PTC, other commonly mentioned systems included: smart-link payment card systems, ticket vending machines, HR/payroll, financial systems, access control and video security systems, building management systems, tunnel ventilation systems, business systems, new Wabtec's TMDS® (Traffic Management and

[1] Canadian Pacific, Conrail Shared Assets, CSX, NICTD, NJ Transit, PATH, the Belt Railway of Chicago, and two other anonymous railroads.

Dispatching System)[1], VHF/UHF, and microwave radios that were of interest to some respondents. Advanced Train Control System (ATCS), bridge remote control, and remote yard operation systems are other connected railroad technologies that are being used or considered for future use.

Regarding communication systems, railroads reported a mix of leased lines and railroad-owned local network "code lines" either via radio or direct internal fibers. For most of the respondents, the communication networks in dispatching systems and SCADA systems are thought of as a dedicated closed network controlled by the railroad.[2] For some railroads, their closed network cannot be accessed by employees and contractors externally.

Commonly used cyber security measures include IDS/IPS intrusion detection/prevention systems, firewalls, HIPS (host intrusion prevention systems), authentication, firewall, anti-virus/malware and SFTP (secure file transfer protocol), log collection, encryption, dedicated equipment, and physical "air-gap," etc. A summary of specific responses to individual survey questions are shown in Table 2-7 below:

Table 2-7 Industrial Survey Responses

Questions	Summary of Responses
Q3	Three companies explicitly mentioned that they use the PTC system. Another company mentioned that they have a perimeter intrusion detection system. One company has a Cisco ISE (Identity Services Engine) system, a Princeton KES and COSMA servers, anti-virus/malware, and SFTP connections to protect their railroad systems. One company said that the access is authenticated by username and password.
Q4	Seven responses were collected, indicating that they have various types of communications, such as leased line, local network code lines, via radio or direct internal fiber.
Q4(a)	Eight responses were collected. Five companies' communication paths are through a dedicated closed network. One company does not use a dedicated closed network. Two responders did not know.
Q4(b)	Eight responses were collected. Four companies use leased lines; three companies replied that they do not use leased lines. One responder did not know.
Q4(c)	Eight responses were collected. Except for one responder who did not know the answer, the other seven companies use closed networks. In four companies, employees or contractors can access the closed system externally, while the other three companies cannot.
Q5	Eight responses were collected. Five companies use SCADA system, while only one company does not. The other two responders did not know.
Q5(a)	Eight responses were collected. Six companies' communication paths are through a dedicated closed network for SCADA system, one company does not have SCADA system, and the other responder did not know.
Q5(b)	Eight responses were collected. Four companies' railroad SCADA systems do not use leased lines, two companies use leased lines, and the other two responders did not know.
Q5(c)	Eight responses were collected. Except for three responders who did not know, the other five companies use closed networks for their SCADA systems. Among the five companies, three companies' closed networks do not allow employees or contractors to access the system externally, while two companies' closed networks can be accessed.

[1] TMDS is an automated dispatching system adopted by a large number of railroads implementing the I-ETMS PTC system.

[2] Note that many of networks considered as dedicated closed systems under railroad control are actually provided by commercial telecommunications as leased lines under various service level agreements.

Questions	Summary of Responses
Q6	Among the eight collected responses, four companies use remote control of locomotives in train consists or in yards, three companies do not use remote control, and one company did not know.
Q6(a)	Three responses: 1) uses "firewalls" and DMZ servers; 2) uses the AAR standard; 3) uses a pitch/catch type of authenticated message via 460 MHz Radio.
Q7	Among the eight collected responses, three companies use code lines for control of switches and signals, four companies do not use code lines, and the other one responder did not know.
Q7(a)	Only one responder knows that their company focuses on physical security of devices.
Q8(a, b, c)	IDS/IPS intrusion detection/prevention systems firewalls, HIPS (host intrusion prevention systems), managed data center with levels of cyber security, log collection, encryption, firewalls & DMZ, along with ID password controlled access to system, dedicated equipment, user controls, and physical "air-gap," etc.
Q9	Three valuable responses were collected: 1) a network management system to monitor network and communications traffic as well as a Cisco system to monitor devices; 2) rigorous testing, alerting, and inspections; 3) fenced areas and deployment of video cameras where possible.
Q10	Smart-link payment card system, ticket vending machines, HR/payroll, financial systems, access control and video security systems, building management systems, tunnel ventilation system, business systems, new Wabtec TMDS® system, and VHF/UHF (very high frequency/ultra high frequency) and microwave radio are all possible to be exposed to cyber attacks.
Q11	Nine responses were collected. Eight companies have a plan to identify and mitigate cyber security risks.
Q12	People think that centralized traffic control (CTC) code lines (ATCS systems), FRA/TC test reporting systems, industrial control systems (ICS) and ecosystem of subcontractors, NIST 800 for all ICS, and physical systems need closer attention.
Q13	A handheld system for the field crews to use to monitor and help control train authority, Bluetooth, bridge remote control, and remote yard operations.
Q14	1. Interchange data, remote control of bridges, detector security 2. Intelligent transportation systems, building and facility management, tolling systems, automating network management & maintenance, mobile smartphone and payment processing systems 3. Motion detection, and intrusion detection with the help of automated notifications in yards and in critical but remote areas

3. General Risk Management Methodology and Use Case Identification

In this section, the research team describes the proposed methodology for cyber risk management of RIoT use cases. After describing this methodology, the team discusses the process by which the RIoT use cases in Sections 4, 5, and 6 were selected for demonstrating the applications of this methodology. The general methodology focuses on the common critical steps to conduct cyber risk management on a certain RIoT system. The methodology aims to serve as a guideline for stakeholders to develop the knowledge repository of the respective items that they concern.

This methodology synopsizes and augments the approach presented in National Institute of Standards and Technology (NIST) Special Publications 800-160 Volume 1, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems" (Ross *et al.*, 2018), NIST Special Publication 800-160 Volume 2, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach" (Ross *et al.*, 2019), and NIST Special Publication SP 800-82 Rev. 2, "Guide to Industrial Control Systems (ICS) Security" (Stouffer *et al.*, 2011). It does not replace the recommendations of these publications, rather it tailors and presents the information in a way that more appropriately meets the immediate needs of practicing railroad industry and government staff who do not possess an extensive cyber security background.

3.1 General Cyber Risk Management Methodology

This section describes the recommended six-step risk management methodology for a selected RIoT use case. It defines the key engineering activities that are required to be conducted. The methodology is independent of system type and engineering or acquisition process model. While it is described as a linear sequence of flows or process steps (Figure 3.1-1), it is actually an iterative process (Figure 3.1-2). Like the more complex NIST model on which it is based (Ross *et al.*, 2018), it emphasizes an integrated, holistic security perspective across all stages of the system life cycle.[1] The specific cyber risks will vary based on the specific application, implementation, positions of in the system life cycle where the application is, as well as the threat and its capabilities. Each major step in the process will be explained in the following subsections.

[1] The term life cycle refers to all processes and activities associated with the system including, but not limited to: processes and activities related to development; prototyping; analysis of alternatives; training; logistics; maintenance; sustainment; evolution; modernization; disposal; and refurbishment. Each activity has security considerations and constraints that must be considered to ensure that security objectives for the system can be met. Depending on the phase of the life cycle, the application of the use/misuse case approach can affect such things as Requests for Information, Requests for Proposal, Statements of Work, source selections, development and test environments, operating environments and supporting infrastructures, supply chain, distribution, logistics, maintenance, training, and personnel clearances/background checks.

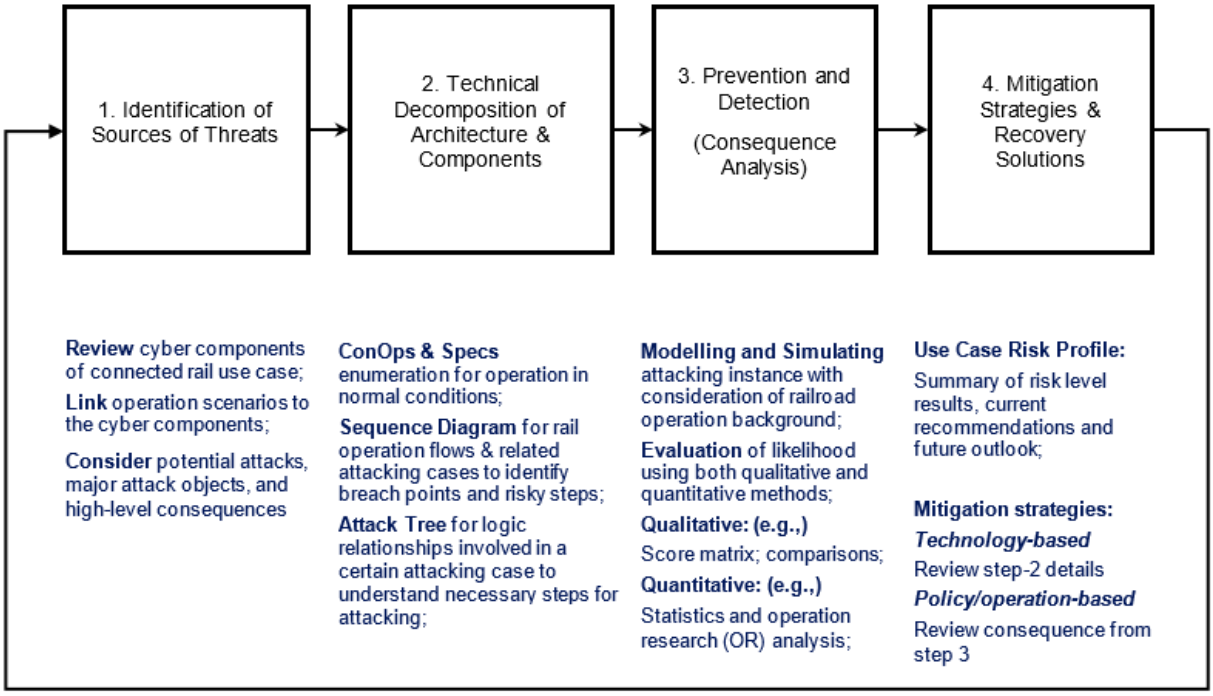


Figure 3.1-1 Execution Flow of RIoT Use Case Risk Management

The recommended methodology is also a loop process, involving a series of iterative steps in risk management (Figure 3.1-2).

Figure 3.1-2 Looping Process of General Risk Management Methodology

3.1.1 Identification of Threats

Threats are "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or DoS, as well as the potential for a threat-source to successfully exploit particular information system vulnerability" (CNSS, 2015).

Threat actors are "causal agents with the capability to exploit a vulnerability to cause harm." Collectively they represent the threat source. Potential PTC threat actors are based on NIST SP 800-82 Rev. 2 (Stouffer et al., 2011), and include:

- Individual attackers
- Bot-network operators
- Criminal groups
- Foreign intelligence services
- Insiders
- Phishers
- Spammers
- Spyware/malware authors
- Terrorists and industrial spies
- Supply chain attackers

Threat actors are not equal in terms of capability and sophistication and have a range of resources, training, and support for their activities. They may operate on their own or as part of a larger group (i.e., a nation-state intelligence program or organized crime group).

One threat model (Hughes & Cybenko, 2014)[1] (Hughes & Cybenko, 2014) postulates that any successful exploitation of a system vulnerability requires three elements to coexist: system susceptibility, threat accessibility, and threat capability (Figure 3.1-3).

[1] An empirical approach first developed by the U.S. Air Force Research Laboratory (AFRL) for secure system research and development.

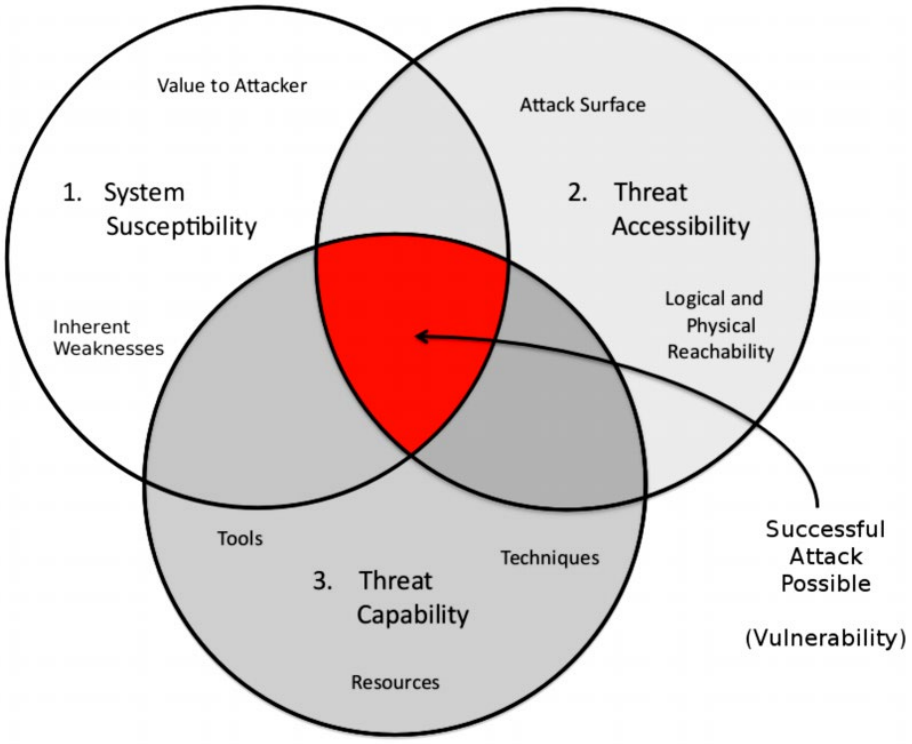


Figure 3.1-3 Vulnerability Venn Diagram

(Adapted from Hughes and Cybenko (2014))

The identification of cyber threats from a RIoT use case involves three following major steps:

1. Identifying system susceptibilities
2. Identifying threat accessibility
3. Identifying threat capability

Identifying System Susceptibility

Figure 3.1-4 illustrates one categorization of threats to a RIoT. These can arise from several source types: human, technological, and environmental. Value to the attacker is a function of the motivation of the threat actor and is an open research question involving social, psychological, business, economic, political, cultural, and other issues. As this is outside the control of the railroad technical staff, the focus of identifying system susceptibility will focus on the inherent weaknesses that the attacker could potentially exploit.

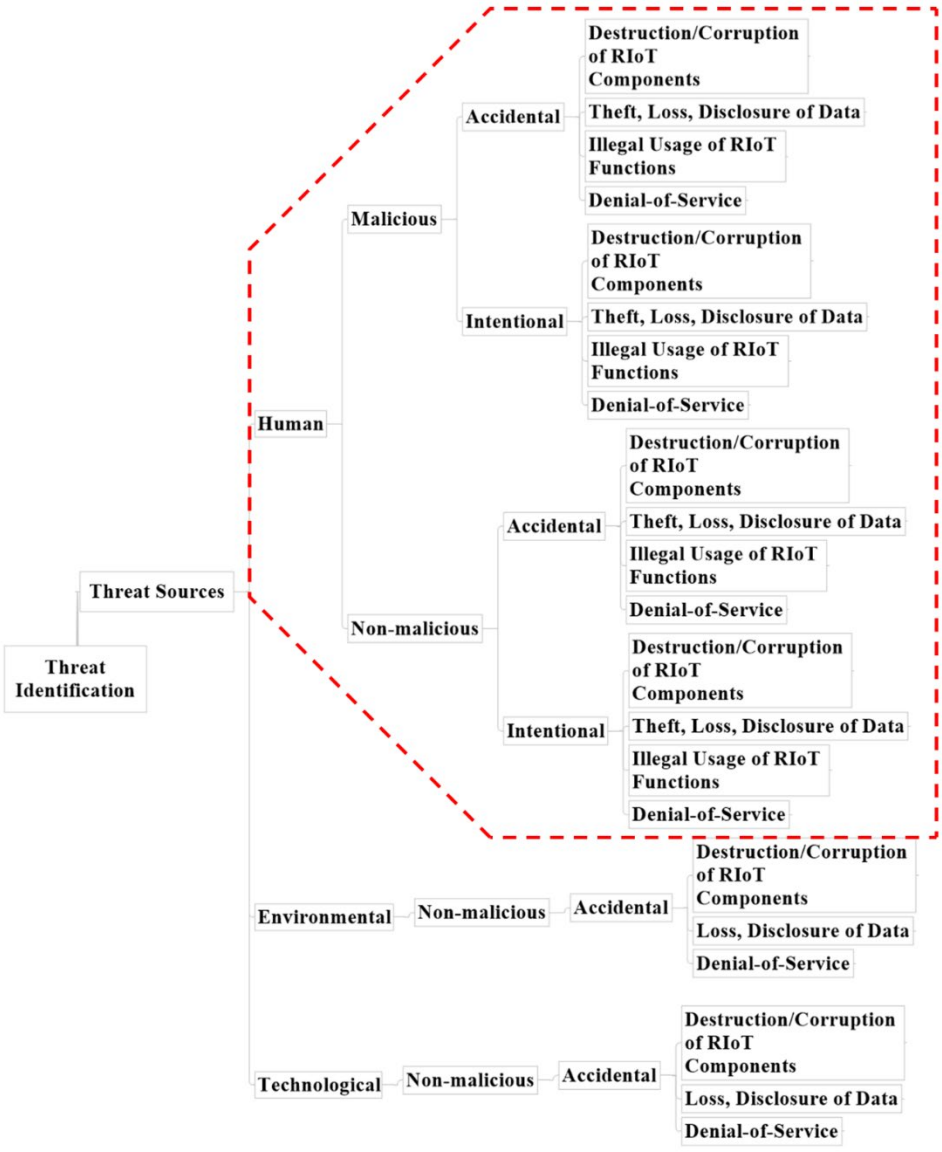


Figure 3.1-4 RIoT Threat Source Categories

(Adapted from Aissa (2014))

According to Barrett (2018), the National Institute of Standards and Technology (NIST) mentions systems, people, assets, data, and capabilities as potential targets of a critical infrastructure system. In RIoT applications, such targets are further categorized in Figure 3.1-5 below:

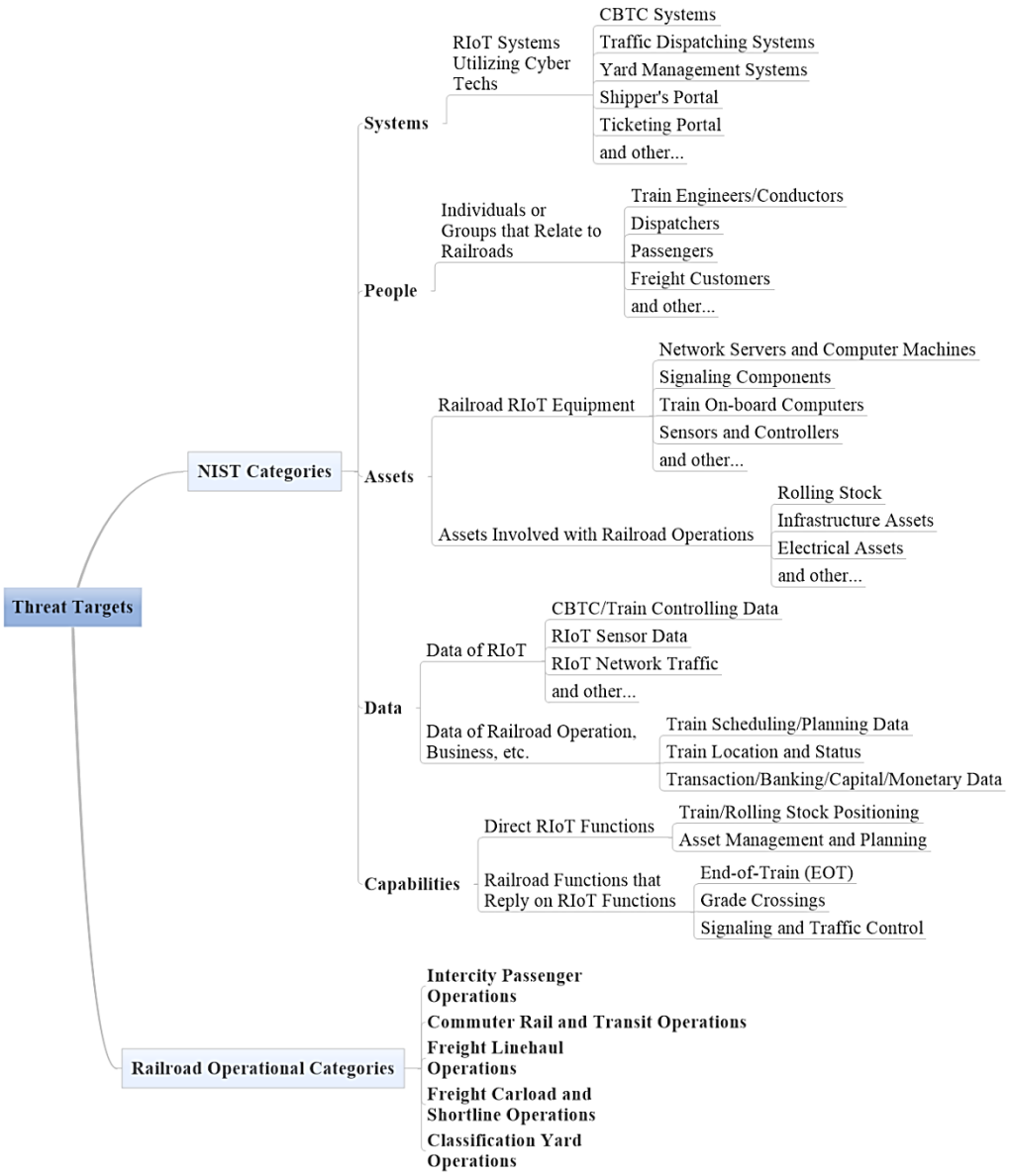


Figure 3.1-5 RIoT Threat Target Categories

Threat Accessibility

Of the three elements, accessibility is the one most directly under the control of the railroads. It is comprised of two critical elements: the attack surface, and the logical or physical reachability.

The attack surface can be regarded as the aggregate of all vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be either physical or digital. Digital attack surfaces are the totality of all vulnerabilities in the implemented hardware and software, while the physical attack surface includes access to all physical endpoint devices. Once an attacker has physically accessed a computing device, the intruder will look for digital attack surfaces left vulnerable by poor coding, default security setting, or poorly maintained software that has not

been updated or patched. The term attack surface is often confused with the term attack vector: the surface is what is being attacked; the vector is the means by which an intruder gains access. Both physical and digital attack surfaces should be limited in size to protect surfaces from access. Railroads can identify, analyze, and reduce both its physical and digital attack surfaces.

Identifying Threat Capability

This refers to the tools, techniques, and resources of the attacker, which are totally outside the control of the railroad. However, one cannot assume that an understanding of them is not critical to the system's owner and operator, such as railroad staff. Because the railroads are commercial businesses, and must implement security measures in a resource-constrained environment, an understanding of a threat capability is critical in making the appropriate, and necessary cost/risk tradeoffs when engaging in security investments. A knowledge of known tools and techniques and exploits is also essential to aid the system designer to determine potentially exploitable susceptibilities.

3.1.2 Technical Decomposition of Architecture and Specifications

There exists some overlap between the activities of threat identification and technical decomposition for a specific RIoT system. The technical decomposition is also an iterative process that begins with the analysis of a comprehensive Concept of Operations (ConOps) and associated requirement documents to understand the intended functions of RIoT systems and their design limitations. It is followed by a system decomposition of the use cases and component architecture to refine and document the attack surface and potential attack vectors.

RIoT Concept of Operations

IEEE Standard 1362-1998 (IEEE, 1998) is a standardized industry approach for defining the contents and format of a Concept of Operations (ConOps) to describe the system characteristics, functions, and performance requirements. Figure 3.1-6 below shows a typical ConOps "V-model" chart for an arbitrary system.[1] The created ConOps documents the selected RIoT use cases for the systems architects, engineers, as well as all stakeholders. The ConOps may already exist as one of a number of existing design and requirement documents. In situations where the ConOps and requirements documents do not exist, are incomplete, or do not reflect the current as-built system, the security engineering team may have to reconstruct/reverse-engineer the practical ConOps (especially in the case of an existing "as-built" system). Once the RIoT ConOps documenting the use cases has been created (or validated), it is extended to identify the potential misuses based on the identified threats of the preceding phase. As the interest of the security team is the potential misuses of the system, the use cases analyzed from the ConOps can be winnowed down to only address those use cases with misuses, narrowing the scope of interest.

[1] While the traditional systems engineering V model lifecycle is illustrated for simplicity, the premise applies to any of the other lifecycle models (for example, Waterfall, iterative model, Spiral, Agile). No matter what type of the models is chosen, each of them has basic stages which are used by every software development company. These can be summarized as: Planning and Requirement Analysis, Designing Project Architecture, Development and Programming, Testing, and Deployment.

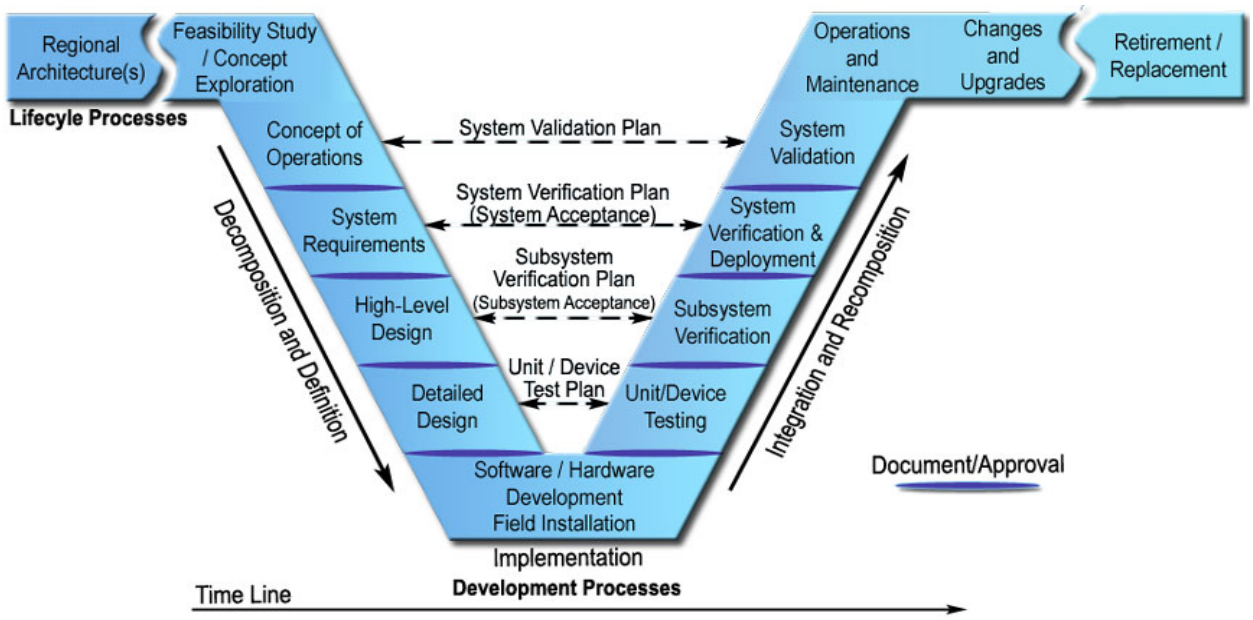


Figure 3.1-6 Systems Engineering "V" Diagram

(Adapted from FHWA (1992))

The usual systems engineering tools and methodologies for use case analysis (such as Unified Modeling Language (UML), sequence diagram modeling, flow chart modeling or finite state machine (FSM)) can be applied to misuse analysis to extract the system functions and working sequences, simplifying the process of identifying the attack surfaces, vectors, and vulnerabilities.

Technical Decomposition and Vulnerability Analysis

With the appropriate RIoT ConOps use and misuse cases modeled, the critical corresponding attack surfaces, vectors, and vulnerabilities can then be iteratively decomposed. The hardware and software cyber components that support these features would consist of network, computation, communication, encryption, authentication, and other computing and software-based resources.[1] The specific hardware and software elements of a RIoT will vary based on the specific system under review. Matching RIoT use case functions to the supporting IT resources is critical to the decomposition and identification of specific attack surfaces, vectors, and vulnerabilities in digital and physical components. These possible attack surfaces, vectors, and vulnerabilities should be identified based on the state-of-the-art knowledge in the literature[2], or from the empirical experience of investigators. The involvement of experienced cyber "Red

[1] Consideration should also be given to not only the potential attack surfaces, vectors and vulnerabilities associated with the physical hardware or software components, but also programmatic issues associated with the personnel, supply chain, and supporting equipment and systems.

[2] For example, the MITRE ATT&CK (Adversarial Tactics Techniques and Common Knowledge) framework – see https://attack.mitre.org/ (accessed 27 December 2019). It is important to note that the literature does not address potential zero-day vulnerabilities, which are previously unidentified vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software).

Teams"[1] in the analysis process to augment the railroad domain expertise of the investigators should be considered. Three common tools to aid in this decomposition and analysis are described below, and examples of their use will be shown in subsequent sections for the selected example RIoT use cases.

Sequence Diagram Modeling

Exploitation of a cyber vulnerability usually involves exploitation of time dependencies of activities and system status. A sequence diagram is one of the UMLs showing the object interactions arranged in time sequence. A sequence diagram shows different processes or objects that live simultaneously as parallel vertical lines (lifelines), and the messages exchanged between them as horizontal arrows, in the order of their occurrence. The message flows depict information flows, dependencies, and interrelationships of sub-events (shown as blocks) as well as their independent owners. The sequence diagram is also capable for illustrating asynchronous events that occur in parallel. This modeling allows for the specification of simple scenarios in a graphical manner.

Sequence diagram is one of the common practices used by researchers to conduct modeling of cyber threats (Marrone *et al.*, 2015; McDonald, 2012; Schmittner *et al.*, 2015). These events consist of the major procedures involved in a cyber attack or threat upon RIoT applications. Since RIoT threats involve not only IT applications, but also physical railroad components, sequence diagram is also capable to capture the behaviors of physical railroad components during a cyber attack.

Attack Tree Modeling

Attack trees are multi-leveled diagrams consisting of the root, leaves, and children nodes. From the bottom up, children nodes are conditions which must be satisfied to make the direct parent node true (conditions for an attack, or other conditions); when the root is satisfied, the attack is completed. Each node may be satisfied only by its direct child nodes. Attack trees are related to and established from fault trees, and are widely used in previous cyber security analyses, as shown in Fovino *et al.* (2009); Ji *et al.* (2016); Kordy *et al.* (2012); Roy *et al.* (2010); Xie *et al.* (2013).

Finite State Machine Modeling

FSM modeling is another well-accepted tool to simulate the cyber-physical system (CPS) architecture and other IT frameworks or communication protocols (Langensiepen, 2015). FSM can model the control part of a CPS system and consists of a finite number of states, a finite number of events, and a finite number of transitions. Such a feature is suitable for reverse-engineering the RIoT applications with pre-designed states for the prediction of any misuses. The modeling processes of FSM on RIoT use case depends on the specific system and application design. Like sequence diagram modeling, FSM would also incorporate traditional components of

[1] A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve cyber security by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team. Source: CNSSI 4009-2015 "Committee on National Security Systems (CNSS) Glossary revised April 6, 2015" (CNSS, 2015).

railroads that consist of CPS RIoT applications, showing the various interactions of the cyber parts within the general system.

3.1.3 Consequence Analysis

Just as there was some overlap between the threat identification and decomposition, there is an overlap between the technical decomposition and consequence analysis. Practitioners should then prioritize the decomposition and vulnerability analysis based on the significance of the potential impact of a successful cyber exploitation to railroad. The latter is a function of consequence analysis. Consequence analysis focuses on identification of the criteria of successful attacks, and their corresponding severity evaluation. For RIoT-focused cyber risks, the authors recommend evaluating the consequence by categorizing the risks into safety risks and non-safety risks. Both quantitative and qualitative approaches for the consequence evaluation are considered for specific practices.

Safety Risks

Safety risk in this methodology refers to the RIoT cyber risks that may lead to railroad safety violations, specifically the safety of train, passenger, crew, and other involved parties. Such risk may result in unsafe rail vehicle movements, or threatening the wellness of passengers or any other individuals as well as the safety of physical assets and equipment. Such risks are of the highest priority during the RIoT cyber security analysis and consequence evaluation since the worst-case scenarios are mostly significant and devastating. Identifying the safety-critical cyber security components is deemed essential to the entire risk evaluation and analytical process.

Non-Safety Risks

Non-safety risk in this methodology refers to the RIoT cyber risks whose final results are not related to unsafe train movements. Such risks may relate to train delay, service disruption, or increased costs. Such risks may not directly lead to destructive damages; however, they may still be harmful to railroad operation.

Quantitative Approach

In the quantitative approach, the consequence is evaluated through a collection of risk indicators to assess the potential damage. These indicators (e.g., train delays and monetarized costs) could be modeled into numerical values.

Qualitative Approach

In the qualitative approach, the consequence is evaluated through empirical evaluation from experts and investigators, who can produce the ranking score based on their experience. Matrix scoring on selected categories or components is often used in this approach.

3.1.4 Mitigation Strategies and Conclusions

The final step of the process is the identification of cyber risk mitigation strategies. RIoT cyber risk mitigation strategies are the activities to prevent expansion of a cyber attack, to mitigate its effects, and/or to resolve or recover from the consequences. The proposed methodology first

focuses on defensive mitigations associated with prevention and detection of the cyber attack. The methodology then shifts to resilience measures associated with mitigation and recovery.

Prevention and Detection

Prevention consists of all actions to be taken in the system planning and design period to prepare for any anticipated cyber risks (either with or without systematic cyber risk management). Information would be needed in preparation for further steps, such as anticipated counter-measure technologies, resources, involved parties, etc.

Detection assumes factual implementation of the RIoT use case and that the implementation has already been put into testing and actual production, so that the anticipated cyber attacks are able to occur. In this phase, systematic procedures to detect an attack are critical for risk management. Designing the detection procedures should consider the following principles:

- Make distinctions between technical failures (accidental) and cyber breaches (intentional).
- Distinguish minor cyber breach attempts from major cyber attacks with malicious objectives.

Mitigation and Evaluation

Mitigation refers to the measures undertaken to limit the scope of damages that can arise from an attack. It follows prevention and detection. Mitigation incorporates two aspects: one is associated with the with preliminary cyber risk evaluation for a specific RIoT use case, and risk mitigation strategies that are needed before potential cyber events occur. Such mitigation strategies should contain specific action items as countermeasures for all identified threats on a RIoT use case. The second aspect refers to limiting the damage if a successful cyber attack has already occurred. In this presented methodology, the authors categorize both aspects of the mitigation strategies as one of two different types: technical strategies and policy-based strategies.

Technical strategies are the application of specific technical approaches to address the vulnerabilities of RIoT systems. These strategies may include encryption, upgrades from older protocols, higher-level authentications, etc. Policy-based strategies involve policies and procedures that indirectly defend the RIoT use case. Policy-based strategies may indirectly require the application of specific tools and technologies to implement. These strategies depend on the actual management, execution, or practices of involved people to prevent, identify, or resolve RIoT use case from being attacked. These strategies may include staff training, regulation adjustment, communication and collaboration with involved authorities and law forces, etc.

Recovery involves restoration of the system to an operating condition that existed before the cyber attack occurred as well as post-attack analysis to determine technical/policy strategy changes that need revision or modification. This allows practitioners to better understand the costs and benefits of the use-case-specific RIoT risk management strategies. Adopting such mitigation strategy evaluation could help the practitioners easily identify the benefits of the cyber risk management as well as the other tradeoffs and improvements.

3.2 Use Case Identification

Enumeration and analysis of all possible RIoT use cases are beyond the scope of this research. The research team therefore selected three representative RIoT use cases to demonstrate the application of the risk management methodology. This section elaborates on the reasoning and criteria for these three use cases.

Following the industrial survey, the research team collected further responses from 6 railroad operators (Amtrak, Conrail Shared Assets, Belt Railway of Chicago, CSX, Canadian Pacific and Norfolk Southern) to identify their critical cyber risk management challenges. The railroads represented a mix of Class I and II freight and major passenger operators. The research team identified eight common RIoT use cases in consultation with the industrial collaborators:

- PTC systems
- Traction power distribution/SCADA system
- Radio controlled movable bridge
- Remotely controlled locomotive
- Remote interoperability on ACSES
- ATCS CTC radio code line systems
- Dual-tone multi-frequency (DTMF) radio-controlled switch.
- End-of-train (EOT) device.

To remain within the period of performance, resource constraints, and resource availability, the research team down-selected from these shared issues to three cases:

1. ATCS CTC radio code line
2. Remotely controlled movable bridge
3. Further cyber security review of PTC

The selection of these three use cases represented a compromise between the available technical resources to the research team, coverage of the rail operation sectors (freight and passenger), and concurrent urgency in terms of cyber threats and current scale of the application.

4. Selected Use Case – Advanced Train Control System

The Advanced Train Control System (ATCS) is a proprietary network protocol that expands the functionality and efficiency of CTC systems. ATCS is widely employed in North America, especially U.S. railroads. Radio code line is one of the multiple media forms designed to host ATCS network communications, utilizing the narrow-band carrier links allocated exclusively to railroads by Federal Communications Commission (FCC). ATCS was designed by Aeronautical Radio Inc. (ARINC), led by the Association of American Railroads (AAR). Besides ATCS, there are similar protocols functioning the same as ATCS to provide the radio code line support, such as ARES protocol by Wabtec, Genisys protocol by Union Switch and Signal (US&S), and the supervisory control system SCS-128 protocol by Safetran. This report uses the name "ATCS" hereafter to refer all the similar protocols that provide radio code line functions for North American railroads.

In this section, this study first explains the justification to select ATCS as a use case object. Then, it introduces the operational functionalities from a railroad user's point of view (a.k.a. ConOps), using working flow diagrams. With the analysis of its technical structures and specifications, this report summarizes the major working sequence of the ATCS to identify potential breach points. Three general cyber threats were discovered and decomposed: 1) Eavesdropping, 2) DoS attacks, and 3) Spoofing attacks.

Specifically, a case study on spoofing attacks in ATCS "Blue Block" mode (naming may vary among ATCS users) has identified one theoretical vital failure. In specific conditions, such risk may result in safety threats to railroad roadway workers. In such a scenario, researchers concluded that the fail-safe designs of ATCS and its correlated systems may not be able to fully prevent the hazard under very specific conditions.

In the final part, the authors propose several mitigation strategies based on the identified vulnerabilities and risk analysis. Specific short-term practical actions are also recommended to prevent the Blue Block safety risk that involves the field vital components.

4.1 Cyber Risks of ATCS Radio Code Line System

4.1.1 Justification of Use Case Selection

ATCS applications in U.S. railroads are widely adopted in both freight and passenger railroad sections. The ACTS protocol enables railroads to improve the efficiency and reliability of their CTC systems for better traffic management and dispatching. Serving as the CTC backbone in the railroads, ATCS has been in place for almost 30 years.

Designed in the 1980s, ATCS protocols didn't foresee the current cyber ecosystem. Few technical designs are integrated in ATCS for cyber threat countermeasures. To achieve cost-effective wireless communications, ATCS chose narrow-band carrier communications as one of the mediums to connect center dispatching office with remote devices, such as control points, interlockings, and independent mainline switches. Such narrow-band communication hosting ATCS applications replaced the old analog code line system used in the early stage of CTC, and hence ATCS applications are called "radio code line system" in many railroads. ATCS radio code line communications are designed to be broadcasted along its CTC territory via the designated railroad frequencies (e.g., 900 MHz channels assigned by FCC). Unfortunately, such

unencrypted design by nature is prone to be captured and decoded by any third party with proper entry-level knowledge.

Major railroads in North America have kept the legacy ATCS protocol to maintain their individual CTC systems. Although actions have been taken to switch from radio code line to fiber-optics or commercial telecom carriers, mostly due to cost considerations, there is still a considerable number of sections of U.S. rail mainlines that continue to use radio code line systems, for both freight and passenger traffic. Since railroad operators seldom update or change ATCS application data, these mainline sections over time became the targets of eavesdropping by radio and railroad hobbyists.

4.1.2 An Eavesdropping Software and Its Nationwide Popularity

First released in 1999, "ATCS Monitor" software became a widely distributed platform for the public to monitor railroad CTC actions through various radio code line protocols. With the nationwide collaborative decoding efforts of its contributive users, the ATCS Monitor community has now collected a significant amount of decoded data for most of the railroads using ATCS. With region-specific decoded data loaded into ATCS Monitor, plus the appropriate radio input tuned up, ATCS Monitor can launch a dispatcher's view displaying all the real-time traffic actions in the region.

ATCS Monitor is developed by an author named Dave Houy (Houy, 2010). This software is still evolving, with the most recent version released in April 2012. A restricted ATCS Monitor Yahoo Group (Yahoo, 2010) is the major forum for file-sharing among approximately 14,000 (and growing) members nationwide. Figure 4.1-1 shows the basic operational procedure to use ATCS Monitor.

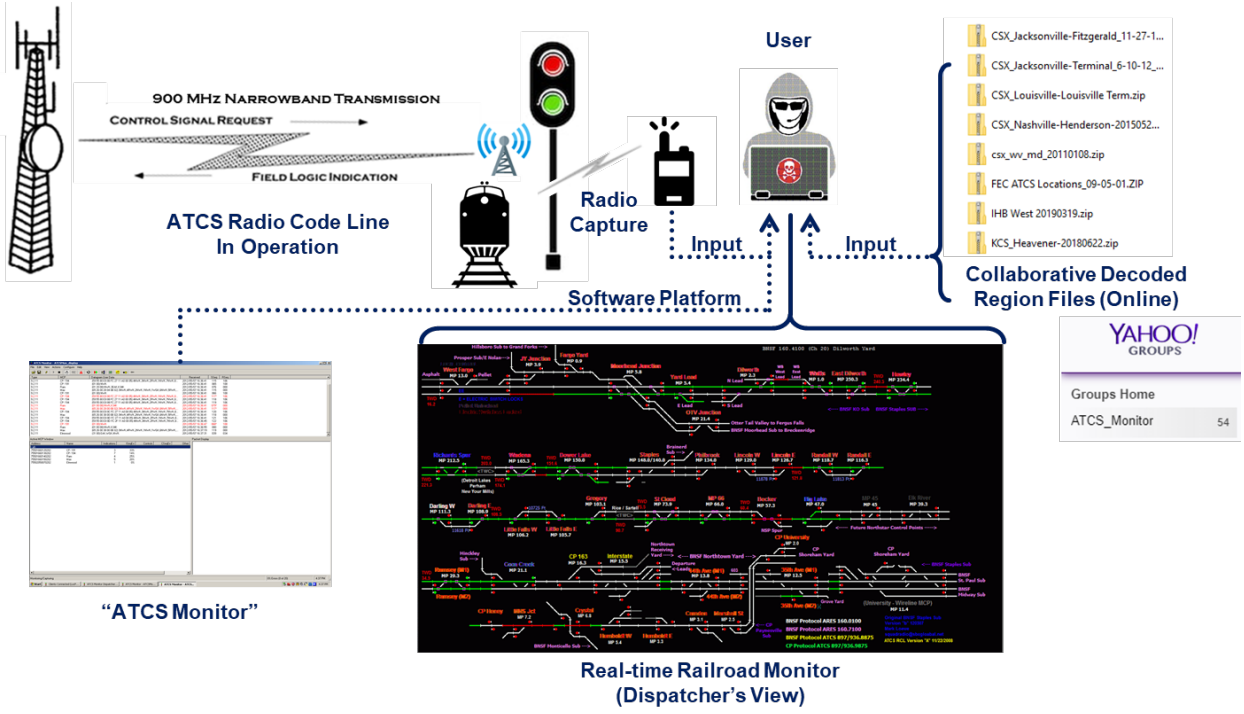


Figure 4.1-1 Operations of ATCS Monitor

ATCS Monitor users have two categories: regular users and contributive decoders:

- Regular users download the software platform and decoded files for free, setting up their own radio input to observe and monitor their railroad of interest.
- Contributive decoders not only monitor the railroads, but also visit the fields regularly to check the correspondence of signaling actions with the captured radio packets. This is the fundamental decoding action to provide more ATCS Monitor coverage and maintain the effectiveness of the already-decoded files.

The collaborative decoding in the user community has touched upon almost every ATCS railroad territory. Table 4-1 (Paine, 2018) shows the railroad sections that have been decoded, or in the process of being decoded by the online community, sorted by state. All the efforts of observing, intercepting, decoding, and documenting the ATCS packets are from volunteer decoders. Regional files and data are uploaded by various decoders over the country in a consistent format as input for ATCS Monitor and then distributed to other regular users for up-to-date, real-time monitoring.

Step-by-step tutorials and instructions for setting up ATCS Monitor and required radio hardware are available within the Yahoo Group. ATCS Monitor itself doesn't provide network-level monitoring capability, and most users can only monitor the region limited to their radio capturing range. However, the authors also noticed that online collaborative efforts have also developed network-level monitoring by integrating radio inputs from multiple locations, with applications on mobile device available.

So far, the research team has discovered that the user groups of ATCS Monitor include but are not limited to: radio hobbyists, train enthusiasts, and railroad trespassers hopping freight trains. Moreover, eavesdropping ATCS Monitor railroad actions and train movements has already become a useful tool for the trespasser (train hopper) to acquire information to select the desired freight train to hop. Specifically, these trespassers select their intended destinations and get remote assistance from ATCS eavesdroppers to facilitate their train-hopping purposes.

Table 4-1 U.S. Mainline Sections Being Eavesdropped through ATCS by State

State	Route Miles	Control Points	Involved Railroads	Subdivisions
Alabama	1,046.7	249	AGRR, BNSF, CSX, NS	18
Arizona	759.5	140	BNSF, UP	9
Arkansas	1,211.8	262	BNSF, KCS, MNA, UP	18
California	2,816.1	623	ACTA, BNSF, Caltrain, Metrolink, PHL, UP	41
Colorado	1,633.5	234	BNSF, UP	18
Delaware	2.2	2	CSX	1
Florida	1,163.9	277	CSX, FEC	20
Georgia	2,281.8	341	CSX, NS	27
Idaho	265.4	76	BNSF, UP, MRL	5
Illinois	3,525.7	703	BNSF, CN, CP, CSX, DM&E, IAIS, IHB, KCS, Metra, NS, P&I, TP&W, TRRA, UP	83
Indiana	1,211.5	265	Amtrak, CN, CSX, IHB, INRD, NS	32
Iowa	862.6	133	BNSF, CN, DM&E, UP	25

State	Route Miles	Control Points	Involved Railroads	Subdivisions
Kansas	932.1	196	BNSF, K&O, KCS, UP	17
Kentucky	973.0	259	CN, CSX, NS, P&I	20
Louisiana	807.6	157	BNSF, CSX, KCS, NOPB, NS, UP	19
Maryland	277.2	58	CSX, NS	11
Michigan	645.9	143	AA, Amtrak, CN, CSX, NS	16
Minnesota	1,352.0	227	BNSF, CN, CP, DM&E, OTVR, UP	35
Mississippi	337.2	71	BNSF, CSX, KCS, MSRR, NS	7
Missouri	2,692.1	455	BNSF, KCS, MNA, NS, TRRA, UP	36
Montana	1,099.0	217	BNSF, MRL	16
Nebraska	2,049.8	415	BNSF, UP	26
Nevada	386.9	64	UP	4
New Mexico	803.0	164	BNSF, NMRX, UP	15
New York	262.4	46	CP, NS	6
North Carolina	603.9	141	CSX, NS	14
North Dakota	355.2	66	BNSF	6
Ohio	1,233.0	293	AA, CN, CSX, I&O, NS	32
Oklahoma	813.0	172	BNSF, KCS	10
Oregon	634.5	193	BNSF, UP	11
Pennsylvania	433.6	93	CN, CP, CSX, NS	20
South Carolina	413.5	98	CSX	7
South Dakota	35.9	12	BNSF	2
Tennessee	1,133.2	240	BNSF, CN, CSX, NERR, NS, UP	29
Texas	3,410.8	706	BNSF, KCS, TRE, TXPF, UP	53
Utah	715.7	194	UP	9
Virginia	1,559.6	385	CSX, NS	35
Washington	1,253.2	219	BNSF, PSAP, UP	17
West Virginia	902.5	138	CSX, NS	17
Wisconsin	431.1	75	BNSF, CN, CP, UP	13
Wyoming	534.3	126	BNSF, UP	10
Total	circa. 35,000	circa. 5,000	34	circa. 500

4.2 ACTS Radio Code Line Specification Decomposition and ConOps

4.2.1 Evolution of ATCS Radio Code Line System

Historically, North America railroads employed wired code lines to achieve CTC functions. The code line wires were installed on the pole infrastructure along the right-of-way. These pole lines often hosted networks, such as circuits used for railroad telephone/telegraph communications, wires used to control aspects displayed by the wayside signal system, and circuits providing commercial power to related installations. Within the code line wires, CTC wires transmitted analog coded messages containing dispatchers' controls between the field and the dispatching center. Transmitted messages enabled the remote clearing of wayside signals, operation of powered switches, and the awareness of dispatching center regarding the field device status and block occupation. Figure 4.2-1 shows the early wired CTC code line system with analog signal controls, accompanied by its code line infrastructure to the right.

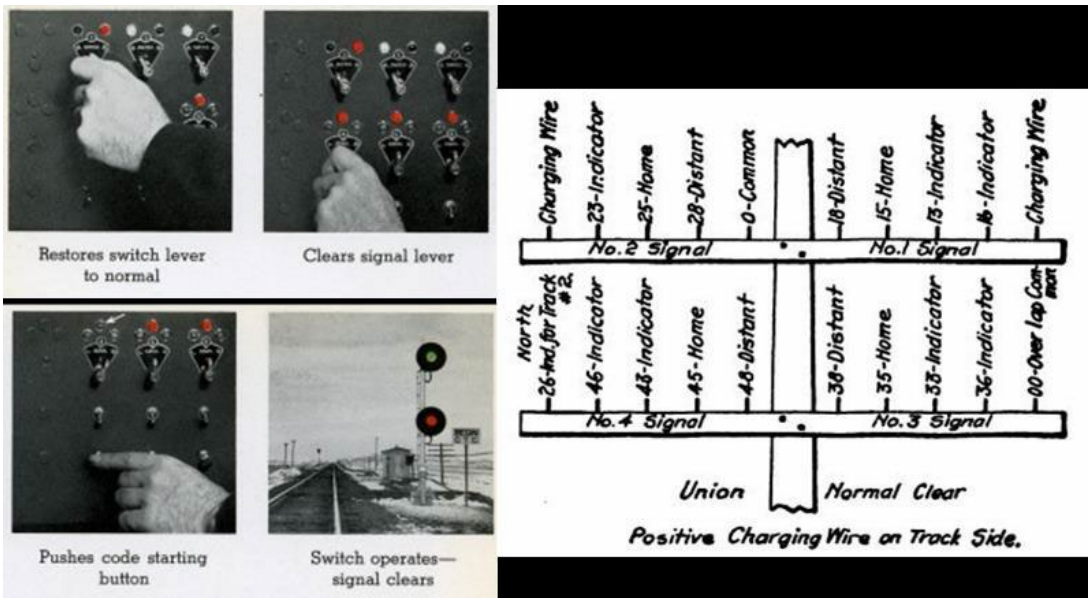


Figure 4.2-1 Analog CTC Code Line and Wire Diagram

(Adapted from Burgett (2016))

This cumbersome infrastructure, using open wire pole lines, has been neither reliable nor cost-effective. It has been vulnerable to damage caused by harsh seasonal weather, vandalism, and theft due to its copper materials. In addition, pole lines are labor-intensive to maintain because of the remote operating environment, such as in mountainous or other inaccessible areas, or in areas where they coexist with vegetation that adversely interfere with pole line physical components. Mostly, pole line failures result in safety protections, such as dropping signals to "stop" aspect. However, there are scenarios where pole lines can fail in a dangerous manner. For example, extreme weather – like thunderstorms – would create electrical surges on the wires and consequently damage the devices or trigger false signal aspects or block occupation messages.[1]

For the above reasons, railroad CTC and wayside signal systems have evolved from pole line systems to modern ones that utilize AC or DC coded track circuits for block occupation. Railroads collaborated with commercial carriers on installing buried cables to replace telegraph lines, retired unreliable CTC code lines, and adopted various wireless solutions. To standardize the various practices, in the 1980s, ATCS was designed and adopted into AAR Manual of Standards and Recommended Practices (MSRP) (AAR, 2005).

The ATCS Protocol was designed as an open protocol for equipment compatibilities among vendors. Except for some minor revisions, ATCS specifications have not had an extensive update since the initial release (Wang *et al.*, 2019). As implied by the name, the ATCS Protocol intended to serve train control functionalities in conjunction with a variety of radio-based applications, including radio CTC code line functions. Similar to a PTC system, the ATCS Protocol was also designed to support proactive train protections whose applications reside in the ATCS train-to-ground radio link (AAR, 2005). However, the actual ATCS practices are mostly

[1] See, for example https://www.vre.org/service/rider/terminology/ (accessed 22 December 2019), and "Evaluation of Signal/Control System Equipment and Technology" Task7: Summary and Final Report, FRA/ORD-78/39-7 dated 7 September 1981.

used to support CTC code line communications only, which are the communication network between the wayside equipment and CTC office. The ATCS-based link connecting wayside infrastructure to moving trains has not been adopted in the industry for two major reasons: the complexity of implementation, and the cost of establishing the required interoperability among the various railroads.

Although the majority of ATCS applications have been restricted to radio code line services, its prevalence in the industry is still significant because of the extensive CTC network of major railroads.

4.2.2 User Group and Setups of ATCS Applications

There are five major applications included in the ATCS network architecture: host applications, network applications, wayside equipment (RF or wireline-connected), mobile applications and locomotive applications.[1] Together with the application categories, the major physical devices within ATCS network are illustrated below:

Host Applications

Host applications are the CTC dispatching software plus other related information management systems that fully or partially use the ATCS network. They are located at the top level of the ATCS network stack, providing the human-machine interface between CTC dispatcher and the radio code line functions. In general, host applications reside in the stationary ground computers in the centralized railroad dispatching centers.

Network Applications

Network applications provide configurations and controls that support the networking functions to exchange ATCS messages among different components. In the ATCS network, front-end processors/cluster controllers (FEP/CC) and base communication packages (BCP) are the physical devices and packages to perform the fundamental networking functions, such as message routing, congestion control, radio link access, and application interfacing.

The major difference between FEP and CC is that FEP routes messages between a group of CCs and upper host applications, while CC routes the messages between lower applications and higher-level nodes, such as FEP or other CCs. Geographically, CCs govern smaller areas than FEPs.

BCPs interface between the ATCS ground network and the radio network base stations. BCP base stations, along with the backhaul network, serve as an interface for ATCS code line messages to pass between the back office and the MCPs located at the field control points. This communication link over the radio is the major object of this study.

Wayside Equipment (RF or Wired Connection)

In practice, ATCS wayside equipment resides at the bottom of the ATCS network stack. Serving as the interface between the ATCS network and the vital logic controller at a data radio location, a mobile communication package (MCP) formats and forwards non-vital ACTS code line

[1] Mobile and Locomotive Applications haven't been developed in practical ATCS applications.

messages to the vital logic controller. The vital logic controller contains the logic that carries out train-dispatcher-originated requests for status changes relative to power switches and wayside signals. The logic also produces information at the dispatcher's display regarding the status changes of the aforementioned field devices, as well as those devices pertaining to track circuits in and adjacent to the control point. In this matter, the MCP's function is to pass non-vital control and indication information in ATCS format between the CTC back office and the vital logic controller.

Wayside equipment includes CTC control points (CP), host field-vital logics, switches, home signals, or other automated detection systems. It mostly works independently, as field-vital logic controlling the interlocking with preset logics. Meanwhile, all CTC requests or indication feedback from wayside equipment go through MCP in the ATCS framework.

The link between MCPs and wayside equipment evolved over time and varies among vendors. For example, spread spectrum link has been adopted by Safetran products between field-vital logic and MCPs for better security, isolation, and performance (Siemens, 2014). ATCS does not specify the communication protocol between MCPs and the specific object with which they connect.

Mobile Applications and Locomotive Applications

These types of applications have never been widely adopted in the industry since the initial ATCS design. Mobile applications and locomotive applications are intended for operation control of trains and track forces via MCPs and BCPs to connect into an ATCS network. Initially, there were vital operational features designed into these applications, such as updating movement authority and speed restriction enforcement. However, for various practical reasons, railroads have employed ATCS used for code line as a non-vital system, relegating responsibility for vital train control to the wayside signal system, supplemented with or replaced by voice transactions between train dispatchers and train crews depending upon the method of operation in use on the territory. As a result, MCPs only serve the non-vital communication links with wayside equipment. Some vendors also renamed MCP to wayside communication package (WCP) for better clarity against the confusion of mobile and locomotive application.

4.2.3 ATCS Network Structure

Figure 4.2-2 below shows the structure of an ATCS network example. Although most applications are radio code line services, this diagram still incorporates a theoretical management information system (MIS) and mobile and locomotive applications to cover the full version of ATCS network in the initial design.

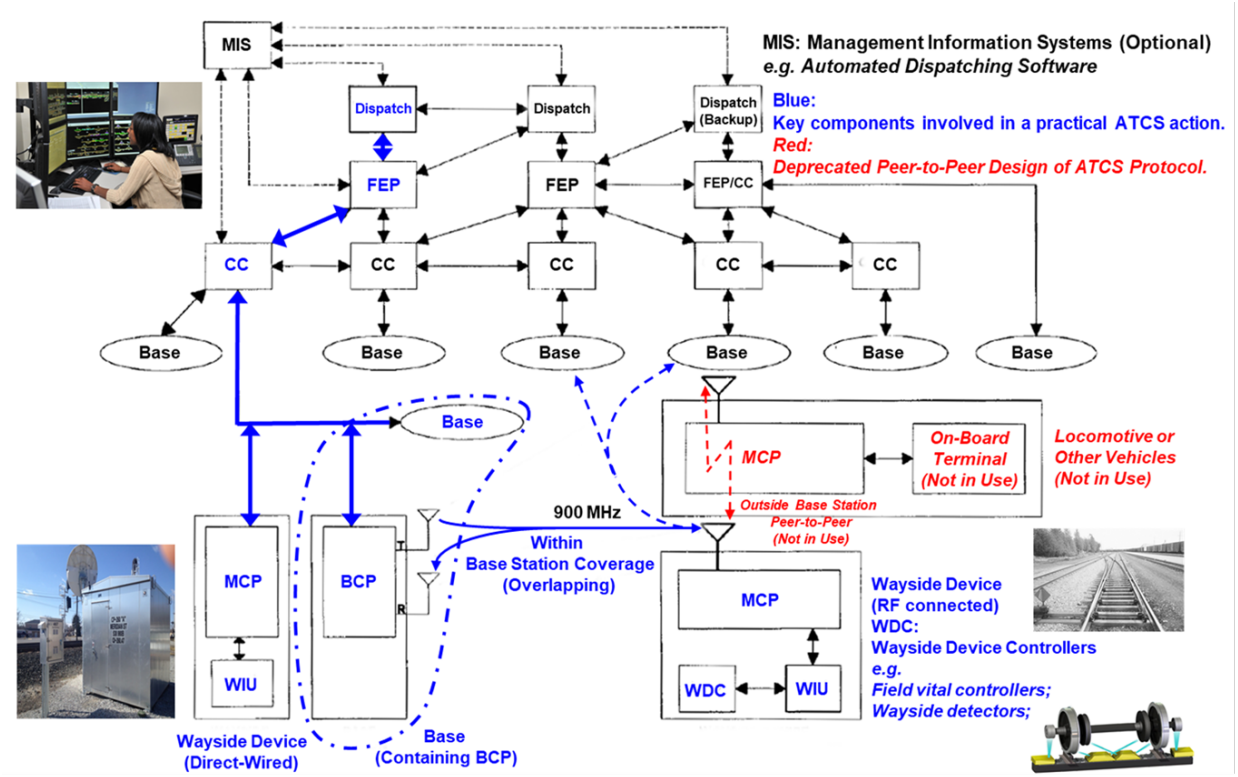


Figure 4.2-2 ATCS Network Architecture and System Users

(Adapted from AAR (2005))

The defunct mobile and locomotive applications are denoted as "Locomotive or Other Vehicles." The blue arrows illustrate the interactions, paths and user relationships in the radio code line service that built upon ATCS network. In most industrial practices, such networks are absolutely closed and isolated from the public internet. The network runs on a private, high-level, data link control (HDLC)-based poll/response protocol (AAR, 2005). A few cost-effective practices also exist that utilize common-carrier-leased circuits to reach significantly distant MCPs, such as ATCS over TCP/IP. Those payload messages are encapsulated into the public network, and it is equally difficult to breach the railroad ATCS public network as the other prevalent services over TCP/IP. Also, as is customary, railroads often use public cellular carriers for backup code line messages, for bad situations where local radio coverage prevents connection of both a normal and backup BCP radio base station for an MCP.

Meanwhile, no matter how the ATCS wireline network is configured, the BCP-MCP radio link connections are universal over most of the ATCS network in various railroads. Such a radio link is easily accessible to the public and identified as the most vulnerable part in the ATCS radio code line applications. The key specifications for the ATCS radio link are summarized below in the OSI-stratified manner:

Physical Layer (Radio)

Radio code line networks specify a simple baseband FSK radio link over six pairs of FCC-assigned frequencies at 900 MHz range (AAR, 2005). The ATCS radio link can achieve full duplex transmission. Six pairs of channels provide the flexibility and redundancy for multiple

railroads to operate at a geographically proximate area, such as the Chicago hub. The common baud rate for the radio code line setup is 4800, with compatible room for upgrading into 9600.

Datalink Layer (Radio)

The datalink layer of ATCS-based radio code line controls the frame synchronization and channel access procedures to support a reliable BCP-MCP radio connection. In the datalink frames, two cyclic redundancy check (CRC) processes have been designed for both the datalink header and the payload of the frame it is carrying. Outside the raw frames, an open ATCS forward error correction (FEC) encoding protocol is deployed to enhance the reliability. In addition, when BCP sends packets, busy-bits are inserted into the FEC-encoded frames to control the channel access. Such access control mechanism helps to avoid the radio collisions by forcing MCPs to wait for non-busy states of BCP to transmit upstream traffic. Encoding designs are available in the original MSRP (AAR, 2005).

Network and Transport Layer

ATCS networks are designed for both virtual circuit mode and datagram mode. In radio code line practices, datagram mode has been universally adopted. The network layer design for ATCS takes responsibilities for the routing of packets among users and provides extra processing actions for packets across the network, such as prioritization, duplication elimination, RF link preprocessing, RF channel access retry, etc. The transport layer of ATCS provides the detailed packet formats that deliver user data and servicing signals among various users. Figure 4.2-3 below shows an example of an ATCS user data packet that enables the various ATCS functionalities. The first octet serves as the preamble; octets 2–4 control the channel logics and sequence; octet 5 provides the address lengths, followed by binary coded decimal (BCD)-encoded user addresses. The detailed functions for each block of the packets are illustrated in the MSRP document that serving as the design manual for vendors to provide the interface with ATCS network, but the lack of encryption and dynamic design for the packets is inherently vulnerable to unauthorized access.

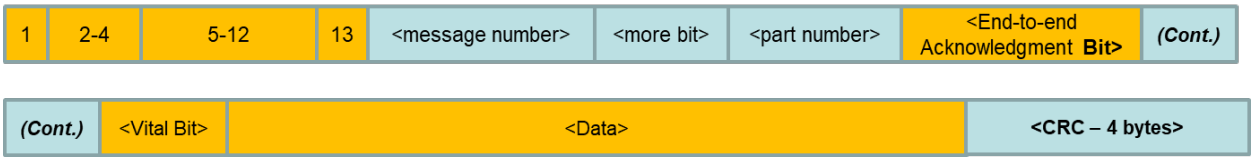


Figure 4.2-3 ATCS Datagram Mode Packet Format (Not to Scale)

Application Layer

Retrospectively, ATCS network was specified as a 7-layer OSI model, including the session layer, the presentation layer and the application layer. In the modern OSI model with 5 layers, the functionalities of those 3 layers are integrated into the application layer, which in the ATCS case is the host applications for the dispatcher. Except for CTC radio code lines, several other applications are also supported by ATCS network protocol. Occasionally outside the CTC network, the ATCS protocol is also scalable to support communications between an isolated vital logic and a corresponding non-vital interface. For example, through ATCS protocol, wayside controllers could implement local-controlled interlocking logics, movable bridges, or DTMF switches within dark territory (Hitachi, 2017).

Theoretically, ATCS can support any type of network applications because the application layer design is transparent to the lower layers. Considering the radio link as a breach point of ATCS network, the application layer serves as a black box whose functions only correspond to the in-situ observations. Therefore, real-time observation of the field responses (switch positions, signal aspects, etc.) can help with the reverse-engineering of the upper-layer applications. This makes it feasible for the ATCS Monitor decoder users to translate captured ATCS radio packets into mnemonics corresponding to the CTC system.

4.2.4 ConOps: Working Flows of ATCS Radio Code Line in CTC Systems

Before the introduction to the system vulnerabilities, it is necessary to walk through the normal ATCS radio code line operations to understand that the functionality of radio code line is playing for the holistic CTC system. According to this research, most CTC actions over the ATCS radio code line employ two major message paths: ***request path*** and ***feedback path*****.** These could also be also interpreted as the downstream message path and the upstream message path, respectively.

Request Path

The request path of ATCS radio code line provides the logic channel that delivers the dispatcher's command to railroad field components, mostly the field-vital logic in the CTC control point. Request examples include clearing a home signal, throwing a powered switch, and granting access to a hand-thrown switch or derail.[1]

In most North American railroads where ATCS is utilized for CTC radio code line, dispatch center host computers contain automated functions such as auto routing. Auto routing or movement planning will initiate most CTC requests for train movements. Human dispatchers not only oversee the operation of the automated systems but to also support many functions that require human interventions, such as the manual issuance of movement authorities. Signal and switch requests made by the automated system are based upon prioritizations derived from a movement planner or equivalent automated system. Such system houses information of the current status of locations and movement authorities in effect for trains en-route or online roadway workers. The movement planner contains other information needed for intelligent decision-making related to train movements including train schedules, train prioritization, slow orders in effect, weather conditions, and many other related factors.

For example, Norfolk Southern's Unified Train Control System could request CTC actions logically and efficiently on behalf of human dispatchers. Such requests are encoded into ATCS messages to request for signal clearing, and then to grant movement authority. ATCS network delivers such messages from the telecommunication infrastructure to the radio link and back to the MCPs at field control points; upon receiving, the field vital logics in the control points decide whether to execute the requests after evaluation based on the local vital logic status.

[1] The ATCS requests are encoded by ATCS protocol to request signal clearing. It may or may not include a request to change position of power switch(es) located within the control point. In most situations in CTC territories, displaying a permissive signal aspect constitutes authority for the train to proceed into the block ahead with no additional authority needed from the train dispatcher.

Field vital logics reside in a set of programmable logic controllers (PLCs). Vital logic controller accepts direct inputs from field devices. Field vital logics determine the acceptance/rejection of a request from ATCS radio link according to its internal logics on its field input conditions. If the current request cannot be executed, such as a signal which is unable to clear because of a train ahead occupying the track, the requests will be held until it can be executed. Requests can never be executed without the consideration of field status because the requests cannot bypass the field vital logic.[1]

In practice, control points with field vital logics are well-guarded in each railroad. Physical access to any part of the vital logics is restricted to authorized personnel. The logic flow for a ATCS Request Path in Figure 4.2-4 is shown below:

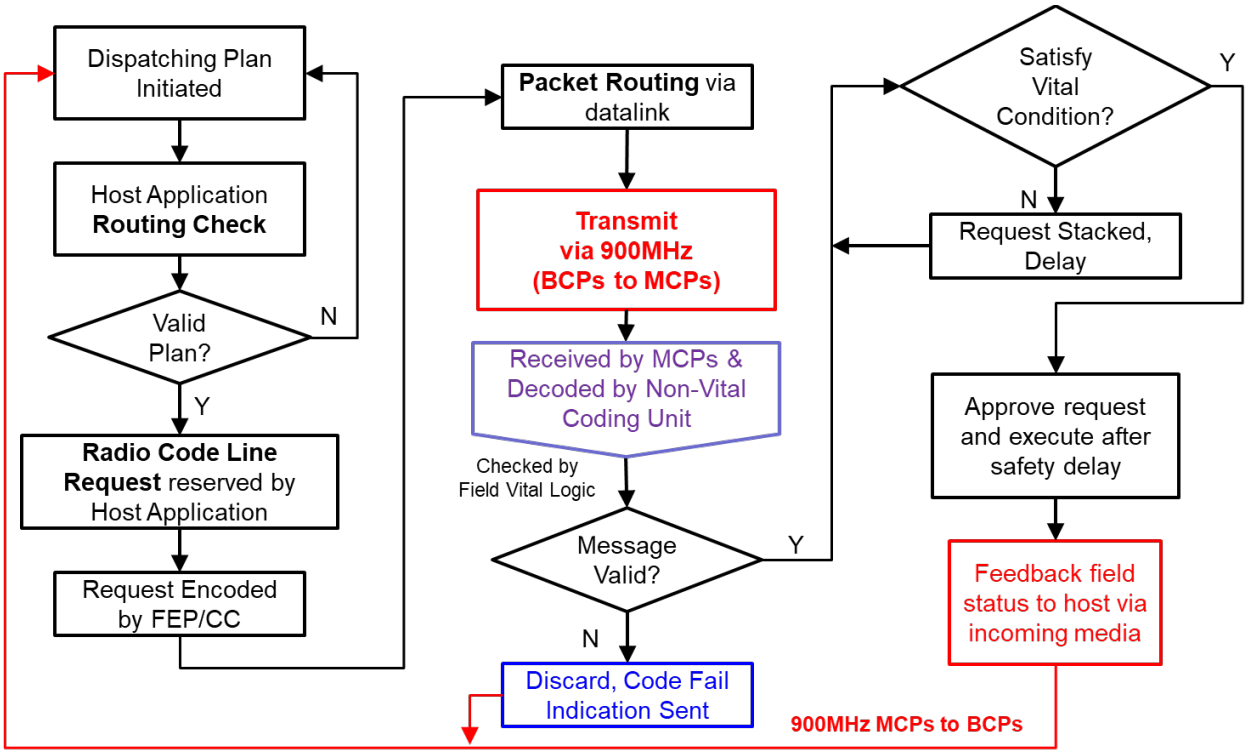


Figure 4.2-4 Logic Flow of Request Path for ATCS Messages

Feedback Path

In response to the change of field status due to execution of CTC requests, train movements or device updates, field vital logic will initiate one or multiple ATCS feedback messages to the

[1] Once an ATCS message from the back office is received by the MCP and in turn the vital logic controller located at the control point, it is the function of the vital logic controller to determine whether it is safe to execute the request based on the field-side status of wayside signals, power switch positions and track occupancies. Once a request results in displaying a permissive signal and the train acts on this request by proceeding into the block ahead, an ATCS message which contains updated indication information pertaining to signal aspects and track occupancies at the control point is generated. This indication is then sent from the control point upstream to the back office via the MCP-to-BCP link, and then the backhaul network. If a request received from the back office such as request for clearing of a signal is unable to be executed at the control point at the time it is received, owing to factors such as occupancy of a track circuit by a train ahead, such requests won't be executed immediately until conditions are safe.

dispatcher host side. Such feedback messages can serve as the acknowledgement to the request execution, or proactively update the field status without preceding actions. Figure 4.2-5 shows an example of one feedback path flow, describing how the host side acknowledges the updated field status. One uniqueness in this logic flow is the reporting mechanism of failures if any intermediate component fails (such as a switch or signal in this example).

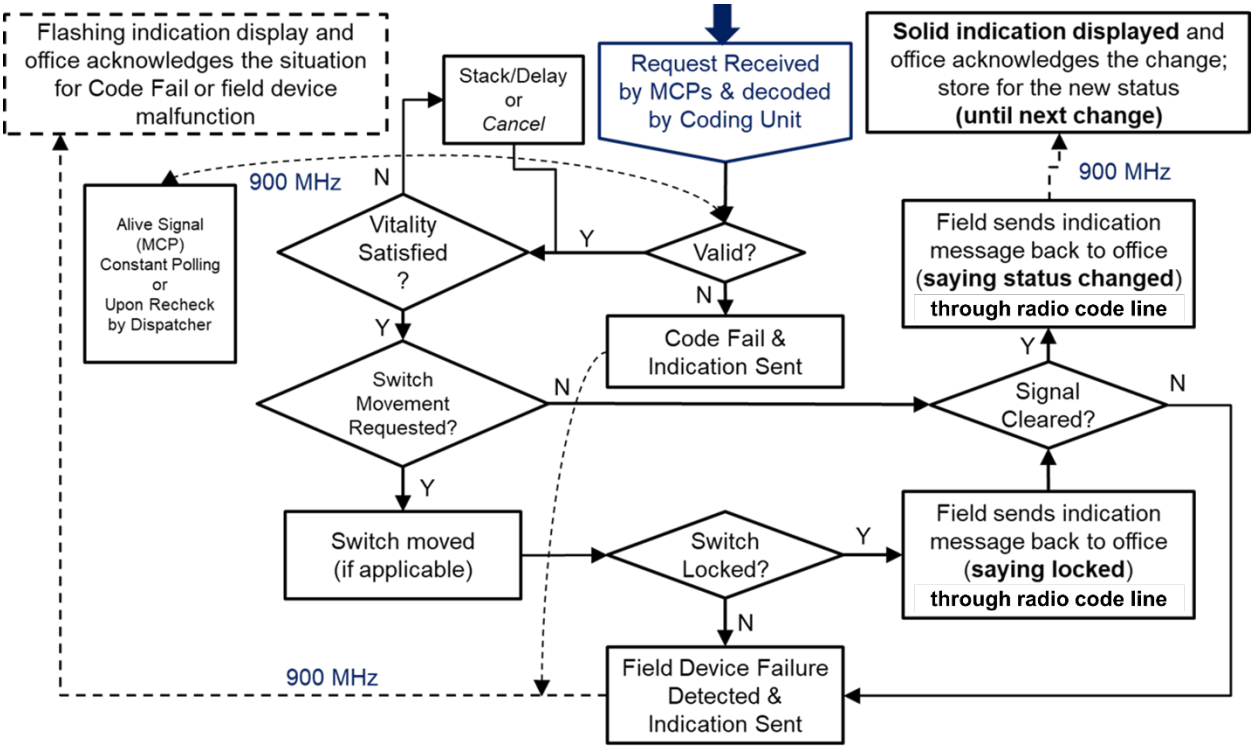


Figure 4.2-5 Logic Flow of Feedback Path for ATCS Messages

Isolation of Vital Logic (Fundamental Fail-Safe Design of ATCS)

As stated, the ATCS radio code line is isolated from the field vital logic in a fail-safe manner. Any ATCS request would be evaluated by field vital logic, preventing inappropriate ATCS messages resulting in unsafe train movements. Likewise, at control points where vital blue blocking (or simply "blocking" in some other railroads) is utilized, request messages are evaluated by field vital logic to prevent inappropriate ATCS messages from creating an unsafe condition for a roadway worker. Under normal circumstances, under the autonomous jurisdictions of field vital logic, ATCS actions would never trigger conflicting movement authorities irrespective of whether the action is initiated by an authorized dispatcher or an unauthorized third party. In addition, field vital logic has its own fail-safe design, which simply voids the movement authorities by stopping all the trains until the failure is resolved. The isolation relationship between non-vital ATCS radio code line and vital logic in normal operation is summarized in Figure 4.2-6.

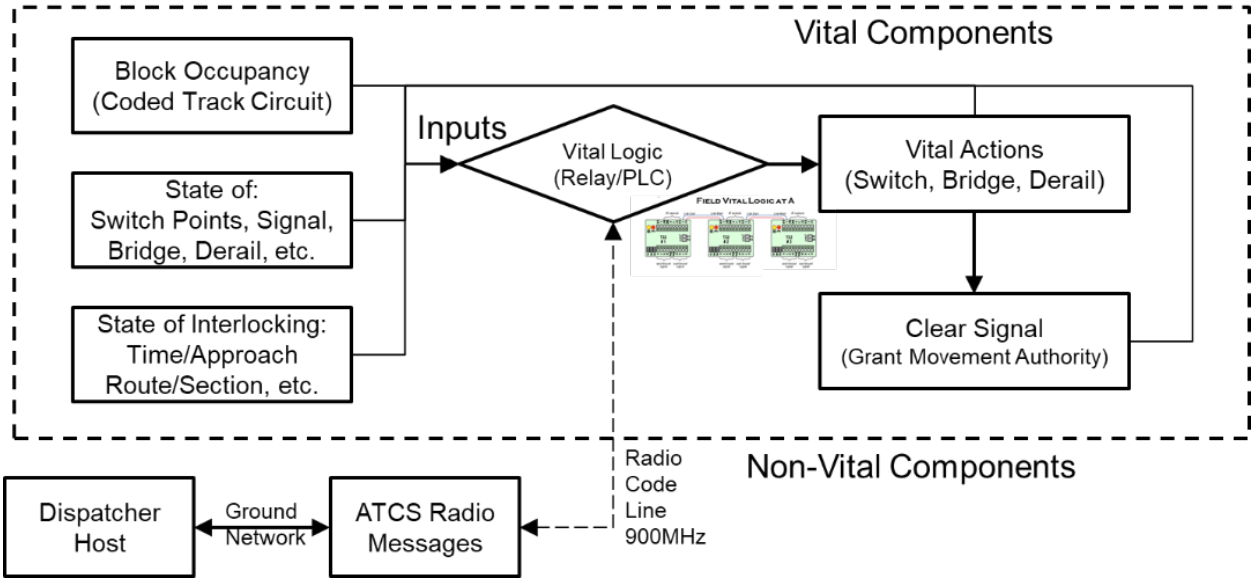


Figure 4.2-6 Isolation between Field Vital Logic and Non-Vital ATCS Radio Code Line

4.3 Identification of Vulnerabilities

In the original specifications of ATCS, the developers categorized six high-level security vulnerabilities:

1. Jamming/channel capture
2. Spoofing
3. Employee sabotage
4. Interception of proprietary data
5. Incidental electro-magnetic interference (EMI)
6. Network overloading

The discussion in this report will focus on the ATCS security vulnerabilities on the radio link due to its easy accessibility, proven by the eavesdropping issues of ATCS Monitor. Items 3 and 5 will not be considered because these approaches either require more physical efforts (such as trespassing) or are easily detectable by administration. In addition, EMI vulnerability in the specification refers to the transponders/balises. In practice, such vulnerability is not available to ATCS, of which the transponders/balises are only designed on paper, and were never carried out in the field.

Considering the differences between concurrent ATCS applications and its initial design specifications, one can re-categorize the vulnerabilities of the ATCS network under the CTC radio code line use case as three major types:

1. Eavesdropping attacks
2. DoS attacks
3. Spoofing attacks

4.3.1 Eavesdropping

As mentioned earlier, ATCS Monitor is one identified ongoing cyber breach in the form of eavesdropping. It is carried out by collecting messages using receivers, such as modified radio devices or software-defined radios (SDR), in conjunction with field observations that map the messages with control point actions (such as corresponding switch positions, signal aspects), generating mnemonics to be distributed online.

Considering the availability of the lower-layer specifications and open datagram transmission over the radio link, it is technically achievable for a third party to reverse-engineer to identify the implications of the datagrams[1] (Craven & Craven, 2005; Wang *et al.*, 2019). Supposedly, due to such inconvenience and concerns about impacting the operations, railroads seldom update the addresses or messages for an existing control point of their CTC radio code line system. Consequently, this helps the ATCS Monitor user community to minimize the effort to decode their interested railroad mainline sections repeatedly. Therefore, decoded ATCS radio code line mnemonics over most of the major North America mainlines remain active over years within the ATCS Monitor community. The mnemonics of each decoded mainline/region/subdivision explicitly show the ATCS datagram implications and details such as bit indication, device/MCP address, and priority sorting.

It is safe to say that a pure eavesdropping attack only affects the confidentiality of ATCS applications without operational impacts. The consequence of eavesdropping cyber breaches cannot lead to direct safety or security impacts to the railroads, and thus the following section of consequence analysis will not include a discussion of this particular aspect. However, the consequences of leaking proprietary information are open-ended and worth further research with more stakeholders involved. In other words, it may serve as the stepping stone for other encroaching attacking attempts (both physical and cyber) with acquired train movement information.

4.3.2 Denial-of-Service Attacks

ATCS's adoption of the use of static narrow-band channels within the 900 MHz band results in vulnerability of these channels to jamming and interference. When an ATCS channel becomes unavailable, unless there is a backup transport medium available such as a cellular phone link, the control point will drop offline. When a control point drops offline for any extended duration this very often has an adverse effect on train operations in the area.[2]

Due to the limited power for commercially available transmitters to the public, only areas close to BCP/MCP antennas are deemed vulnerable for a successful ATCS radio channel-targeted DoS attack. Although there is no research directly showing the interaction between proximity and DoS attack effectiveness, Craven (2008) has established an ATCS radio network simulator to

[1] As a practical matter, the accurate decoding of ATCS control and indication messages mostly requires multiple site visits to verify bit representations within these messages as they pertain to signal aspects, switch positions, and track occupancies that are utilized within the control point.

[2] Practically, DoS attacks targeting ATCS 900 MHz channels could feasibly be achieved by transmitting white noise (or other interfering waves) on the center frequency of a selected ATCS channel.

analyze the radio performance provided with disabled or defective ATCS network nodes (BCP/MCP).

However, the isolation design of vital logic, which achieves the fail-safe mechanism of the ATCS radio code line, could minimize the severity of consequences in terms of railroad safety. In other words, attacking actions like jamming to impair the channel availability would finally result in the invocation of the protection mode of field vital logic that prevents any unclear and unsafe train movements, but introduces unscheduled train stops that delay operations.

The following section the authors develop a simulation platform to deduce and understand the impact on the railroad's level of service when a DoS attack is engaged in its ATCS radio code line.

4.3.3 Spoofing Attacks

The legacy mechanism of the ATCS protocol and the eavesdropping community would substantially weaken the upper layer security design. However secure the upper layer is, the radio link could still leak the private messages in the lower layer; even worse, it would potentially inhale unauthorized messages that spoof authorized ATCS network users. Although the owner of ATCS Monitor claims that the software doesn't provide message encoding and transmission features (Houy), the decoded mnemonics and static ATCS setup of the railroads makes it achievable to transmit packets into the ATCS network from a third party. Lacking authentication, ATCS networks are vulnerable to injected packets in the forms of: 1) replaying, 2) packet injection, and 3) packet modification, solely or jointly.

Although there is no knowledge of any spoofing attacks to date, the following section will analyze the potential impacts of spoofing attacks on ATCS using logical deduction tools: sequence diagrams and attack trees. These approaches helped us successfully discover one special vital case (Blue Block risk) that may induce unsafe conflicting train movements threatening working zone safety.

4.3.4 Generalized Attack Flow

The latter two attacks mentioned above would respectively impact the availability and integrity of the messages in the system, possibly resulting in direct effects on the safety and efficiency of railroad operations. Figure 4.3-1 below shows the generalized attack flow on an ATCS radio code line system (CTC applications) covering its major vulnerabilities.

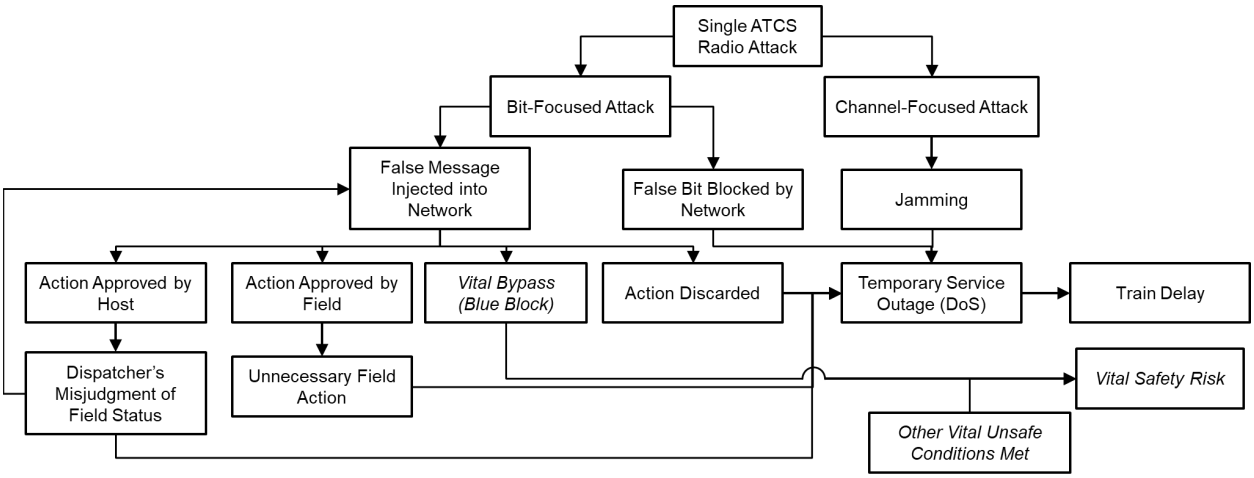


Figure 4.3-1 Generalized Attack Flow Targeting ATSC Radio Code Line

4.4 Consequence Analysis

With the identified risks and vulnerabilities, the research team selected the DoS attack and spoofing attack for further detailed analysis to explore the risks and corresponding consequences. The two types of vulnerabilities represent non-vital risk and vital risk, respectively.

4.4.1 Non-Vital Risk Case: DoS Attack on ATCS Radio Code Line

DoS attacks engaged in ATCS systems are the misuse case that follows the jamming misuse case. The execution flow of the simulation evaluation adopted by this subsection is shown in Figure 4.4-1 below.

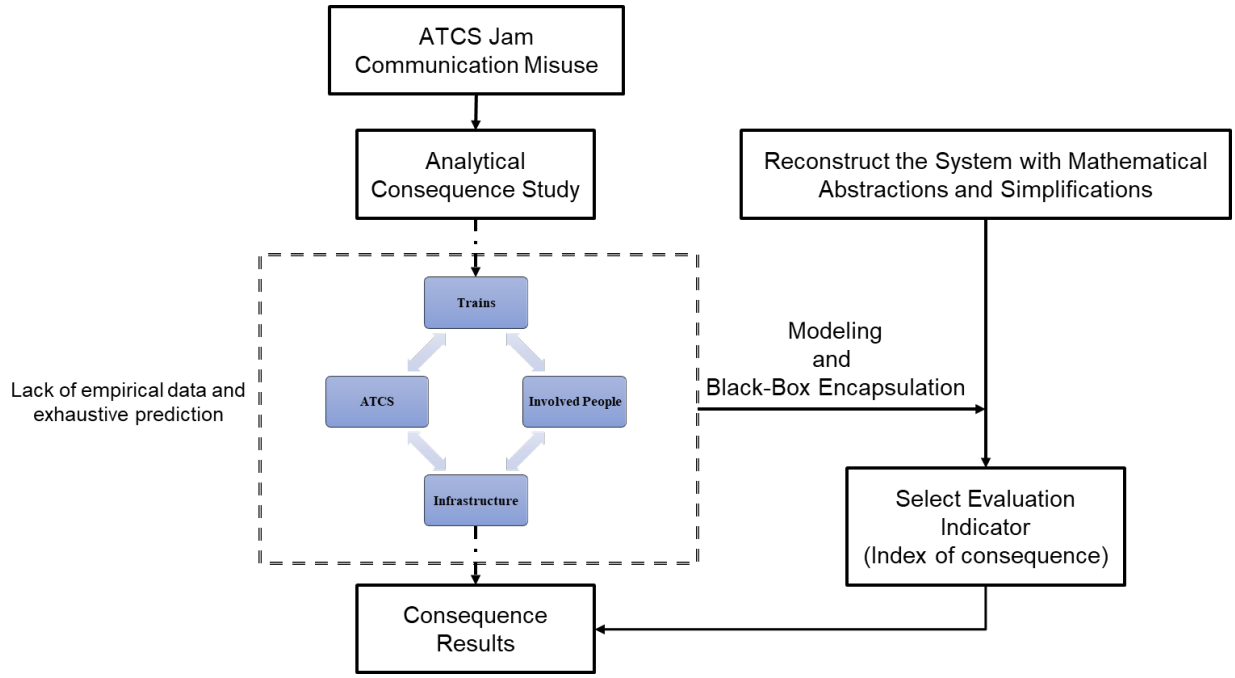


Figure 4.4-1 Execution Flow of Simulation Analysis for ATCS DoS Attack Risk Analysis

Consequence Analysis Methodology for DoS Attacks – Simulation Approach

Since engaging normal DoS attacks to block or jam the ATCS radio channel will not affect the function integrity of field vital logics, such vulnerability of ATCS radio code line cannot direct a railroad's operation into catastrophic incidents because of the vital isolation. An ATCS network only plays as a non-vital part of the CTC system. However, DoS attacks can create a service outage of an ATCS system, triggering the fail-safe mechanism of various layers to stop train movements immediately; in addition, operating rules always require the train crew to take the safe course (GCOR, 2015) to slow or stop the affected trains until the DoS is dissolved.

On the other hand, common countermeasures such as network intrusion detection systems and directional antennas take time for authorities to recognize and take actions (Alnifie & Simon, 2007). Presumably, the duration and aftermath severity depend on both the DoS attack itself and the response time of authorities. Although the intentions may not be clear for someone engaging DoS targeting railroads, its achievability justifies the research team to understand how the attacks would influence regular operations in the railroads. Therefore, once DoS attackers engage actions onto ATCS network, it would eventually introduce severe service disruptions and significant related costs.

As DoS attacks are fundamentally similar to a period of traffic outage, the corresponding rail traffic behaviors depend more on the railroad's networks/corridors with miscellaneous internal characteristics. In the consequence analysis of the non-vital risk case, the authors sought answers to the following questions:

1. How does the severity of the aftermath vary under a DoS attack at different locations or with varied durations with the same traffic pattern?
2. How do different traffic patterns (e.g., traffic density, volume, direction, heterogeneity) influence the severity of the same setup of a DoS attack?
3. Would traffic recover after an attack? If so, how long is the recovery time under different conditions?
4. To what extent does the degree of influence vary among trains by attributes (e.g., speed, acceleration, priority)?

Since traffic behavior in a railroad's operations is closely associated with the train delay, the focus will be on the delay level introduced by a DoS under different prior operational patterns. According to industry experiences and common practices, software-based simulations are suitable tools for this problem. Most off-the-shelf rail simulators are proprietary software for regular planning or validation usages, so that customizing for special cases (e.g., DoS analysis) is hard to achieve. Therefore, the research team developed its own simulator based on open-source platforms, especially the Python 3.7 programming language and the Networkx 2.X library for the framework of the rail network. One may assume that a successful DoS attack on ATCS radio code lines would trigger the vital logic signal protection to indicate a stop aspect at that location, in which the affected trains are assumed to react accordingly, simulating the congested traffic scenario. Research results in this report will focus on simplified unidirectional traffic patterns.

Simulation Setups

The ATCS railroad network could be regarded as control point nodes with MCPs linked by a series of railroad blocks. Therefore, the minimum representative unit for a large railroad network is a single-track segment with both end points as traffic in/out vertices. Naturally, the block inside the segment is the minimum unit to be affected under a DoS attack. The authors assumed the block to drop signals from any favorable aspects to stop as the inherent response to a DoS attack. There are also blocks with passing sidings to allow a train to pass another. In the simulation case study, a simplified single-track segment with 10, 5-mile-long blocks was designed. Two passing sidings were located at the fourth and seventh block to represent a typical U.S. single-track corridor with a ACTS radio code line. For simplicity, it was also assumed that bi-directional traffic in general trends would react similarly to unidirectional traffic in terms of DoS attack responses. Figure 4.4-2 below shows the topology of this segment as the subject of this simulation.

Figure 4.4-2 Setup for a Single-Track Corridor Used in the Simulator

By default, only one train is allowed in a block at the same time. The signaling logic in this section is defined as a "speed signaling" scheme, indicating the simulated trains would have their individual target speed in each block. Different target speeds are defined and set to assure safe train separations. In this case, the target speeds are assumed to be four constants: Clear, Advance Approach, Approach, and Stop. Corresponding train actions are reflected in Figure 4.4-3 below.

- Clear (target speed as 72 mph, indicating the next three blocks are unoccupied)
- Advance Approach (target speed as 40 mph, indicating the third block has a train)
- Approach (target speed as 20 mph, indicating the second block has a train)
- Stop (target speed as 0, indicating the next block has a train or a DoS attack engaged at this location, triggering the fail-safe protection of the ATCS system)

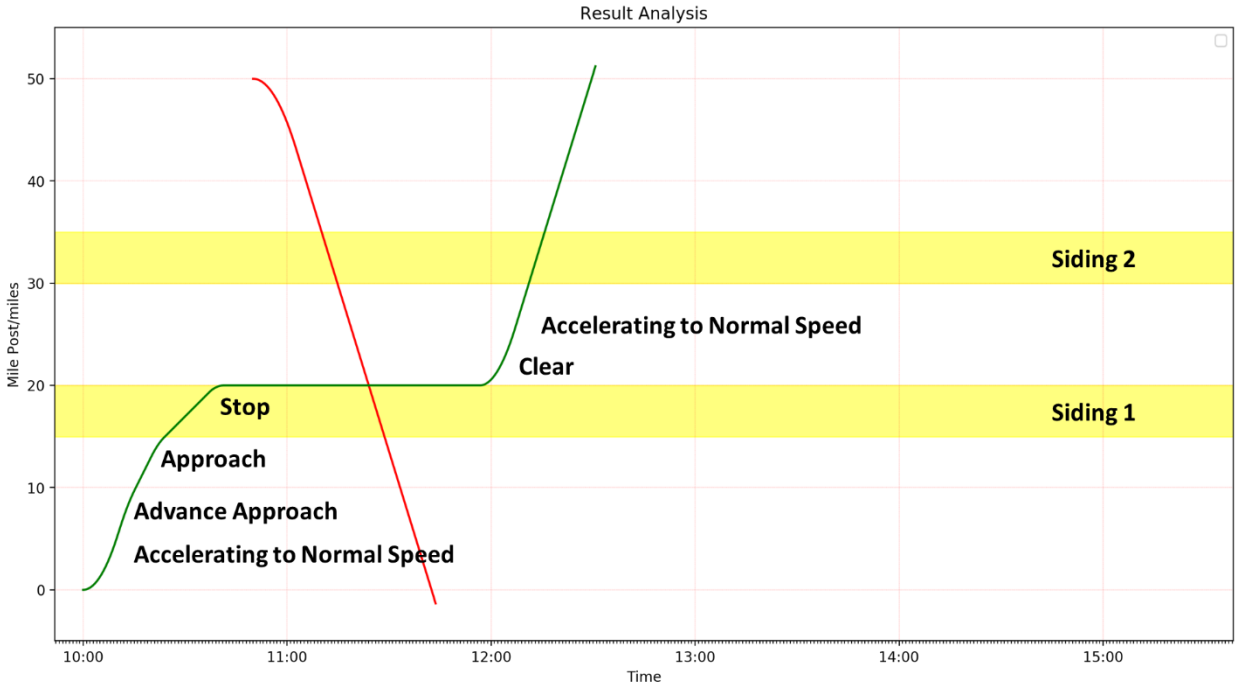


Figure 4.4-3 Speed Signaling Mechanism Adopted in the Simulation Tool

In reality, trains operating on the same corridor vary in types. They have heterogeneous attributes due to their individual operational characteristics, such as mixed traffic among passenger trains and freight trains (e.g., manifest, intermodal, and unit freight trains). Such traffic heterogeneity essentially includes intense interactions among different trains. The heterogeneity is also the major factor impeding the analytical method to evaluate DoS effects of railroad operation. This introduces more unpredictability and a higher delay level compared to trains initialized with homogeneous patterns (Dingler *et al.*, 2009). In the simulation corridor, each train is programmed, defined, and initialized from the starting point (left) of the first block. Rail traffic heterogeneity consists of randomized train speed, acceleration, and headway within a realistic range, as shown in Table 4-2.

Table 4-2 Demonstration of Train Attributes Used in the Simulator

Train Attributes	Mean Value	Variance
Speed	54 mph	18 mph
Acceleration	6 mph/min	2 mph/min
Headway	500 seconds	100 seconds

Values of the target speeds and any other parameters are flexible to change according to customized simulation needs. The target speeds (signal aspects) in the simulation is updated in real time with the presence of trains and passing logics. As for the numerical parameters, in this simplified preliminary model, the block length has been set as 5 miles each, totaling 10 blocks for this segment. Two passing sidings are located at the fourth and seventh block to represent a typical American single-track corridor setup.

In addition to the range of the speed, the higher-speed trains have been constrained with higher acceleration (and vice versa), indicating the mixed passenger trains with freight trains. With unidirectional traffic, this simulator defines higher-speed trains with higher priority, serving as the judging condition when a passing is about to occur at the pre-defined siding locations.

Compared to industrial practices where train passes are determined by the train dispatcher with consideration of miscellaneous factors (e.g., train priority, de facto delay, dynamic traffic demands, working zone windows, etc.), in this simulation researchers pre-defined the passing conditions before the simulation started, for simplicity. This eliminated the human influences onto the rail traffic output and made the results impersonal and objective, providing a theoretical baseline for further simulations that contained more realistic variables. However, it is discovered that such simplification would also sacrifice some practicality compared with industry practices. In general, since the train with higher speed has higher priority, one can argue the current setup still holds. In the future, the research team will use some industrial-level practical data to calibrate the simulation for better results. The adopted passing logics are described below:

- When a train encounters a block with a siding, and the train immediately behind it has a higher speed, set the slower train as pending pass status.
- If the slower speed train has an acceleration within a 10 percent difference (10 percent is an assumed value) from the higher speed train, the passing would occur (mimicking the common dispatching logic that protects the heavy, slow trains from frequent starts and stops).

When a passing event is confirmed, the home signal aspect for the slower train is dropped to stop at the end of the siding, indicating that the target speed drops to zero, and correspondingly clears the signal for the passing train behind. Similarly, when a DoS attack engages at a certain block, such as jamming the 900 MHz channels, any signal guarding the block is also dropped due to the fail-safe mechanism, until the attack is resolved.

Team researchers acknowledge that various DoS attacks may have their individual mechanisms to affect the rail traffic. For example, in some scenarios, a train can be slowed down instead of completely stopped. They assume the traffic responsive behaviors to be consistent due to a lack of practical information on railroad operational practices. In this simulation, the braking capability of trains in the simulator is extremely underestimated (to make a conservative case leading to maximizing the effect of DoS disruption). In other words, all trains in the simulator have to brake earlier to satisfy safety rules, causing additional traffic delay besides DoS-induced service disruption. Although this is not as realistic, it provides a more conservative scenario where the DoS attacks will make more severe impacts on general traffic because of the conservative brake calculation and a quasi-realistic acceleration pattern of trains.

The simulator runs on a time-incremental traversal basis. The optional refreshing time value (time resolution) is set as 1 second, depending on the scale of simulation system. Trains are generated according to a dynamic and customized headway, reflecting the variable rail traffic density. In each refreshing loop (traverse), all trains are calculated in sequence with the next incremental position value depending on its target speed, braking curve, and current attributes, in which the target speed encapsulates the block status, passing logics, as well as abstracted DoS attack information.

In the simulation, the train starts to react to an updated target speed immediately after the target speed updates. In reality, it is subject to the visual distance from signals to the locomotive engineers. However, immediate reactions are achievable if any advanced cab signal is in place. In the current case, the team adopted the latter scenario, and trains calculate braking or accelerating consistently with newest target speed that acknowledged by each.

DoS attacks are defined with two variables: location and time period. It is specified that the DoS attacks in this simulator will drop the stop signal for the specific location (block) per its start time and clear the signal per its stop time. The time period is assumed to cover from the attacker engaging the DoS until the DoS is destroyed or defeated by counter forces. After the DoS attack, the operation resumes, and trains start to recover from the DoS congestion. If the headway is very small, presumably the DoS would keep its influence; on the contrary, the traffic may recover faster from a DoS if the headway is set larger, indicating light traffic density.

Simulation Execution and Results

In this study's 10-block, single-track corridor, researchers selected the left point of the corridor as the originating base for right-bound unidirectional trains. They chose three types of traffic density (defined by train headway distributions) with varying DoS durations and locations for analysis illustration. Except for the headway being controlled, the other traffic heterogeneity attributes (train speed and acceleration) and simulation epoch period were set by default. The setup parameters are listed in Table 4-3, and corresponding simulation results are shown in stringline diagrams as Figure 4.4-4, Figure 4.4-5, and Figure 4.4-6.

Table 4-3 Simulation Setups for Analysis

Attributes	Setup 1	Setup 2	Setup 3
DoS Duration	*From* 11:30:00 *to* 12:30:00	*From* 11:30:00 *to* 14:30:00	*From* 10:30:00 *to* 11:00:00
DoS Location	3rd block (not siding)	4th block (siding)	2nd block (not siding)
Headway Range	[400s, 600s] Medium traffic	[300s, 500s] Dense traffic	[1200s, 1500s] Light traffic

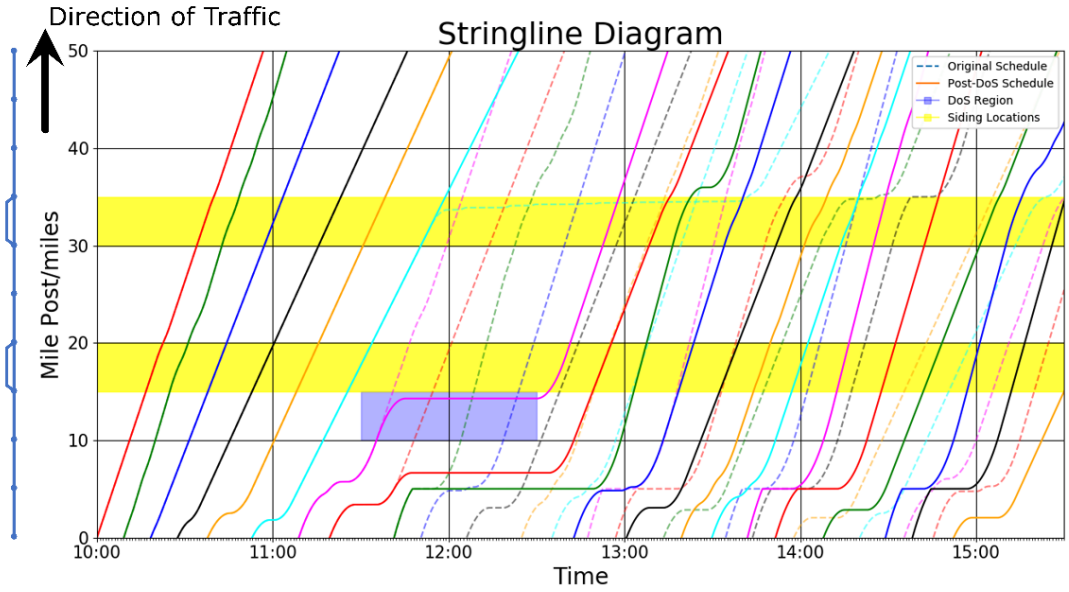


Figure 4.4-4 Stringline Diagram for Simulation with Setup 1

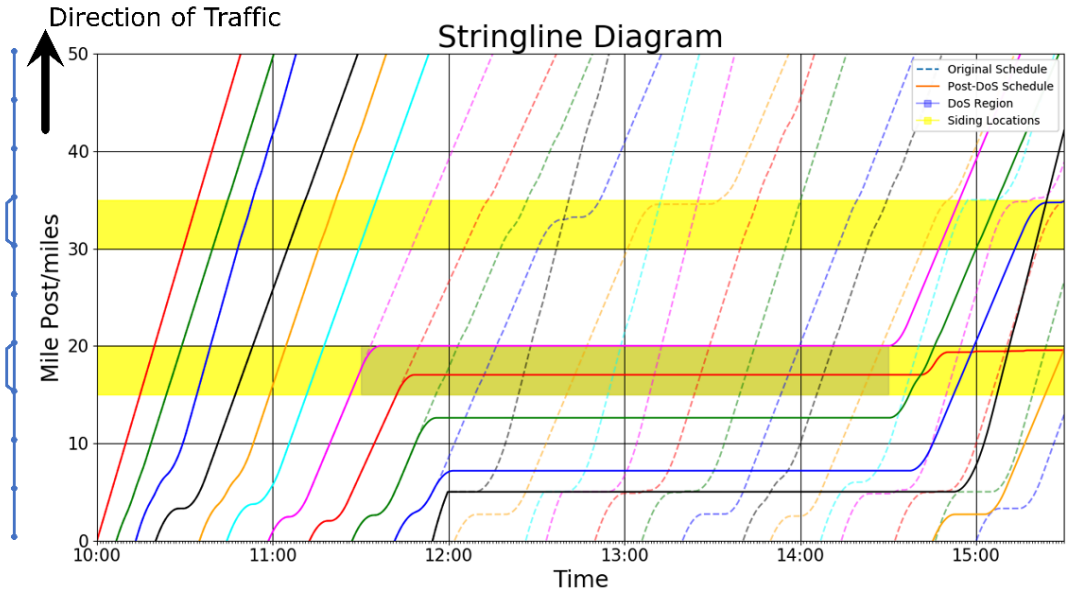


Figure 4.4-5 Stringline Diagram for Simulation with Setup 2

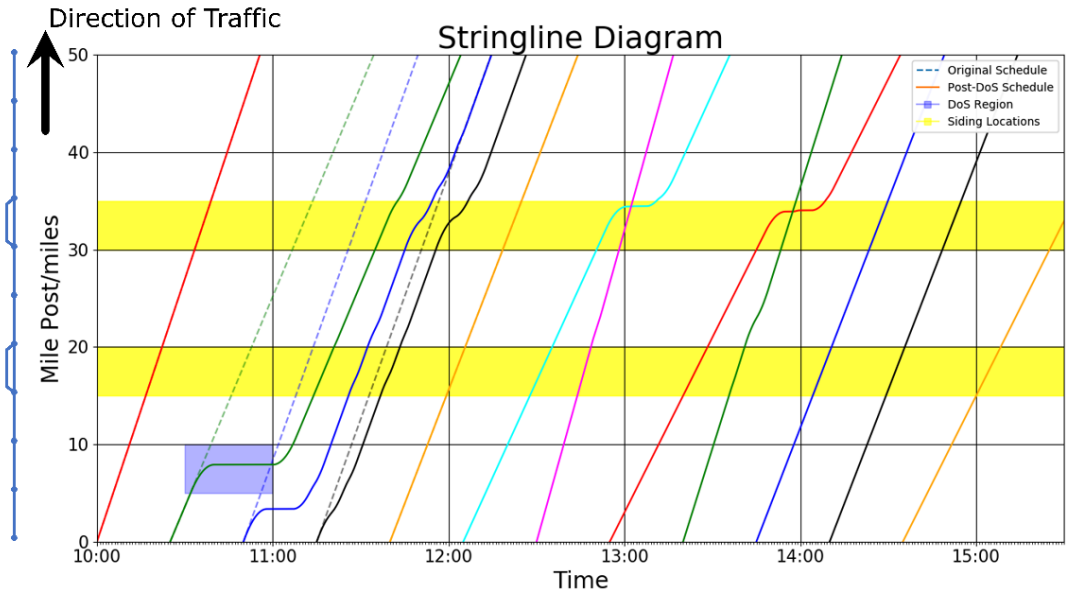


Figure 4.4-6 Stringline Diagram for Simulation with Setup 3

As can be interpreted from Figure 4.4-4 to Figure 4.4-6, under certain circumstances, including comparatively lighter traffic with shorter DoS duration of effect, traffic can recover from the delay.

Conclusions of Simulation-Based DoS Attack Risk Analysis

Preliminarily, researchers focused on the capacity and redundancy of unidirectional traffic in this single-track corridor. Because of such redundancy, when DoS attacks are engaged, rail corridor sections left of (upstream of) the attacked area will reach its capacity. Meanwhile, the section right of (downstream of) the attacked area is freed from traffic because of the blockage. Once the attack is dissolved, the traffic recovery potential will automatically use this freed downstream capacity to ameliorate total impacts. This triggers the research for further simulations to understand the how the changing variables (e.g., DoS delay durations, DoS attacking locations (such as MCP-targeted, BCP-targeted, etc.), DoS attacking time slots, etc.) would impact the DoS disruption, as well as the sensitivity of train delays to the DoS attacks themselves.

With the current simulation tool, researchers could analyze case-specific ATCS DoS impacts provided with specific rail traffic data and network topology. On top of the DoS impact analysis, the tool can also output the traffic amelioration behavior once the DoS attack is dissolved. The limitation of this simulation approach is that the team didn't have any real data of DoS attacks targeting railroad ATCS systems. The simulation results are based on assumptions and modeling only. As a summary, the major assumptions and simplifications adopted in this approach are listed in Table 4-4 below. In the future, team researchers will work closely with real data to calibrate the simulator to ensure the integrity of cyber attack-related analyses.

Table 4-4 Major Assumptions and Simplifications Adopted in DoS Risk Simulation Tool

Categories	Items	Description	Notes
Train Motions	Train Acceleration	Fixed braking and acceleration rates are adopted for individual trains.	See Table 4-2
	Train Size (Length)	Trains are treated as 1-D object with fixed length and/or single mass point compared to the corridor size in analysis.	1 mile/none
	Train Speed	A variety of maximum train speeds following Normal Distribution are assumed for the 1-D operations.	N ~ (54, 18) mph
	Human Factors of Train Operation	Train motions are immediate in response to the signal aspects that the train is approached to.	0 s delay
		Human factors are ignored when operating trains.	
Signaling and Train Dispatching	Signaling Response Time	No delay time between signaling responses, such as block occupation update, cascading signal aspect changes, etc.	0 s delay
		DoS attacks would only result in successful fail-safe mechanism kicking-in with the most restrictive aspect displayed for the affected block.	0 percent fail-safe failure rate
	Target Speeds of Aspects	4 aspects speed signaling is adopted with consistent target speed for each aspect of each signaling location.	
		Target speeds are selected based upon ideal corridors without physical constraints.	72, 40, 20, 0 mph
	Trains Occupancy Rule	Only one train (part or whole) is allowed in a block or siding at each time moment without exceptions.	
Rail Corridor and Infrastructure	Track Topology	Single track corridor with passing sidings is selected to represent the most common U.S. freight railroad network components.	
	Track Alignment	No grades or curvatures are considered in this simulation for train tractive or braking calculation.	
	Block Length	5-mile fixed long blocks are consistent for all blocks used in the simulation.	5 miles
	Passing Sidings	2 5-mile passing sidings are arranged symmetrically for one train to pass another;	2 sidings at MP (10-15) and MP (30-35)
		Diverging speed limit is not considered.	
Traffic and Dispatching Logics	Traffic Directions	Only unidirectional traffic is selected for traffic response analysis because of time and algorithm constraints.	
	Traffic Patterns	Traffic density of trains is defined by individual headways in the simulation tool. The headways in each simulation are following uniform distribution.	e.g., uniform ~ (400, 600) seconds

		Trains are auto-generated when satisfying the individual headway requirements and block availability.	
		Trains exit the corridor automatically when reaching the end of the corridor.	
	Human Factors of Train Dispatching	Dispatching actions are immediate in response to the logical dispatching requests initiated by the dispatching logic.	0 s delay
		Human factors are ignored when for dispatching trains.	
	Train Priority	Trains with higher maximum speed have higher priority than trains with slower maximum speed.	Priority ~ maximum speed
	Passing Conditions	Only higher priority trains pass lower priority trains.	
		When higher priority trains follow the slower priority trains by one immediate block behind, the dispatcher logic diverges the slower train into siding.	
DoS Attack	Location	DoS attacks initiated in the simulations are assumed to be applicable to individual blocks. Entire block will be affected, and no entrance of trains will be allowed.	Block index 1, 2, 3 are selected in the three simulation setups.
		Signal aspects will be correspondingly downgrading according to the aspect favorability when DoS attack engages on a certain block.	
	Duration	DoS attack durations are flexible in settings. Usually in hours. Block will immediately be freed from DoS attacks when the end time is reached.	0.5, 1, 3 hour(s) are selected in the three simulation setups.

4.4.2 Vital Risk Case: Blue Block Working Zone Spoofing Vulnerability

Based on the working flows and spoofing attack potentials, the research team identified the Blue Block feature as one of the few exceptions of ATCS-based CTC operations where spoofing messages may potentially bypass the fail-safe design and impose a higher risk of unsafe train movements, where it is theoretically possible for a permissive signal to be displayed, authorizing a train movement into a previously-established roadway working zone. Under a particular cyber attack context, such risk may threaten roadway workers' safety.

Blue Block Functionality

The Blue Block feature in CTC operations enables the dispatcher to remotely set the blue protection for a certain track segment. Blue protection in railroad operations provides safety to workers from the inadvertent movement of equipment on which they are working (Wang *et al.*, 2019). When Blue Block is set up, its switch (either a physical analog relay switch or a vital PLC-controlled logical switch) will disconnect and disable the corresponding home signal from being cleared into the protected section, while the default state for such switch is "connected," to enable the home signal to be cleared for regular operations. Blue Block switch is "connected" by default, normal CTC operations won't require any actions of the Blue Block switch.

Blue Block feature enables the dispatcher to take a segment of track out of service by isolating the entry signal from field vital logics, so as to keep the most restrictive aspect for the protected

track segment. Ideally, this feature would provide an extra layer of protection to further reduce the risk for the unexpected clearing of a signal. Modern CTC radio code line systems inherited the Blue Block feature from the analog era. For example, in the early Blue Block design, a relay switch could prevent signals from being cleared due to a false lightening surge. This also enabled workers to perform maintenance over a protected track segment, such as C&S maintenance, switch machine maintenance, and general infrastructure maintenance. Figure 4.4-7 shows the normal conditions without a Blue Block setup (Blue Block switch keeps "connected," shown as a relay in this diagram). Although the procedures to set up a Blue Block (or similar functions) vary among different systems, they share similar basic principles.

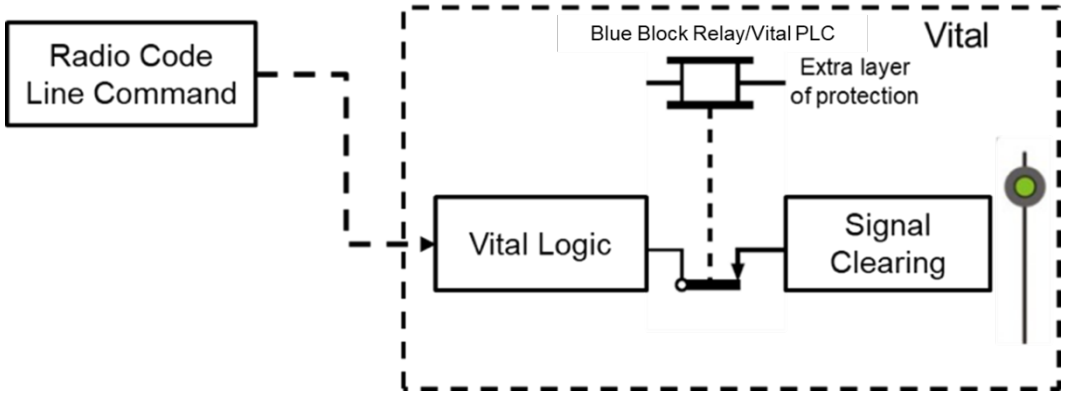


Figure 4.4-7 Default Condition (Without Blue Block Setup)

Simplified Risk Case – Feedback-Free Blue Block Setup

In a scenario where no feedback is required to request a Blue Block setup, researchers assumed that a single ATCS message would enable the Blue Block setup in the field, by disconnecting the Blue Block switch (shown as picking up the relay in the following diagrams). The switch is regarded as the abstraction of modern vital PLC-integrated function for the ease of illustration, instead of a relay-based switch in the analog era. Figure 4.4-8 shows the expected setup for a Blue Block – as requested by the dispatcher, in this case.

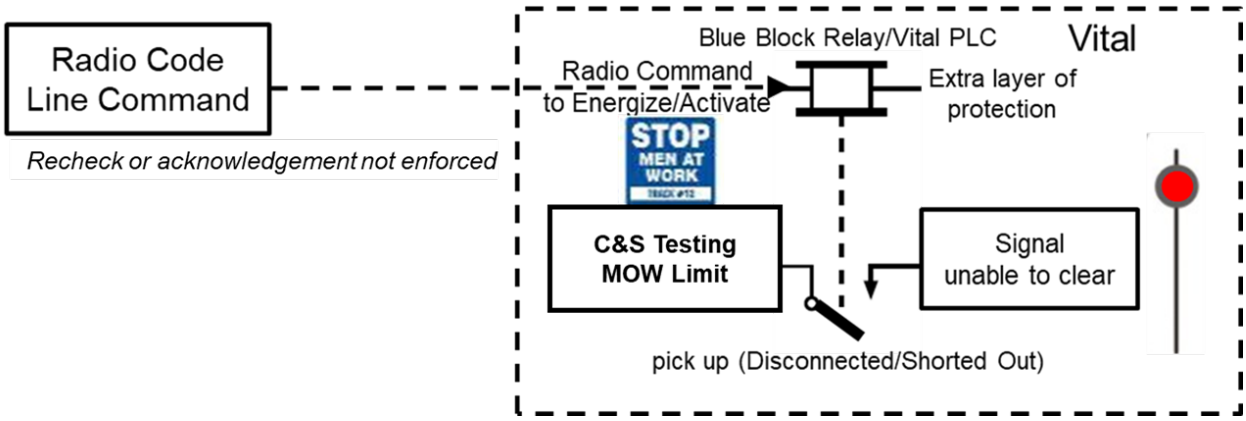


Figure 4.4-8 Blue Block Setup Condition (No Feedback)

According to the ATCS security vulnerabilities, jamming and interception may impede the ATCS request to set up the Blue Block against the dispatcher's desire. If this happened, the ATCS radio code line by itself is not able to validate if the Blue Block is successfully in place. In

the worst case, if any C&S testing actions are engaged by assuming that the Blue Block is in place, the signal may be accidentally cleared as part of the testing items. Figure 4.4-9 shows the worst-case scenario that an unsafe train movement that may occur due to Blue Block failure.

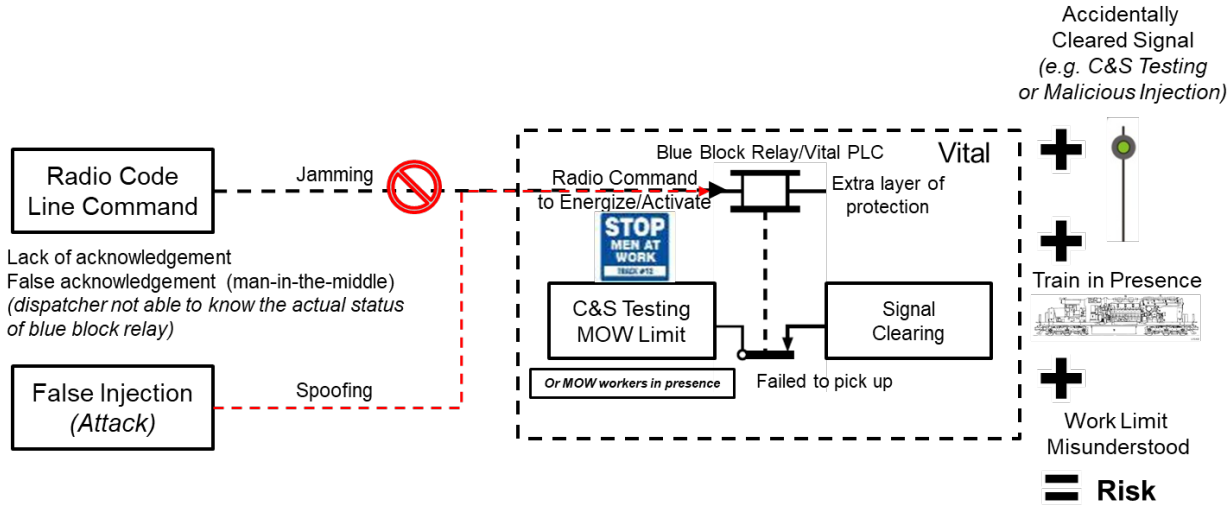


Figure 4.4-9 Unsafe Risk Potential by Blue Block Setup Failure (Feedback-Free Case)

Realistic Risk Case – Blue Block Setup with Acknowledgements

Realistically, the Blue Block setup sequence over the ATCS radio code line has integrated the acknowledgement feedbacks over the radio code line, plus multiple redundant verifications such as voice radio confirmation, track warrant issuance, etc. Railroads have strict requirements for voice radio acknowledgements and extra validations for a Blue Block operation.

In an example use case based on the practice of one eastern Class I railroad, the sequence flow to set up a Blue Block and speculated attacks against a Blue Block are illustrated in the sequence shown in Figure 4.4-10, below.

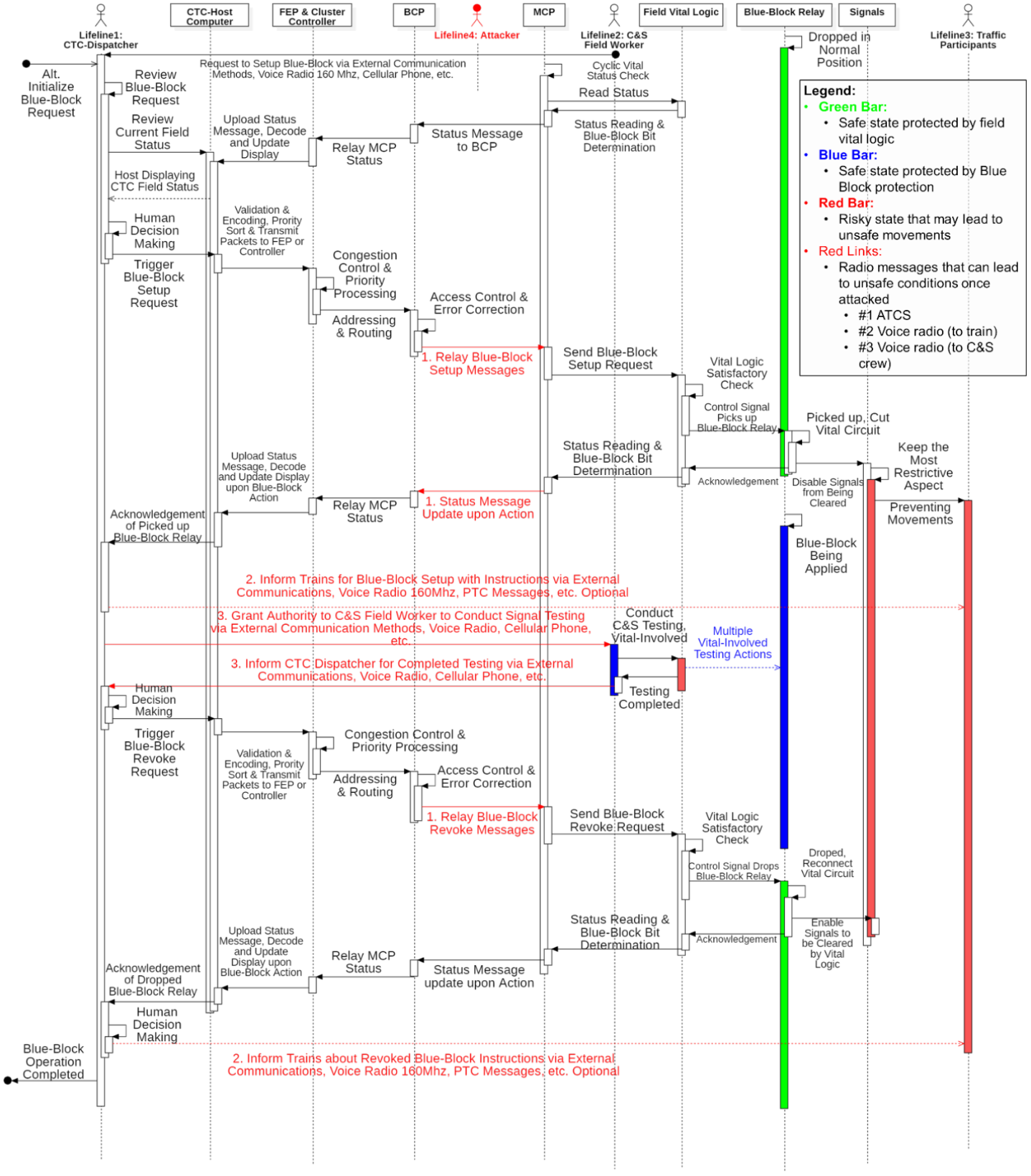


Figure 4.4-10 Sequence Diagram for Blue Block Setup over ATCS Radio Code Line

In Figure 4.4-10 above, there are three legitimate participants and one speculated radio attacker in place, in which the traffic participants represent crews operating trains or other track vehicles. The intention to set up a Blue Block comes from the dispatcher at the leftmost point. In this specific context, the roadway workers may conduct a series of signal testing on the field side, which needs the Blue Block application to avoid the accidental clearing of signal while testing. One can assume that the radio attacker stands at the radio link between central dispatcher and the remote MCP location, and he or she is able to jam or inject false ATCS radio messages. In this case, one can also assume that the spoofing attacks successfully avoided detections and surveillances during the whole process.

1. Regular Working Sequence of Blue Block:

   The setup or revocation of a Blue Block requires at least two pairs of ATCS radio messages. In each pair of messages, a request can setup/revoke the Blue Block, and an acknowledgement will update the field Blue Block status to the dispatcher's display. The acknowledgement keeps the two sides synchronized. Meanwhile, railroads impose the operational regulations for the three participants to verify the Blue Block status over each other via multiple mediums, such as using voice radio granting the authority to the field workers or C&S testing crew, as well as verifying the movement limit with involved trains or any maintenance vehicle on the track intended to be protected.

   Shown as red messages in the sequence diagram, these radio-based communication paths are critical for the consensus over the Blue Block status. They are also the necessary jamming objects to achieve the goal of introducing conflict train movements in the general spoofing attack. Shown in blue bars, the status of Blue Block and C&S maintenance verification provides the vital protection against conflicting train movements; the red bars for signals and trains show their individual restricted status under the protection from Blue Block.

2. Attacks against Blue Block that May Induce Hazard:

   By employing the spoofing attacks upon the vulnerabilities of ATCS, the knowledgeable attacker may prevent the field side from accepting the request message (e.g., by jamming), and then forge an acknowledgement message back to the dispatcher, faking a successful Blue Block deployment (e.g., by replaying, encoded simulation injecting, etc.). In this case, the protection and related restrictive signals may be assumed being deployed by the dispatchers, maintenance crews, and train crews. If this action proceeds, the C&S testing would bypass the intended protection and result in undesired signal clearing, imposing the risk unsafe train movement.

   The following necessary prerequisites are identified for the risk factors that could result in an unsafe train movement under a Blue Block attack risk case:

   - Successful request jamming and acknowledgement spoofing
   - C&S testing or successful ATCS spoofing may trigger signal clearing
   - MOW roadway workers' maintenance vehicle (e.g., hi-rail trucks) may not shunt the track circuits due to rubber tires, or other track shunting devices being absent.

(*Note*: shunting track circuits would enable the field vital logic to protect them, and this cannot be spoofed by remote attackers.)

- Successful voice radio spoofing (or lack of voice radio verification) – C&S testing crew's confusion of field status
- Periodic repeating of the jamming/spoofing sequence to match with routine health-related polling occurring between the back office and control points which will prevent a field site from indicating to be offline in the back office
- Train in presence
- Successful movement authority spoofing (or lack of clear movement limit) – train crew's confusion of movement authorities
- Miscellaneous human error, such as:
    - Miscommunication
    - Unsafe assumption
    - Negligence of risks of cyber security attacks

In some cases where no C&S testing is being conducted, the attacker needs to forge another fake signal clearing message request into the attacked control point and spoof the following ATCS messages between dispatching center and the control point. Any failed spoof in the following communications may result in the awareness of dispatchers and the discovery of the ongoing attack. This requires even more spoofing actions with accurate timing and encoding. The possibility for this attacking case is significantly less than the C&S testing risk.

Generally, due to multiple layers of required verifications in regulations or rules, plus frequent polling mechanisms in ATCS protocol and upper-layer detective features (e.g., the polling mechanism described below), such risk could be well-controlled by the railroads and related authorities. Although spoofing of a Blue Block is technically possible, the design attributes of a ATCS radio code line and railroad safety protocols render successful spoofing extremely challenging to accomplish as a practical matter, particularly for a duration where onerous safety implications could come into play.

One of the most prominent attributes of current practices is frequent polling designed between the back office and control points: control and indication radio code line messages contain all status bits for a given control point that can be generated at any time without warning the attackers. Such continuous monitoring and logging of events being executed at the back office compare the actual field status with an expected operation. Deviations are immediately pushed out and made known to railroad personnel in real time. In terms of railroad protocols, when such deviations are observed, qualified personnel are notified in a timely manner to investigate. Another equally relevant factor is when observed deviations appear to be inconsistent with routine status, railroad safety practices dictate that the signal system in the affected area shall be removed from normal service until qualified personnel can investigate and make necessary recovery responses. To date, no similar attacking precedents have ever been reported.

4.5 Risk Mitigation Strategies

Aiming at the analyzed risk cases above, this study proposes some recommended practices to minimize the corresponding risks. Although the risks cannot be exhaustively enumerated, the proposed mitigation strategies may also eliminate some undiscovered risks because of the patching to ATCS flaws.

From the cyber security standing point, the authors regard the legacy radio communication protocol of ATCS as the "condemnable" flaw that needs patching improvement and specific protection. To minimize the risk, researchers selected three major aspects for consideration: communication mediums, encryption algorithms, and network protocols.

4.5.1 Communication Mediums

Spread Spectrum

The jamming and spoofing of an ATCS signal could be made more difficult by using spread spectrum radios. Many spread spectrum radios use unlicensed radio frequencies. Railroads have looked into using an 802.11 protocol (spread spectrum[1] on unlicensed frequencies) and CDMA (cell phone spread spectrum on licensed frequencies) as possible alternatives to ATCS frequencies (Craven & Craven, 2005). This would mean that ATCS would either be replaced altogether or piggyback on these other transport protocols, similar to the cellular backups introduced below.

Fiber-Optics and Other Carriers

Another effective way to prevent DoS attacks and spoofing attacks would be to use an entirely different medium as a backup for communications. Conrail Shared Assets and Amtrak's Northeast Corridor have already deployed fiber-optics as the substitution to 900 MHz radio code line for their CTC system. It is unclear if ATCS networking protocol is still hosted by their fiber-optics network or not. However, even if ATCS protocol is still in place, concurrent eavesdropping attacks can also be forced out because of the almost-impossible accessibility of fiber-optics. One of the supporting facts is that there is no active ATCS Monitor activity in New Jersey. This is because the major freight lines (Conrail Shared Assets) and passenger lines (Amtrak, NJ Transit) are not using ATCS 900 MHz radio code line as the CTC communication medium.

If the ATCS protocol is deployed within a small area, local area network (LAN) without wireless transmission is also an alternative to the radio code line. In remotely controlled bridges and

[1] Initially, U.S. railroads chose to utilize licensed channels for most safety-critical wireless communication applications transmitting voice or data. This is mostly due to the general perception within the industry that using spread spectrum radios and their unlicensed frequencies would result in decreased reliability of applications where these types of radios were employed. However, in recent years, owing to the wide availability of spread spectrum radios featuring deployment costs that are often less expensive than radios that utilize licensed frequencies, railroads have utilized spread spectrum radios in some applications where the radio's frequency hopping feature can be used to help maintain reliability of the links. Railroads have also utilized cellular phones operating on common carrier networks for code line, generally as backups to dedicated leased circuits or where there is no redundant BCP available for an MCP-equipped control point.

DTMF switches, if any ATCS protocol is in place, the communication links over ATCS protocol could be hosted by LAN because no long-distance radio links are needed for the application.

4.5.2 Encryption Algorithms

The CRC check is currently available in the ATCS protocol as the only authentication for messages. However, in the ATCS application, CRC is used to verify message integrity and thus transmission efficiency rather than to enhance message security. CRC mainly serves the validation of the communication to improve the packet loss rate. CRC cannot prevent unauthorized access if the CRC checksum polynomial is open to attackers. Meanwhile, encryptions have already been integrated in PTC systems such as I-ETMS. Security algorithms are in place to prevent the unauthorized access and spoofing of safety-critical messages when they are communicated via radio, internet or a public switched network. Advanced Encryption Standard (AES) is selected in I-ETMS as approved by National Security Agency for top secret information. Referring to PTC, a ATCS radio code line may also implement similar encryption algorithms to screen for public accessibility.

One of the foreseeable limitations is that the legacy networking protocol may restrict the throughput of ATCS when encryption is implemented. Any imposed encryption may increase the traffic level, and packet size in its network that may top out its limited bandwidth.

4.5.3 Network Protocols

PTC Hosting

Radio code line over PTC is another feasible solution to eliminate ATCS vulnerabilities by hosting radio code line traffic on the 220 MHz PTC communication protocol. It is being discussed internally by some railroads. Once switched over, the PTC protocol with encryption can help to eliminate radio code line eavesdropping and spoofing unless the PTC is hacked. Discussions over such vulnerability is out of the scope of ATCS, instead, it is the security topic of PTC system. In addition, the greater capacity in PTC 220 MHz channels would significantly facilitate ATCS traffic, as the latter was designed with only 4,800 bauds (AAR, 2005). The only challenge is to set up transition plans and preventive strategies to eliminate risks associated with unstable ATCS/PTC services in system modification, which by nature also associates with costs.

Cellular ISP Hosting

In addition, to improve system redundancy and reliability, most Class I railroads have already selected their collaborators to back up their 900 MHz radio code line service over cellular carriers. For instance, Union Pacific and Norfolk Southern have selected Verizon in some subdivisions as the emergency cellular backup for their CTC applications. These railroads still prioritize the use of their dedicated 900 MHz radio channel to operate the ATCS protocol to save cost. Therefore, even if the jamming of the radio code line is successful, CTC territories with cellular backups can switch to cellular services with a flexible transition, unless the cellular channel is jammed, too. Generally, cellular hosting is more stable than ATCS 900 MHz channels because of more sophisticated carriers. Cellular hosting used for code line has two primary advantages over the use of 900 MHz: the timeframe for deployment and the cost of initial setup. Disadvantages of use of cellular services are that they involve monthly recurring costs which in the long term can be considerable, and costs for occasional equipment replacements brought

about by changes in technology. In practice, for mission-critical applications, railroads prefer communications solutions that they own and maintain, rather than depend on external parties to maintain these services.

4.5.4 Risk Mitigation for Blue Block-Targeted Spoofing Attacks

The risk mitigation strategies mentioned above could significantly reduce the risk of spoofing and jamming attacks. However, this study specifically considers some practical solutions to counter Blue Block risk under a concurrent ATCS application scheme.

Since the discovered Blue Block risk case imposes theoretical vital risk on roadway workers and a C&S testing crew when the track cannot be shunted, the first practical mitigation strategy is to require the application of shunting devices on tracks or jumper wires inside the control point bungalow to shunt the track circuit. Such actions can safely simulate an occupied track as an input to field vital logic.

However, the research team also noticed that the application of jumper wires has its own human factor risks: For example, the derailment of Amtrak at Niles, Michigan on October 21, 2012 was caused by mistakes in jumper wire application (NTSB, 2012). NTSB said the accident was caused by the negligent use of jumper wires when trouble-shooting defects in the signaling system. In addition, application of a traditional shunt device requires the crew to enter the gauge-side of the track – with inherent risks. Therefore, further research is needed to study the tradeoffs between the application of shunting to prevent Blue Block spoofing attacks and the risks introduced by the application of track circuit shunt. If adopted, more training and specific regulations are necessary for introducing new devices.

In a similar vein, some state-of-the-art devices can also be installed along the tracks for fast and efficient working zone safety protection. Such a design shunts the track circuit immediately when requested by a smartphone without entering the tracks. With such devices available, the Blue Block risk could be minimized without introducing extra risks.

In addition to the jumper wire or shunting solution, another possible practical way to prevent Blue Block risk is to require an additional foreman for extra layer of protection. The additional foreman may be responsible for monitoring the radio channel availability and abnormality, as well as warning the workers if any rail traffic is approaching.

4.6 Conclusions

The applications of the ATCS protocol in North America are mostly confined to radio code line communication, supporting the CTC systems in a non-vital role. Due to the non-vital part of the design and its placement in the architecture of higher-level systems, direct adversarial manipulation of the ATCS protocol itself and its corresponding communication networks would not result in an instant failure of railroad safety protection against hazardous train movements.

However, ATCS communication networks are easily accessible by the public, making the network susceptible to channel disruption and DoS jamming, which can disrupt regular railroad traffic to varying degrees. Public eavesdropping activities are already widespread throughout the country, causing proprietary non-vital railroad information to be leaked to external observers. Although precedents involving intentional ATCS channel jamming and DoS attacks have not

been discovered, this study's preliminary consequence analysis has shown that hypothetical DoS attacks may be able to achieve severe traffic interruptions of CTC operations.

In extreme conditions (such as Blue Block-targeted attacks), successful packet injections into a ATCS network may result in vital risks to train movements. This requires attackers to have extensive knowledge of the ATCS system, its upper-layer applications, railroad operational rules, and accurate timing of involved parties. A series of conditions (like modeled steps in the sequence shown in Figure 4.4-10) need to be satisfied in a chained manner to achieve the ultimate goal of unsafe train movements. Therefore, the vital risks of ATCS do exist, but they would be extremely hard for lower-capability attackers to exploit.

Noticeably, recent trends in RIoT developments at North America railroads focus on the growth of the PTC system. ATCS protocols are getting phased out as more advanced communication systems are being introduced to RIoT applications to support PTC, which has higher safety and efficiency system requirements in all dimensions than ATCS itself.

5. Selected Use Case – Remotely Controlled Movable Rail Bridges

Movable bridges are complex structures requiring considerably more design efforts and maintenance than non-movable bridges. Movable railroad bridges require a system for moving the bridge and for notifying both railroad personnel and watercraft operators about the correct timing when it's safe for them to move across. Additionally, the movable bridge system must be able to determine when the bridge is safe to move: when the bridge is locked, and the movable rails are properly aligned with the stationary rails. Such requirements ensure the trains can smoothly move over the joints between the two separate parts.

Although both modern and recently reconstructed movable railroad bridges have vastly more complex systems of communications and controls than older bridges, many bridges are still manually operated, often by an operator stationed on or near the bridge. As local conditions change, the desire to reduce the number of operating employees increases; when finances permit, many of these manually controlled movable bridges are being rehabilitated to permit remote control.

Since communications-based applications are adopted for governing the traffic of both water and railroad, the authors deem remotely controlled movable bridges as RIoT applications. Following the ATCS section, a remotely controlled movable bridge is the second use case object for this cyber risk analysis. This section will explore the security vulnerabilities and concerns that these movable bridges may induce. Typically, there are three types of movable railroad bridges – swing, bascule, and vertical lift. This section focuses on a railroad swing-type movable bridge, shortened as "swing bridges."

5.1 Overview of Remotely Controlled Movable Rail Bridges

Modern, movable railroad bridge systems control physical equipment using both hardware and software for communications and signaling. Their mechanical and electrical components are engineered to move heavy concrete and steel structures to allow traffic flows on rail, highways, and water, many times a day while withstanding harsh weather conditions, such as storm surges, earthquakes, and high and low temperatures. The span of such bridges must also support varying loads of rail and/or vehicular traffic. Figure 5.1-1 shows a typical movable railway swing bridge operated by BNSF Railway.

Figure 5.1-1 A BNSF Movable Swing Bridge

In the U.S., swing bridges are mostly found in low coastal areas (such as the coasts of New England, Louisiana, Florida and New Jersey, and the Great Lakes area) or states with long inland waterways (such as Wisconsin, Illinois, and Oregon) (Abrahams, 2000).

While automobile bridges may be somewhat lighter, railroad bridges must withstand the weights of the track and trains, as well as vibrations that differ from highway bridges. Such characteristics impact the higher dynamic impact loadings of railroad bridges. These and other concerns have resulted in safety specifications of both over-bridge and under-bridge traffic. Railway bridge recommendations are detailed in AREMA's Manual for Railway Engineering Section 15, Steel Structures Part 6 on Movable Bridges (AAR, 1997). In addition, 1980s federal regulations (Bridge Lighting and Other Signals, 33 CFR § 118, 1986; Movable Bridge Locking Inspection, 33 CFR § 236.387, 1984; Movable Bridge, Interlocking of Signal Appliances with Bridge Devices, 49 CFR § 236.312, 1984) and the recent Signal & Train Control Manual (Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances 49 CFR § 236, 2010) collectively specify safety regulations for over-bridge railways and under-bridge seaway traffic.

Modern movable bridges have complex structural and mechanical designs where the movements are controlled by latest processor-based control systems. Meanwhile, some movable bridges are still manually controlled, such as the Livingston Avenue Bridge in Albany, New York. The structural components consist of a fixed span, movable span, machinery that moves the movable span, locks that hold the movable span in place, and the over-bridge and under-bridge mechanisms that regulate the passage of rail and seaway traffic to be synchronized with the bridge movements.

Movable bridge components consist of a drive train, gearing mechanisms to move the movable span and locks on the bridge and govern the approaches to the bridge. Safety is enhanced by having safe designs for all these components and their operations, including inter-component synchronization, as shown in Figure 5.9-1. In addition, for electrified railroad lines having third-rail or overhead power catenaries, corresponding components need to be moved up-and-down in order to allow the movement of bridge's main structure.

Most movable bridges are electro-mechanical controlled, either manually or by micro-processor or logic-based relay components. These components are located on both the movable and non-moving components of bridges, communicating via wired or wireless networks providing the following functions:

- Communicate status and instructions between the individual controllers, sensors, and actuators.
- Simplify bridge management for operators, such as *open* and *close* commands.
- Administrative interfaces that communicate system events and faults, and update software/firmware.

Undeniably, motivated attackers may attempt to target such bridge systems for catastrophic outcomes, such as installing flawed controller and communication logics that can affect actuators, manipulating wireless signals to alter PLCs, sensors, and communication systems. Movable bridges rely on elements both inside and outside their physical environment; by nature, mechanical and electrical components wear down over time; the transportation authority that owns the bridge may rely on a third party for electrical power, and these electrical grid systems may have their own unknown risks; the system architect also may not be able to eliminate human threats to the movable bridge. Potential motivated attackers for a critical infrastructure system may include adversarial nation states as well as insider (internal) threats, which is out of the control of bridge operators. Focusing on the internal elements, incorporating a process to identify and mitigate vulnerabilities within the system design process will reduce its overall risk.

In the post-Stuxnet era (Langner, 2013), there are new risks that have been introduced by PLCs (Henrie, 2013) and networked industrial control systems – the same components that control movable bridges. Therefore, the safety of a modern movable bridge is affected by both the faults in the physical, mechanical, and control aspects of bridges and the cyber security of the electro-mechanical components that move the bridge and regulate traffic over and under the bridge.

In these systems, unforeseen security vulnerabilities in the underlying system components could be exploited to cause service disruptions and function degradations. These in turn can cause failures, resulting in unsafe operational conditions. Conversely, control systems have built-in failure tolerant mechanisms (such as service degradations and terminations as fail-safe protection) that are called in response to observed failures. An attacker who is aware of such mechanisms can exploit these designs to intentionally trigger service degradations and terminations, compromising safety or causing other types of loss. A motivated attacker can exploit the intertwined nature of these two phenomena and create complex attacks that would cause unsafe conditions.

5.2 Composition of Movable Bridge Systems

This section describes the basic components and subsystems of railroad movable swing bridges.

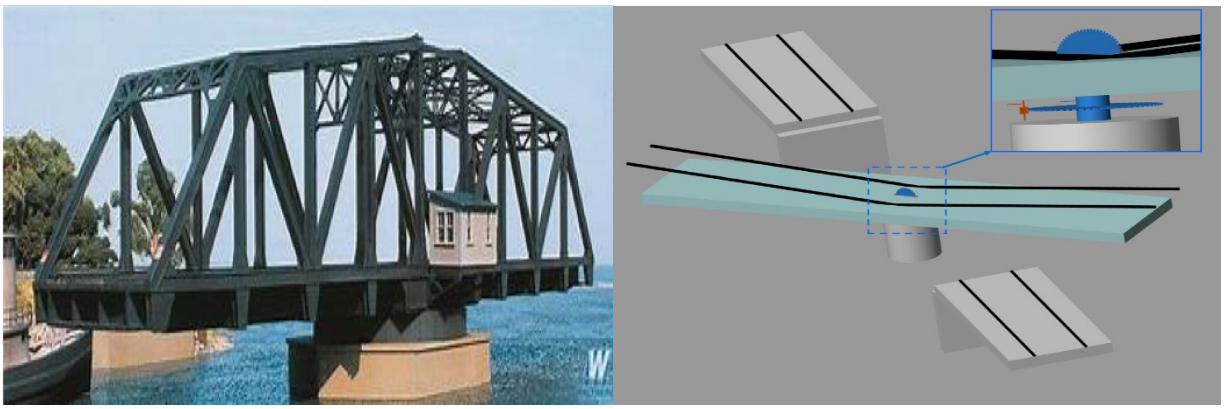


Figure 5.2-1 A Swing Bridge and Its Moving Parts

5.2.1 Superstructure and Substructure

A swing bridge *superstructure* consists of steel through truss or deck truss spans for longer bridges, or steel through girder or deck girder spans for shorter bridges. A swing bridge *substructur*e consists of the pivot pier and the rest piers, which are usually constructed of concrete or stone masonry. The pivot pier is typically located under the center of the rotating span with a navigable channel on both sides to allow water traffic to pass through the opened bridge, as shown in Figure 5.2-1. This also allows the span to remain balanced as it rotates, as shown in the right-hand side of Figure 5.2-1.

Fires, vehicular collisions, and environmental forces are some primary failure causes of a bridge superstructure system (Cook, 2013). As an example, in 2014, the 104-year-old Portal Bridge in New York City caught fire, resulting in power being cut to the bridge and a 70-minute outage requiring the delay or cancellation of 52 trains (McGeehan, 2014). Fires are especially a risk to the operator's house on the swing span that generally stores the bridge's drive control systems and electrical panels. Recent swing bridge renovation projects to address center bearing issues include the Court Street Bridge in Hackensack, New Jersey (Wolf, 2009) and the East Haddam Swing Bridge in Connecticut (Wolf, 2009). In 2010, the Somerleyton Swing Bridge in Norfolk, U.K. suffered a catastrophic failure due to its bearing system (Rimmer, 2010).

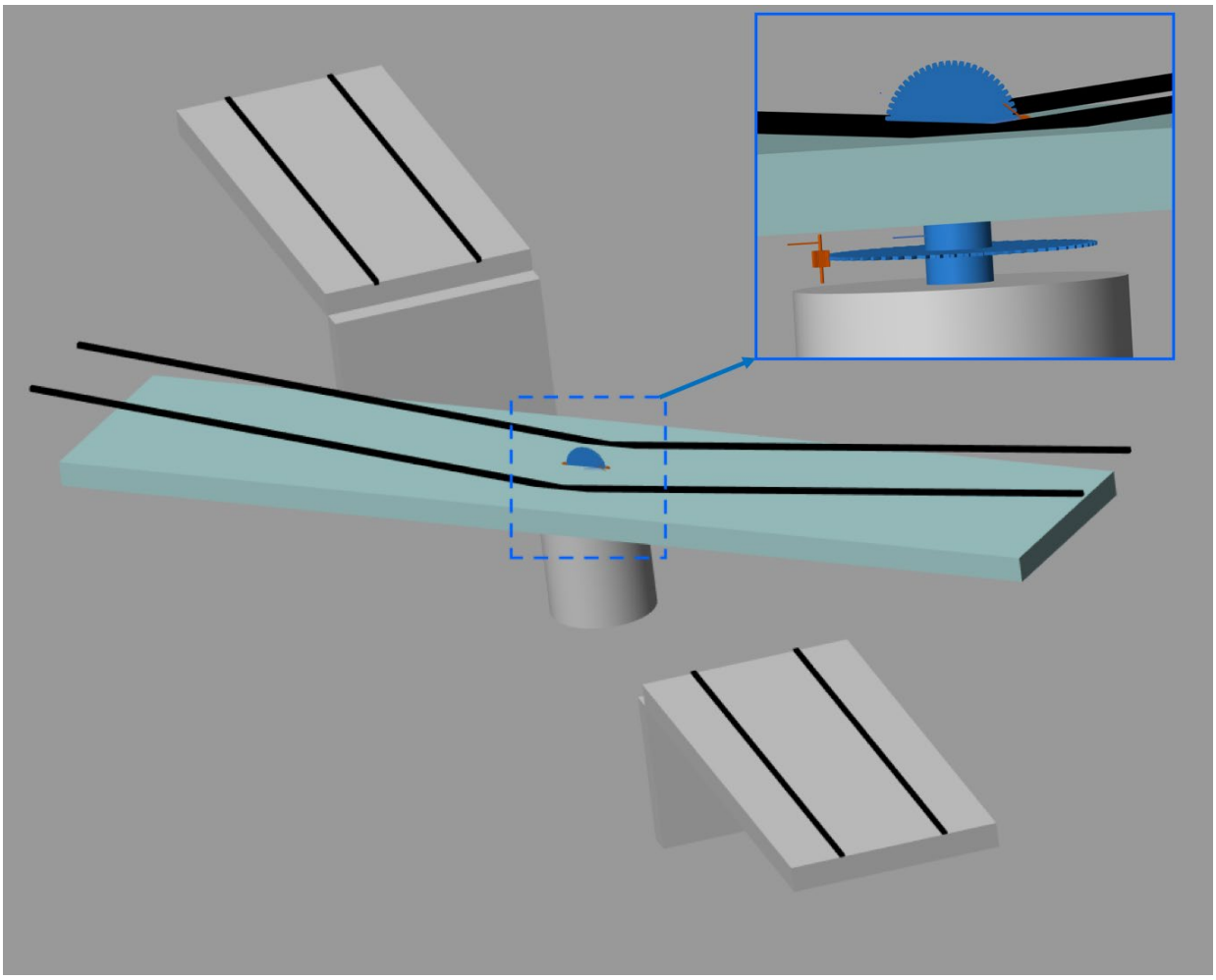


Figure 5.2-2 Swing Bridge Moving Span with Center Mounting Gear and Raised Rails

5.2.2 Mechanical and Electrical Systems

This section describes the mechanical and electrical systems that work together in modern swing bridge systems to control bridge movement, along with related faults and attacks that will be incorporated into an attack fault tree (AFT) model (to be defined later).

Support Systems

Modern swing bridges use mechanical bearing designs. From the mid-nineteenth century, the most popular ones have been *center bearing, rim bearing,* or *combined bearing* – this study used the first, as shown in Figure 5.2-2.

Systems that use a center bearing have a circular disk with a convex spherical surface fixed to the top of the pivot pier, which supports the bridge's weight while sitting atop a fixed convex disk on which the bridge rotates. When bridge is rotates, it is supported by its center bearing and balance wheels riding a circular track around the top of the pivot pier. The pivot pier distributes the weight and balances the structure, which requires regular lubrication. Older center bearing designs were known to be prone to failure due to inadequate lubrication and worn balance wheels and becoming unstable when unbalanced.

Wedges, or some other support systems, used to support the swing span when supporting live traffic loads, often require additional electro-mechanical components. Bridge failures could occur due to older parts in wedges that have degraded over time, such as the 2017 Little Current Swing Bridge failure in Ontario, Canada (CBC, 2017), or if a wedge completely fails, as in case of the 2014 Walk Bridge failure in Norwalk, Connecticut (ConnDOT, 2014). Wedges may also simply seize and stick in place, usually due to inadequate lubrication at the beginning of the movement process, preventing any further movement until the problem is manually resolved.

Rim bearing systems are supported by a set of tapered rollers that run along a track which spreads the load around the edge of the pier while the bridge moves. On top of these rollers is a large steel structure called a drum girder. The bridge rotates around a vertical post located in the center of the pier. Rim-bearing designs do not require auxiliary bearing supports such as wedges, which are required by center bearing designs. Combined bearing systems distribute the load by both rim bearing and center bearing components.

Drive Systems

The support system is rotated using a drive system, engineered to reduce friction, limit the impact of resistance during movement, and reduce the amount of torque output generated by the motor. A *shaft* is used to connect the support system to the drive system, generally connected to the rack and pinion system using a grid-type *coupler*. Additional force on the bridge span caused by overweight vehicles could result in damage to a worn shaft or rack-and-pinion system. Gear drives could be either open or enclosed gearing systems (for example, a gearbox as an enclosed example), depending on the bridge and the designed gear ratio. Possible gearbox faults could be water seepage or poor lubrication. The final endpoints are typically open gearing components that make up the rack-and-pinion system used to rotate the bridge. Gearing systems require regular maintenance to ensure proper lubrication and cleaning in order to reduce wear. The drive system is powered by an *electric motor,* which produces the output torque to drive the system. *Motor brakes* are spring set and electrically released (M. Abrahams, 2000). The electric brake, consisting of linkage, brake shoes, spring, and actuator, is chosen carefully and mounted depending on the electric motor type. As an alternative to electric motors, hydraulic drive systems could be used, but have generally fallen out of style.

These components are often specially designed for an individual bridge application, often installed without consideration of ease of access for maintenance personnel. Because these components work together to drive the swing bridge, a failure or attack against one of these components would cause the rest of the system to fail, stopping the bridge and then stopping the involved traffic. For example, in 2010, the Whitby Swing Bridge in North Yorkshire, U.K. stopped operation for a week due to a gearbox failure (BBC, 2010).

The electric motor and electric brakes connect mechanical and electric components within the bridge system and could be exploited for either logical or physical attacks. The electrical drive control system in modern movable bridges is designed to handle all of the moving components to ensure proper bridge control. PLCs (49 CFR § 236, 2010) are connected to a control network that gives local and/or remote operators the ability to instruct the bridge to open or close. Each electric motor may have its dedicated drive controller that controls variables such as speed and torque to move the bridge. The sequencing involves instructing networked drive controllers used to manage the system's electric motor(s) and motor brake(s), controlling bridge lighting, and instructing interlocking system actuators. Local operators may open and close the bridge using

radios or a control panel in the operator's house, generally located in the middle of the swing bridge span.

Wayside and roadside cabinets may be interconnected to allow for manual override, actuate railroad switching components, remotely manage the traffic control system, or provide sensor interconnections. Network access may be remotely connected over a WAN to a back office controlled by the transportation authority, or the bridge may be considered in *dark territory* if there are no remote capabilities. It is also possible that the bridge is fully monitored and controlled remotely without a local operator. To communicate from wayside cabinets to the control system located in the operator's house, a specialized submarine cable connection may be run or wireless technologies such as microwave or radio signals may be used.

Interlocking Systems

Unlike bascule or lift bridges that are vertically lowered into place, swing bridges rotate into place on a vertical axis. The rotational movement requires a separate (stand-alone) interlocking system that aligns the swing span with the connecting spans to fully close the bridge. As a swing bridge is a multi-span structure, the bridge-specialized interlocking system serves three purposes: (1) to ensure that the opening bridge does not become unbalanced and remains stable, (2) to ensure that the closed bridge does not become unbalanced due to a live load, and (3) to center the bridge and ensure that it does not over-rotate. For the first two purposes, an *end lift system* is designed to relieve dynamic stresses caused when the bridge begins to move and withstand both static and dynamic stresses caused by passing traffic when the bridge is closed. As detailed by Protin and McGuire (2004), end lifts can be designed using a number of alternative methods such as end wedges, hydraulics, end wheels on an inclined plane, screw jacks, eccentric rotors, center jacks, and span locks. For the third purpose, *centering devices* are used to ensure that the bridge doesn't over-rotate on the horizontal plane. This component is generally designed to solve the problem in two ways: (1) the end lift drive shaft activates a lever which triggers a centering latch that locks the bridge as it reaches the closed position and holds it there; or (2) a centering device with its own motor and drive system forcibly aligns the bridge into a closed position after the bridge's drive system has moved the bridge to an almost-closed position.

Once the bridge is in the proper horizontal position, the railroad tracks must be closed to allow the train to pass. Among many methods to lock the track, (1) *miter rails* are the most common type and are lowered at the end of each side of the span via a joint when the bridge is locked into place, and are lifted before the bridge begins opening. Figure 5.2-2 shows the movable rails of a swing bridge. The ends of these rails are beveled so they overlap with the rails; and (2) *square cut rails* are machined so that the head fits against the head of the running rail. Both types are lowered at the end of each side of the span via a specific rail joint. The rails are only lowered into position once the bridge is locked into place, and they are raised before the bridge begins opening.

In 1996, Amtrak Train No. 12 derailed on the Portal Bridge near Secaucus, New Jersey, due to defective miter rails. The miter rails were not detected as defective by the control and monitor system: the signal system gave a false-positive indication, saying that the miter rails were in place, and hence gave a false-proceed indication to the rail traffic dispatching system, thereby allowing trains to move when the miter rails were still raised (NTSB, 1994). In 2014, the Walk Bridge in Norwalk, CT (ConnDOT, 2014) was closed due to an interlocking issue with its miter rails.

The interlocking system may have electrical requirements similar to the drive control system, depending on the bridge design. Without electrical control, it is not possible to fully eliminate the human operator due to the complexities of the interlocking system. Older swing bridges may have two separate drive systems, with the second used to operate the end lifts. Newer designs use separate actuation devices for each component, requiring more interconnections and synchronizing actuation.

Both the end lift systems and centering devices could utilize electric motors and motor brakes, requiring the use of the power system and separate drive controllers or actuators. In the case of end lift systems, these components may be found in wedge or eccentric rotor designs (Protin & McGuire, 2004). The centering device system may also have these components. Limit switches and actuators may be used to monitor and to seat miter rails.

Navigational Guidance System

Generally, the navigational guidance system consists of two functional components: (1) lighting, and (2) notification systems. These components are regulated in the U.S. in 33 CFR § 1, which provides more specific requirements regarding placement and functionality. For swing bridges, lighting is required under the bridge and along the rotating span. Red signal lights along the span signify that the bridge is closed, and green signal lights signify that the bridge is open to marine traffic. During the interconnection sequencing, this signal lighting is managed by the drive control system. If the bridge is high enough, FAA requires additional lighting for air traffic. A separate marine radio system may also be required to provide additional notification. Other notification systems in the interconnection sequencing could include a public address system or some audible notification (bells, whistles, or horns). Both lighting and notification systems have additional interconnection cabling and power requirements for proper functionality.

Electrical Power System

Modern movable bridges are controlled by solid-state electrical power systems using silicon controlled rectifier (SCR) technology made of power distribution panels, switches, circuit breakers, fuses, ground fault relays, over-current protection relays, cabling, etc. Specialized submarine cables run underwater to the center pier to power to the operator's house located on the swing span. The primary driving factor for the design of the power system is the power draw required by the electric motor when the bridge is rotating. Data points such as the weight of the span and peak wind speeds along the waterway also factor into this design decision.

Both AC and DC motors are used in modern bridges. Due to their complexity, power systems have the highest failure rates of any other system in a swing bridge (Bardsley, 2002). Consequently, AREMA recommends having an emergency auxiliary power source such as a generator.

5.2.3 Some Reported Failures of Movable Bridge Components

Hydraulic issues, such as bridge scour resulting from water scooping out the soil and sediment that supports the bridge pier, have been identified as the cause of 60 percent of complete bridge failures in the U.S. between 1950 and 1990 (Cook, 2013). To prevent impacts, a timber or crib fendering system can be installed to prevent ships from striking the center pier and rest piers or guide them away from the piers. Allisions, resulting from a marine vessel striking the pier's base,

were identified as the second greatest risk to the substructure and foundation of the bridge (Cook, 2013). The resulting impact could shift part or all of the superstructure and the internal systems. Heavy winds can impact swing bridges, as strong forces pushing against the horizontal swinging span in over-movement if the bridge's substructure is already stressed or weakened. Concrete stress results in cracks that could be further weakened by chloride from the sea water or spills. In recent years, the Gasparilla Island Swing Bridge in Charlotte County, Florida was replaced, as the original bridge's concrete girders from 1958 were structurally deteriorating, and there were high risks of failure due to storm surge and vehicular impact (Sinson, 2016). An interesting story from 2002 in troubleshooting the failed electrical system complexity of the Old Saybrook Bridge can be found in Paul X. O'Neil and Ostrovsky (2002) – this bascule bridge had components dating back to its original design and build in 1907.

Any networked components within the bridge's system could be logically or physically attacked by hackers, and should be carefully designed and included in the system with security in mind. Networking control protocols used to communicate with these systems, such as Modbus (MODICON, 1996), have historically been designed without security in mind. The research team concluded that this poses a significant risk to movable bridges in the modern interconnected world.

5.3 Justification of Use Case Selection for Remote-Controlled Movable Bridges

On September 22, 1993, an accident occurred at the Big Bayou Canot movable railroad bridge near Mobile, Alabama (NTSB, 1994). At 2:53 a.m., a barge being towed in dense fog struck the bridge, resulting in a displacement of the span and deformation of the rails. Eight minutes later, Amtrak Train No. 2, the Sunset Limited with 220 people on board, struck the displaced bridge and derailed. The crash resulted in killing 42 passengers and 5 crew members, and injuring 103 passengers. The National Transportation Safety Board (NTSB) noted that precautions could have been made to address the associated risks that led to the crash. NTSB specifically called out that the lack of a national risk assessment program to determine bridge vulnerability to a marine vessel collision led to the accident.

Considering that bridge faults are not a new problem, the authors note that Horace (1969) summarized and analyzed stationary and movable bridge faults in his thesis. He observed that most failures in structures today are not due to the design of the system itself, but *are a result of dishonest performance and noncompliance due to ignorance or a matter of economics rather than improper design*. The authors agree that fault and vulnerability analysis of any bridge is an ongoing process and a matter of due diligence long after a bridge was constructed, in order to prevent accidents or attacks. Cook (2013) mentioned that bridges are generally assessed for risk using several methods, such as reliability analysis and failure analysis using data from known collapses. He observed that the types of risk analysis used on bridges generally vary due to types of threats or the individual transportation departments. He also discussed that fault trees could be used as they have in the nuclear industry for decades. Cook conducted a quantitative analysis of bridge collapses using sample data from the U.S. and noted the average number of bridge collapses based on the sample population was 1/4,700 annually, with 4 percent of collapses resulting in loss of life. Cook did not discuss the possibility of logical attacks and cyber security risks. But this is the first attempt that the authors know where vulnerabilities were directly considered in addressing the overall risk of movable bridge systems, including cyber security induced risks.

Generally, to study faults or vulnerabilities of a given system, data is collected and analyzed for in-depth failure analysis. As a result, design corrections are made, and data is shared with the community to provide further knowledge about addressing and mitigating known hazardous conditions. However, to the best of the team's current knowledge, this data does not exist for movable bridges for two reasons: first, no two movable bridge systems are built the same and operated under the same environmental conditions; second, the scale of faults can vary in these systems, and resulting outages could be resolved quickly by operators to get the system back online without centrally collecting this data. To address these problems, the authors have been researching methods to model the impacts of failures and exploitability of vulnerability of modern movable rail bridges and decided to use dynamic fault-attack trees in this study.

As stated previously, modern movable bridges include computational logic that automates the movements for many years. This logic provides an additional layer of complexity to bridge systems as a layer on top of the mechatronic systems. Conducting cyber security risk assessments of these systems is similar to assessing other industrial control systems (ICS). PLCs are used to control the movements of the bridge in a structured and timely manner and also to identify faults. Zhu *et al.* (2011) provides a detailed taxonomy of SCADA attacks and the security properties of their mitigation strategies. Over the past decade, much research has been conducted on known and theoretical ICS attacks and mitigating approaches in a number of industries, including the water industry (Amin, 2013), energy grid (Robert Lee *et al.*, 2016), and chemical plants (Krotofil, 2015).

Given that electro-mechanical faults and potential cyber attacks can affect the risk profiles of movable rail bridges, the current section develops comprehensive methods to analyze the risk of movable railroad bridges that can quantitatively account for risks that are consequences of either natural or mal-intended exploitation of faults and cyber vulnerabilities.

5.4 Related Work for AFTeR Model

To describe the reliability modifications researchers incorporated into the attack-fault trees with reliability (AFTeR) model to be elaborated later, an overview on movable bridges, quantifying safety and security, safety and reliability, and the cyber kill chain is in order.

5.4.1 Quantifying Safety and Security

Historically, safety and security risk management in CPS has been treated as independent efforts, with individually customized standards incorporated into system design processes. Models have been developed for describing how these risks could impact a system, such as fault trees for safety (Ericson, 1999) and attack trees for security (Mauw, 2005; Schneier, 1999). Recent attempts to combine these models for qualitative analysis have taken several approaches, most notably using Boolean logic driven Markov processes (Bouissou, 2010) and petri nets (Ericson, 1999; W. Vesely *et al.*, 1981). McGeehan (2014), Kumar and Stoelinga (2017) discussed the shortcomings of these models and introduced attack-fault trees, which uses stochastic, timed automatons to provide both qualitative and quantitative risk analysis. The research team applied this model to a movable swing bridge system but identified problems in the model that limited its practical application for quantitative analysis, including the lack of system repairs and failure recovery (Y. Wang, 2019). The team incorporated reliability engineering techniques into AFTeR, which will address these problems to provide additional quantitative analyses.

5.4.2 Safety and Reliability

Reliability is the probability that a product will operate for a specified time (design life) under the design operating conditions (such as temperature, load, volt, etc.) without failure (Y. Wang, 2019). Attack-fault trees incorporated an exponential failure rate, λ, into the quantitative analysis of system faults. However, λ does not adequately represent component failure rates without further definition. AFTeR incorporates repairable and non-repairable components with maintenance cycles to further refine λ.

In reliability engineering, failure rates and downtime for repairable components are calculated using mean-time-between-failure (MTBF) and mean-time-to-repair (MTTR). These rates are calculated based on repair intervals between failures, and repair records resulting in the component returning to some usable state. Non-repairable components cannot be repaired, and their failure rates are calculated as the expected time between two successive failures using mean-time-to-fail (MTTF). These equations and their relationships to λ are refined in Y. Wang (2019) under varying scenarios. For electronic systems, MIL-HDBK-217F (Handbook, 1995) has been used by both commercial companies and the military for reliability prediction (Baklouti, 2017). The authors note that MTBF and MTTF are good probabilistic measures for planning and budgeting for component failures over time, but they are not as precise a measure as variables such as load; also, the operating environment and climate are not considered (Boyd, 1992). Although AFTeR leverages these probabilities, it is also limited by known weaknesses in modern reliability planning. AFTeR also accounts for maintenance cycles that can leave the system in an *as-good-as-new* state, resulting in a minimum set of repairable component faults. However, the authors note that simulations using UPPAAL SMC (David *et al.*, 2015b) resulted in exponential failure rates closely bound to MTBF for individual repairable components.

5.4.3 Cyber Kill Chain

Lee (2015) introduced the two-stage ICS cyber kill chain. The kill chain model was developed to define the steps required for a successful attack. In Stage 1, the attacker conducts cyber espionage to gain persistent access and intelligence on the system's functionality. In Stage 2, the attacker uses the gathered intelligence to develop and execute a targeted attack designed to control or disrupt the system. If the defender can disrupt the kill chain in progress, the attacker's goal may be stopped without being realized. Examples of these stages can be seen in recent cyber-physical malware campaigns conducted by advanced persistent threats (APTs), to include Stuxnet (Symantec, 2014), Havex (F-Secure, 2014), the Ukrainian power grid attack of 2015 (Robert Lee *et al.*, 2016), CRASHOVERRIDE (R. Lee *et al.*, 2017). This study incorporated these stages into the AFTeR analysis to quantify attack behaviors against a movable bridge.

5.5 Remote Controlled Movable Bridges ConOps and Technical Specification

A movable bridge is considered *opened* when the bridge is rotated parallel to the navigable water traffic direction, allowing water traffic to flow and prohibit over-land traffic; and considered *closed* when the bridge is aligned with overland railroad tracks and thereby preventing water traffic.

When an opened bridge needs to transition to a closed state, an operator signals a closing request to the bridge's control system. When closing, marine craft is alerted via radio, lighting, and/or alarms and given time to steer clear of the bridge. The control system will check sensors, such as

from rail or automotive traffic control, to avoid unsafe operations. Once all sensor checks are completed, the drive system mechanically walks the pinions around the curved rack, rotating the bridge into the closed position. End lifts are then secured, wedges are pushed into place (in the case of center bearing systems), the centering device is engaged, and the track is locked on both ends of the bridge (Koglin, 2003). The bridge is now closed, and the system uses lighting and signals train/automotive signal operator to permit overland traffic. After overland traffic passes over the bridge, this process is reversed to begin opening the bridge to the opened state. The research team modeled these functional use cases of a swing bridge as a Moore finite state machine with opened, closing, closed, opening states, as shown in Figure 5.5-1. The team introduced failure states within the states and during state transitions. In the diagram, f/a represents a fault or attack that results in a failed state. In the automation, the arrows with labels (f) or (a) refer to a fault or an attack that can take the bridge to a failure state.

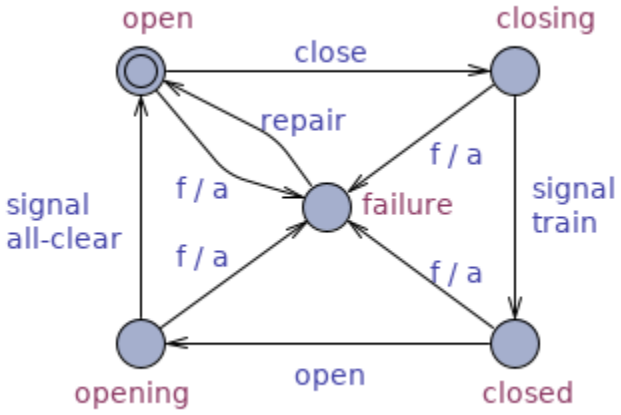


Figure 5.5-1 Finite State Modeling of Movable Railroad Bridge Operations

5.6 Systems Architecture and Specific RIoT Use Cases in Movable Bridges

This section describes the system architecture and the use cases in this case study of fault and attack analysis-based risk assessment of swing rail bridges. Although this case study depends on the specific architectural design of the chosen example plus equipment placed on that physical architecture, the methods used here can be applied to other movable bridges.

Researchers used a swing bridge with a movable center span that carries rail traffic and allows for seaway traffic when the bridge is open. Figure 5.2-2 shows that the center span being mounted on a wheel cage, which is rotated using an electric motor. Figure 5.6-1 shows a notional architecture of such a bridge with the center span consisting of an electric motor, a telematic speed controller that controls the motor movement, and a compact PLC that communicates wirelessly with three equipment cabinets/bungalows. The cabinets are located at both bank-side portions of the bridge, next to a riverside roadway, in order to control rail grade crossing traffic. As shown in Figure 5.2-2, human operators can request the bridge to be open using either DTMF hand-held radios with a private sequence or manual switches housed in a secure box. Figure 5.2-2 also shows the rails on the movable span that are lifted mechanically before swinging the bridge; and rails are *lowered* + *locked* prior to rail traffic being allowed on the bridge.

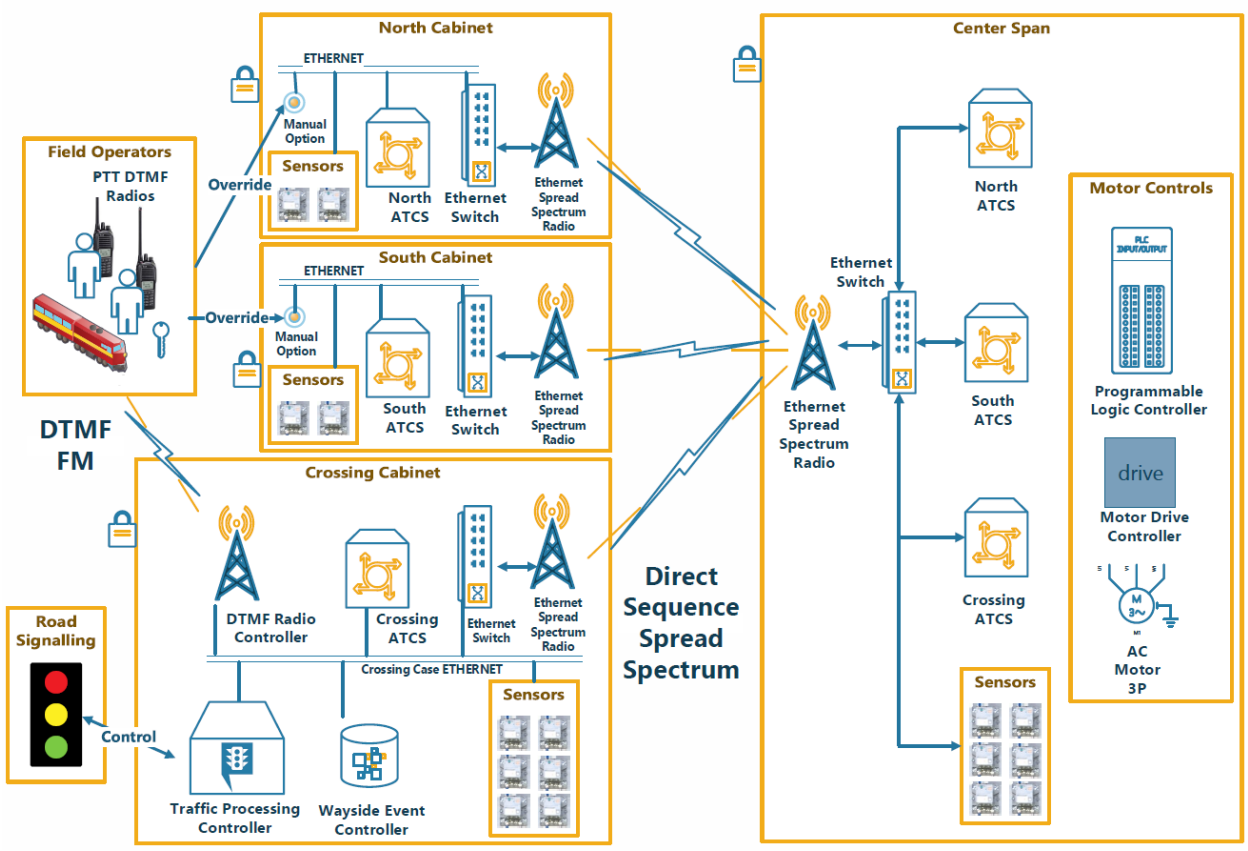


Figure 5.6-1 System Architecture of a Rail Swing Bridge

The two primary use cases of the movable rail bridge system (RIoT application) are opening and closing the bridge to seaway/railway traffic, which are mutually exclusive operations. Initiated by human operators, each is enabled by executing control operations using a series of subsystems. Figure 5.6-2, as a sequence diagram, shows the operations involved in bridge opening for seaway traffic, where the solid rectangular boxes stand for the entities participating in each task. The solid vertical bins under each entity are activation boxes that represent the time needed for each entity to accomplish its current task. The horizontal arrows show the control command messages and return responses as solid and broken lines, respectively. In this use case example, when the seaway is closed, a boater requests opening the bridge using a radio command to the signaling controller, shown as s_1 request bridge (to open) in Figure 5.6-2. Upon receipt, the signaling controller performs a sequence of subtasks. The signaling system signals any present trains to stop, confirms that rails are unoccupied, retracts any power catenary sledge (if available), sets derails to the derailing position, and de-energizes traction power before it informs the bridge controller to open the bridge, shown as signal s_7 *informBridgeToOpen()* in Figure 5.6-2. Upon receipt, the bridge controller energizes the bridge control panel, sounds an audible alarm to warn nearby entities, pulls out the centering device, pulls out wedges, releases all brakes for the motors, rotates the movable span until the bridge is parallel to the seaway, locks the moving span, and de-energizes the control panel. Finally, a signal indicating permission to pass across the bridge will be sent to the boats from the bridge controller. Closing of the bridge to rail traffic reverses the message order of the opening.

Use cases are implemented by having multiple subsystems (such as the signaling system, bridge operation controllers, DTMF radios and bridge rotation system) that work in synchrony using communication technologies. These subsystems may have individual internal subsystems with their own administrative commands, leading to a *system of systems* design. This study analyzed the state transitions of the subsystem that moves the bridge span (shown in the rightmost box of Figure 5.6-1) using hierarchical state charts (Elliot, 2013), as shown in Figure 5.6-3. Here, states are shown as rectangular boxes and their conditional transitions as curved arrows. Researchers modeled the administrative component of any subsystem as comprising of three subsystems of fault handling that checks, detects and handles system faults (shown as *fault handles)*, firmware updating (shown as *firmware updates)* that manages all the software improvements and testing interfaces (shown as *status checks)* that monitor the system on the left side of Figure 5.6-3. For example, checking motor speed may not be directly conducted by any human operator; the control system may periodically check the motor speed to generate the requisite horsepower to move the bridge span. But a knowledgeable attacker may exploit system vulnerabilities to take control of the motor speed, thereby causing safety and/or security issues. Upon completion of the previous steps, the bridge controller will send a command to span rotation controller to rotate the span using a command *rotateSpan()* in Figure 5.6-2 and Figure 5.6-3.

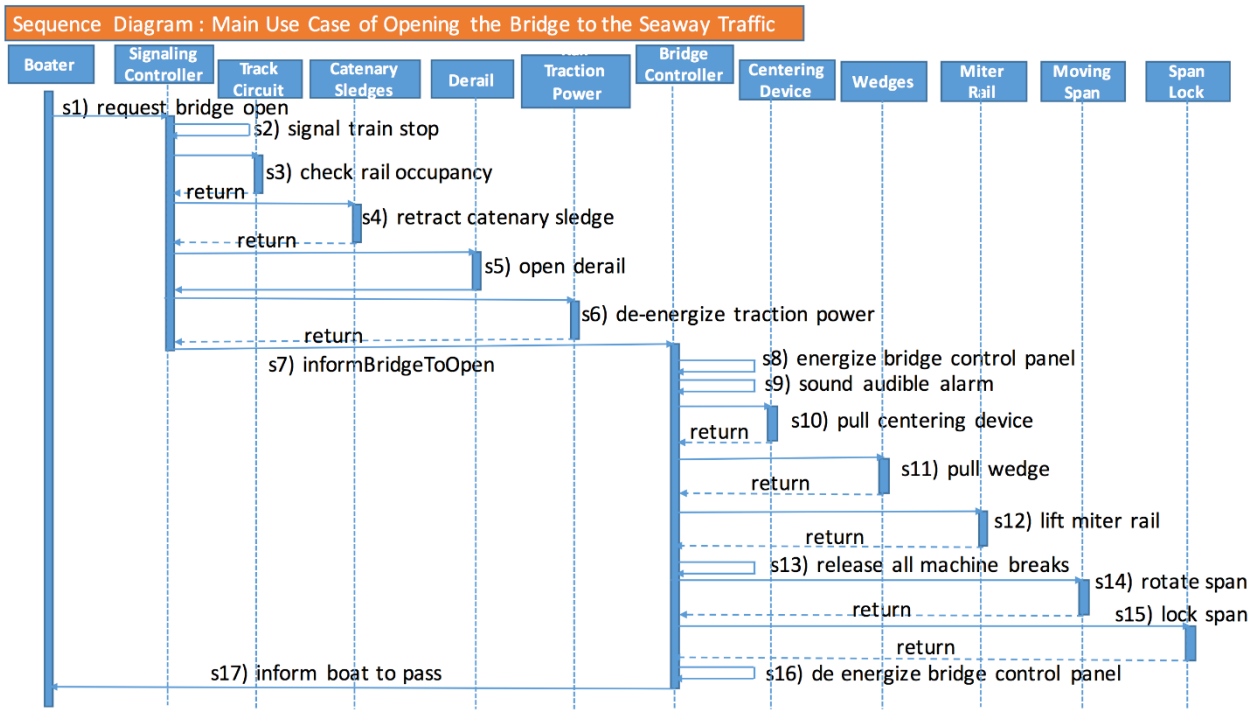


Figure 5.6-2 Sequence Diagram to Open a Closed Bridge to Seaway Traffic

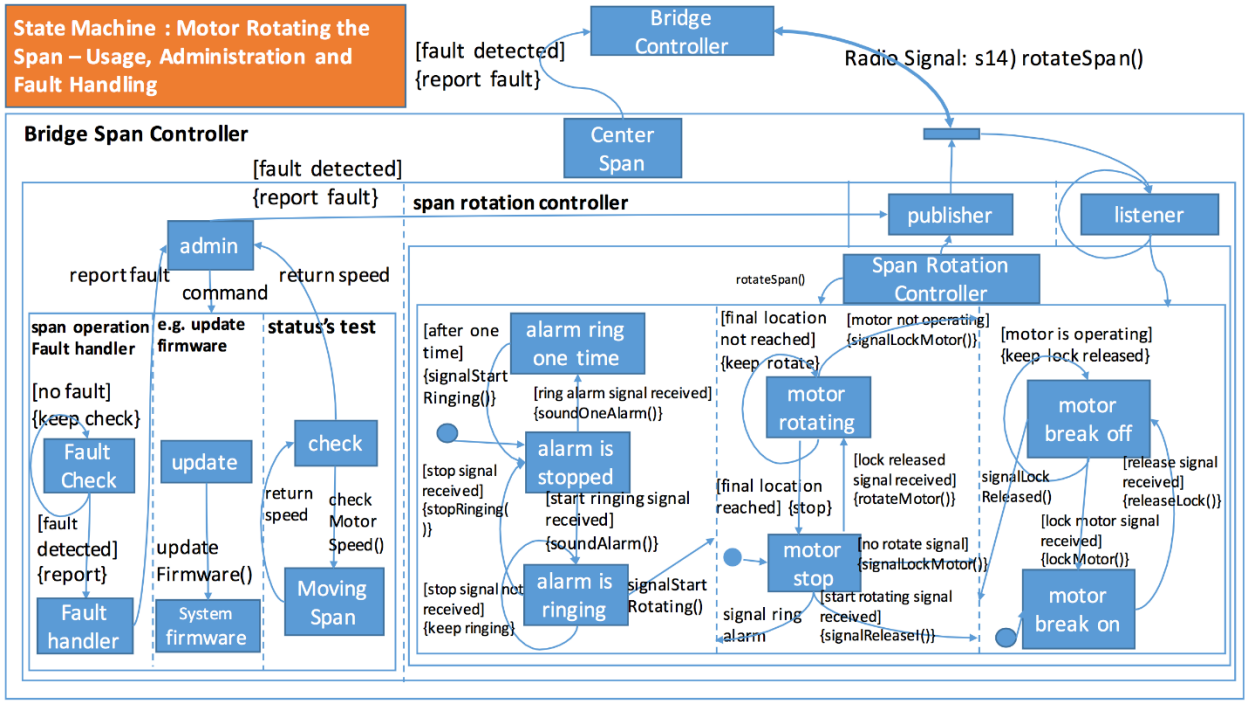


Figure 5.6-3 A Hierarchical State Machine Model of the Swing Bridge Control System

An important system in use is the motor and the motor-brake control subsystem, which is usually supplied by a vendor with its own embedded design. To model this subsystem, the research team assumed that the motor has a *motor rotating* and *motor stop* as its two main states; the motor brake has two states: *motor brake off* and *motor brake on*. The correct operational scenario for this subsystem is to have the motor brakes released when and only when the motor is rotating. When the motor stops rotating due to either completion of operation or loss of power, the motor brake must immediately kick in and finally lock the motor in order to prevent free movement of the span. The motor braking is often achieved by creating a resistance using either friction or magnetic force on the motor when the motor brake is de-energized. As shown in Figure 5.6-3, when starting, the motor is in the *motor stop* state and the motor brake is in the *span brake locked* state. Upon confirmation of the warning alarm, *signalStartRotating()* and *signalRelease()* are sent to the motor brake. The motor brake will move to the *motor brake released* state and the motor will move to the *motor rotating* state. When either condition *(final location is reached* or *motor is not operating)* is satisfied, the state transition model will move the motor brake to the *span brake locked* state and the motor to the *motor stop* state. By intended design, the two conditions are detected by location sensors and motor controllers.

5.7 Identification of Risks

With critical infrastructure, such as movable railroad bridges, proactive risk management through safety and security planning has similarities with military planning in combat. In both cases, the primary goal in planning is to ensure that the timeline remains *left of the boom* (a point of timeline reference to stay ahead of and avert attacks). In 2010, Stuxnet malware was discovered as an attack against network control systems, which was designed to cause physical destruction at the Natanz nuclear facility in Iran (Langner, 2013). As a result, the security community pivoted their research efforts into identifying proactive security measures to prevent

similar attacks against cyber-physical systems (CPS) and the IoT. Recent research has shown the viability of the threat from attacks against the sensors, actuators, and networked components that comprise these systems, resulting in recommendations for novel defensive measures that will help in staying *left of the boom* (F-Secure, 2014; R. Lee *et al.*, 2017; Symantec, 2014).

To this end, risk management should be a part of the lifecycle of any critical system. In movable railroad bridges, federal regulations are designed to impart safety controls. These regulations include managing the safe operation of bridge systems (Coast Guard, Department of Homeland Security, 33 CFR § 1, 1986; Movable Bridge Locking Inspection, 33 CFR § 236.387, 1984; Movable Bridge, Interlocking of Signal Appliances with Bridge Devices, 49 CFR § 236.312, 1984), ensuring that signals are in place to properly communicate to vehicles when it is safe to proceed (M. Jablonski, 2019), and requiring regular annual inspections (M. Abrahams, 2000). Regular maintenance and repairs are conducted to ensure that the mechanical and electrical components are not left degraded. On the security side, proper management of risk is left up to individual authorities that maintain these bridges. General recommendations involve assuring the system's confidentiality, integrity, and availability. More specific recommendations to achieve these goals in CPS and RIoT should include securing the network infrastructure and perimeter, ensuring that regular security patches are deployed to networked systems, maintaining physical and network intrusion detection systems, and regular security assessments.

As a part of risk management, an additional question that should be considered is what happens *right of the boom*, namely the consequences post-attack. In movable bridges, failures in either safety or security can result in such a hazardous event. When modeling threats against a CPS, safety failures are classified as *faults* while security failures are considered *attacks*. The difference between faults and attacks and their impacts usually is a matter of intent or motivation. An attacker intends to cause a failure through some physical or cyber ways, while faults can be attributed to accidents, unintended actions, or improper maintenance (M. Jablonski, 2019). In general, the first reactions to a hazardous event are to ensure that the system does not remain in a failed state and that both lives and property are properly secured and protected. The next steps involve identifying the root cause of the incident to ensure that lessons can be learned and, if an attack did occur, the attacker can be made accountable for their actions. Ideally, this root cause analysis can identify if an attack is the cause of the incident. Further attack analysis would involve attribution to the specific actor.

5.8 Risk Consequence Analysis

This study classifies failure events of a fail-safe movable bridge system as faults or possible cyber attacks. In order to analyze the consequences of a cyber attack, researchers conducted three levels of analysis:

1. Traditional fault trees (that have been used to assess safety risk by the rail industry extensively) and attack trees (used by the cyber security community extensively to analyze potential attack scenarios on networked IT systems)
2. Risk analysis of using a modern mode analysis of AFTs for movable swing bridges. The advantage of this analysis is that it allows one to model potential cyber-physical attacks that exploit known faults to create attacks or parts thereof and cyber attacks to generate faults. These attacks would either bring a fail-safe system to a fault-stop as protection, or

make the system invoke built-in fault handling methodologies that would continue in a degraded level of service.

3. The team observed several inadequacies of an AFT-based risk analysis to model fine-grain risks in movable rail bridge systems against capable cyber-physical attackers who can exploit faults and cyber vulnerabilities as stated in (2) above. In the meantime, the team also quantified the required attacker capabilities and efforts to launch such attacks.

5.8.1 Fault Trees

Fault tree analysis was first developed to study the Minuteman launch control system by H. A. Watson of Bell Laboratories in connection with a U.S. Air Force contract in 1962 (Ericson, 1999). Since then, extensive studies have been conducted with such analysis methodology in safety-critical systems, including railroad-related systems (Zhang *et al.*, 2018) in train derailment analysis, high-speed rail safety, and restricted-speed accidents (Liu *et al.*, 2015; Wang *et al.*, 2014; Zhang *et al.*, 2018).

Fault tree analysis is a top-down, deductive failure analysis in which a top event is analyzed using Boolean logic to combine a series of basic events that model all possible failure paths. As a graphic model, a fault tree displays various combinations of events, such as equipment failures, human errors, environmental factors, etc. (Zhang *et al.*, 2018)

5.8.2 Dynamic Fault Trees

In 1992, Boyd (1992) introduced dynamic fault trees (DFT), which extends standard (or static) fault trees by modeling the behaviors and interactions of complex system components (Boudali *et al.*, 2007). DFT is comprised of various elements: basic events, static gates (AND, OR, and K/M gates), and dynamic gates (functional dependency, priority AND, and spare gates). Each of these elements is viewed as a process moving from one state to another. States denote either the operation or a failure of an element. Each element, or process, also interacts (communicates) with its environmental context by responding to certain input signals and producing output signals. These elements could also possess a purely stochastic behavior by allowing (in a probabilistic fashion) the passage of time prior to moving to another state. As a top-down failure analysis, DFT analyzes the top undesired event using logic gates to connect basic events through failure paths (Zhang *et al.*, 2018).

To quantify the safety and reduce the risk of a movable rail bridge operational system, researchers used a DFT (Baklouti, 2017) approach to explore the causal chains of failures. DFTs model all potential failure paths leading to an undesired state configuration of state machines. An example of an undesired state from the prior section would be: if the motor brake is released while the motor is stopped despite a presence of strong winds. Such an example could then lead to uncontrolled movement of the bridge span, being unable to support any rail traffic safely across a waterway.

The research team, to the best of its knowledge, was the first to apply DFT analysis to rail bridge safety. DFTCalc (Arnold *et al.*, 2013), among the free and open-source fault tree analysis tools, showed its superiority over others in its usability to model and analyze dynamic fault trees (Baklouti, 2017).

5.8.3 Attack Trees

One historic problem with attack trees is that the complexity of the time required for their generation has the potential to grow with the size of the system being studied. Ammann *et al.* (2002) noticed this problem, and introduced the concept of monotonicity in attack graph generation. Monotonicity eliminates redundant paths in attack graphs through observing that an attacker's exploit is never invalidated by the successful application of another exploit. In 2006, Ou *et al.* (2006) built on Ammann's approach through their concept of logical attack graphs. They observed that all logical attacks have rooted causes in configuration information, and all attack preconditions can be represented as propositional formulas taking the configuration as input. To demonstrate the benefit of their approach, they developed multi-host, multi-stage vulnerability analysis language (MulVAL), which can generate the logical attack graph for a system in quadratic time relative to the size of the system (Ou, 2013). We leveraged MulVAL to conduct the analysis on our reference movable bridge system.

For logical vulnerability analysis, different attack tree approaches have been applied to a wide variety of systems and complex applications, including SCADA systems (Ten *et al.*, 2007), privacy in vehicular ad-hoc networks (Ren *et al.*, 2011), and ambulatory medical devices (Luckett *et al.*, 2017) etc. As examples, Ten *et al.* (2007) used attack trees as a method to derive quantitative vulnerability measures in SCADA systems, Ren *et al.* (2011) used attack trees to identify threats against privacy in vehicular ad-hoc networks, and Luckett *et al.* (2017) demonstrated their applicability toward ambulatory medical devices.

5.8.4 Attack-Fault Trees

Kumar and Stoelinga (2017) introduced attack-fault trees that provide a quantitative and qualitative analysis combining both safety and security vulnerabilities within a single model. AFTs model how a top-level (safety or security) goal can be refined into smaller sub-goals, until no further refinement is possible. In that case, one arrives at the leaves of the tree that model either the basic component failures (BCF), the basic attack steps (BAS) or on demand instant failures (IFAIL). Since subtrees can be shared, AFTs are directed acyclic graphs, rather than tree-leaf behavior from attack trees and dynamic fault trees described above. As such, they can very well capture the multistage, the dynamic temporal, and causal safety and security interdependencies. All BCFs are governed by exponential probability distributions. For example, the probability of a disruption occurring before time t is given as: $P(t) = 1 - e^{-\lambda t}$, where λ is the rate of exponential distribution. Further, BCFs are enriched with cost structures such as damage. BAS represents the active steps taken by an attacker to compromise the system. They are equipped with an exponential distribution representing the attack duration, discrete probabilities quantifying the attack success irrespective of the execution time, and a rich cost structure, the latter of which includes the cost incurred by an attacker and the damage inflicted on the organization. Though researchers used exponential distributions, their methodology can handle other complex distributions, such as phase-type distributions. By doing so, multiple quantitative annotations on the AFTs like cost, time, failure probabilities, and damage, which can functionally be dependent on each other, can be modeled by AFTs.

5.9 Fault Trees and Attack Trees for Movable Rail Bridges

This section shows the fault tree and attack tree models of a movable bridge control system that is shown in Figure 5.9-1.

5.9.1 Dynamic Fault Tree Modeling and Attack Tree Modeling

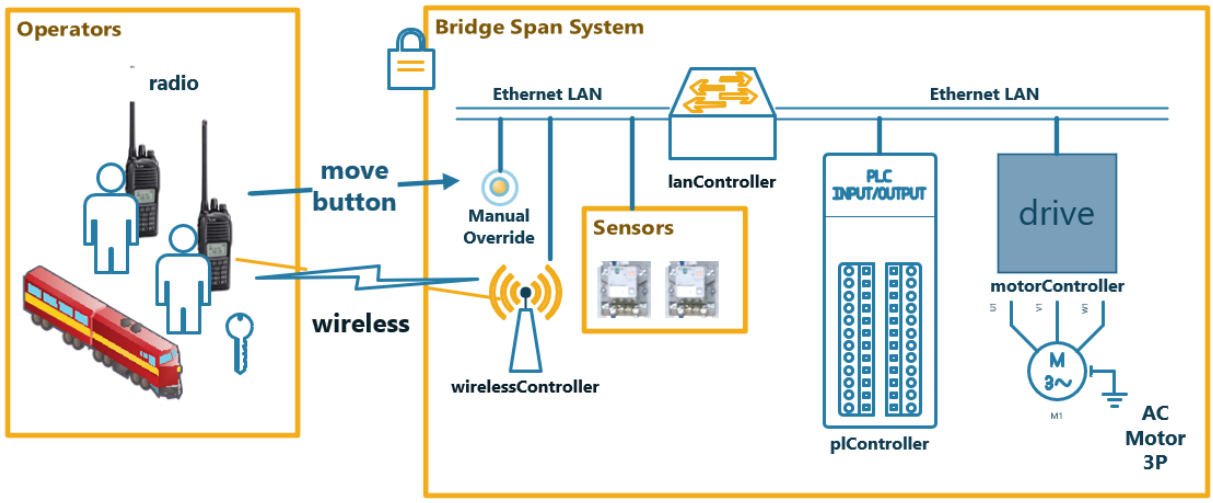


Figure 5.9-1 High-Level System Structure of a Rail Swing Bridge

The reference diagram includes two networks – *wireless* and *LAN*, managed respectively by a *wirelessController* and a *lanController*. In this system, operators may issue *move* commands to the bridge over the wireless channel using handheld radios, or they may use a button on a panel physically controlled within the bridge control cabinet. The LAN is used as a wired network to pass network traffic between the control systems, sensors, and controllers. The *plController* is a PLC used to manage the movable components in the bridge with a high degree of control and is used to diagnose faults. The *motorController* is the drive controller used to control the speed, torque, and direction of the bridge's electric motor. The *plController* and the *motorController* issue and receive commands using the MODICON Modbus protocol (Modbus running on TCP port 502), and are configured in a master/slave relationship. Modbus is a standard control protocol used in industrial control systems, such as a moving bridge (MODICON, 1996). Commands to *move* or control the bridge components are passed to the *plController* over the LAN using Modbus. When needed, the *plController* will issue Modbus commands to the *motorController* to *move* the bridge by driving the electric motor.

Figure 5.9-2 shows the DFT of a bridge span controller. The top undesired state *Failure of Bridge Span System* can be caused by either *Motor Failure*, *Motor Brake Failure*, *Failure of Motion Systems,* or *Link Failure,* and are modeled as an OR gate. For the FDEP gate of Figure 5.9-2, the output occurs only when the trigger event of *Motor Failure* occurs, and the dependent event *Gear Failure* has to happen simultaneously. The *Link Failure* event has two child nodes connected using an OR gate, one of which is a PAND gate (Priority AND). PAND gate's output occurs only if the inputs occur in sequence the from left to right. That is when the *Transmitter Failure* precedes a *Receiver Failure*. The other component of the has a *Spare gate* as the head, whose output occurs if all its inputs occur. This models the situation when the main receiver and spare receiver are present. Both of them need to break down for the receiving module to fail. The DFT of the rail lifting controller is mostly identical to the discussed one, except missing a *Wheel Failure* node.

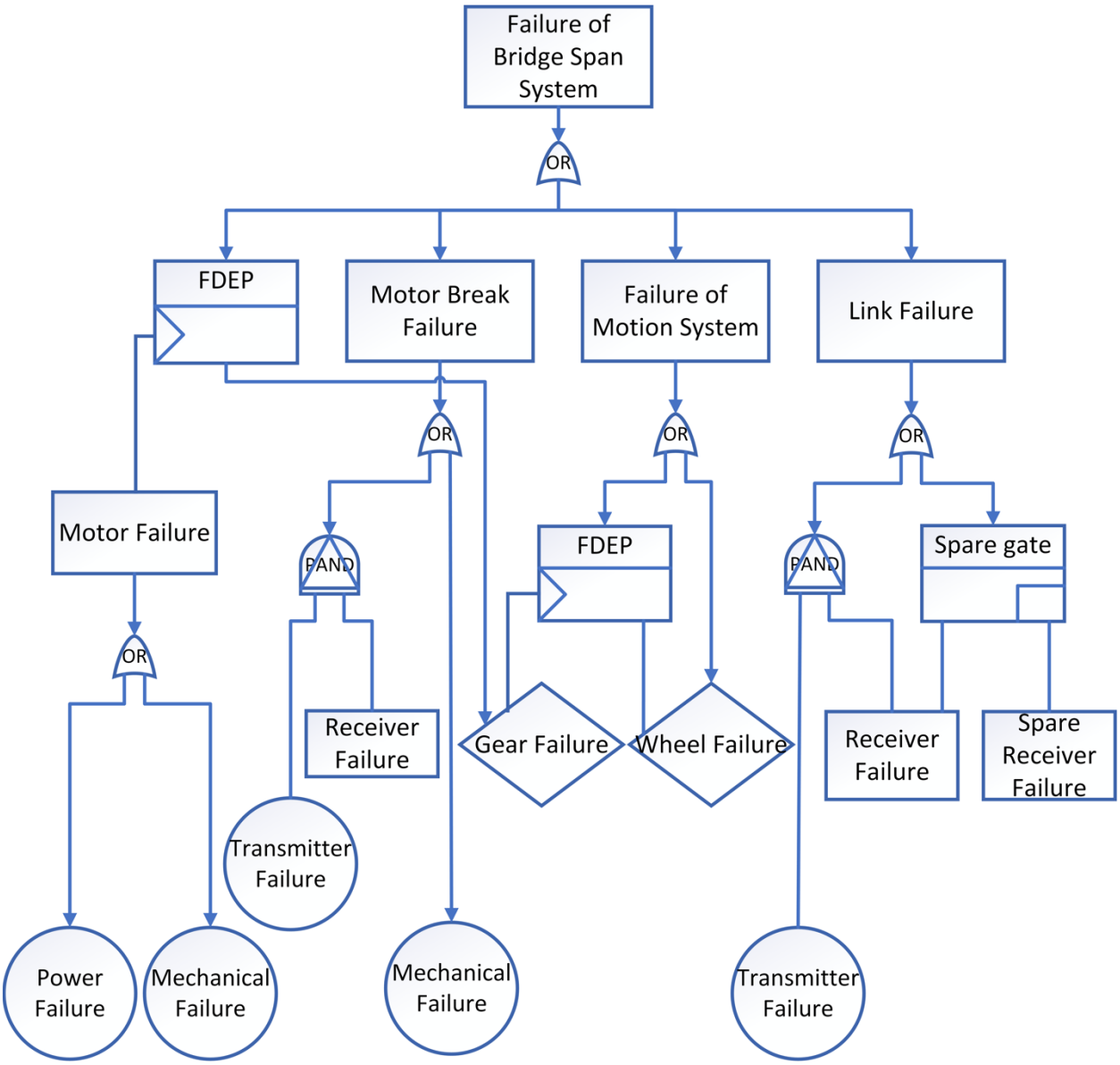


Figure 5.9-2 A Dynamic Attack-Tree for the Motor Controller

After the system is defined, the system configuration details are used as inputs to an attack tree modeler. The referential attack tree in Figure 5.9-3 was generated using MulVAL, an attack tree modeler that takes configuration information and vulnerability details from network scans and shows paths by which an attacker could take to achieve defined goals (Ou, 2013; Ou *et al.*, 2006). The resulting tree consists of host access control lists (*hACLs),* interaction rules *(Rules)*, and *Attacker's Goals*. All network accesses between hosts are *hACLs*. Rules are defined to show when an exploit can occur, how system compromises could propagate, or how an attacker could take advantage of multi-hop network access scenario. If one considers a *Rule* as literal L_0, and input *hACLs* and *Goals* as literals L_1, …, Ln, MulVAL generates the rules in the attack tree using a Horn clause: $(L0: -L1, \ldots, Ln)$. This means if all input *hACLs* or *Goals* are true, then the rule is also true and the path is included in the tree (*Rules* are equivalent to AND-nodes). *Goals* represent a privilege or access that the attacker wishes to obtain. In order to achieve the *Goal,*

any input *Rule* could be exploited by an attacker (*Goals* are equivalent to OR-nodes) (Ou *et al.*, 2006). Each *hACL* (rectangle), *Rule* (oval), and *Goal* (diamond) is numbered accordingly in Figure 5.9-3 for further reference.

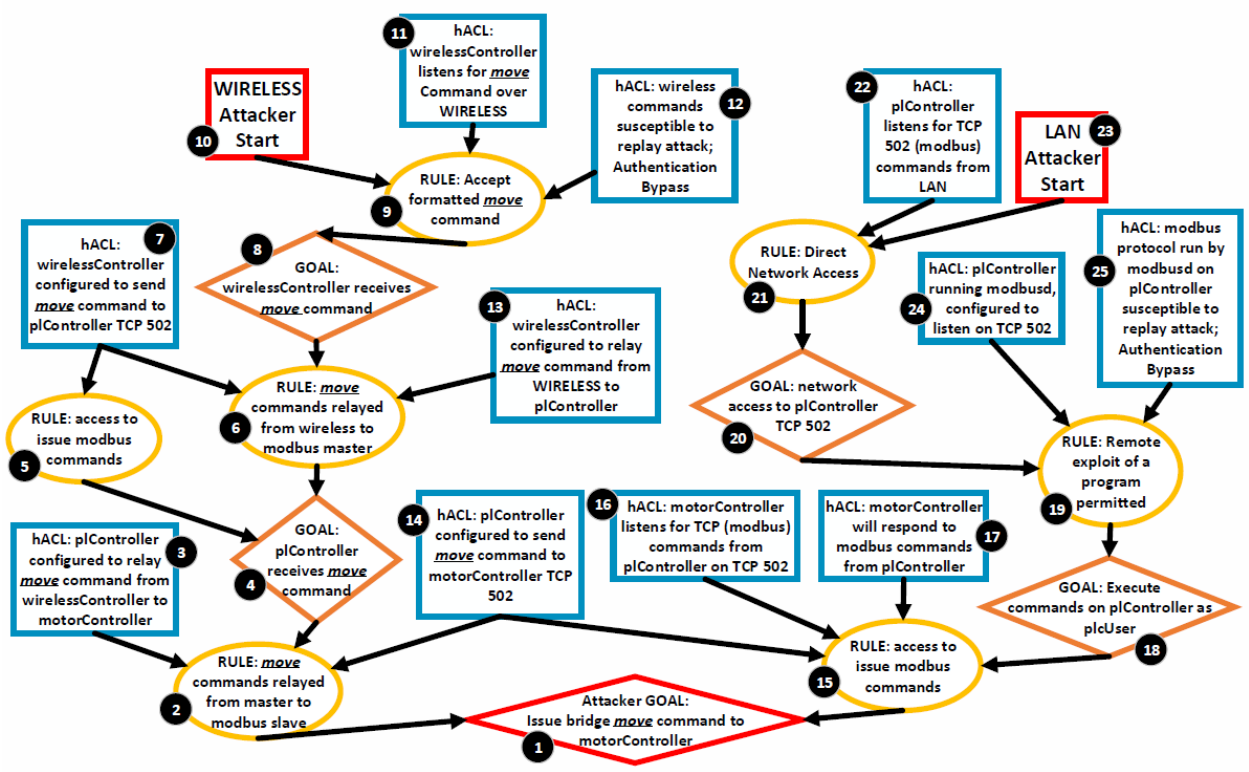


Figure 5.9-3 An Attack Tree for the Motor Controller

The primary attacker goal is found in 1 – logically issuing *move* commands to the *motorController*. Issuing commands to the controller could result in the following scenarios:

- Deception attacks through unauthorized movement of the bridge's position
- DoS attacks preventing use of the bridge for highway, rail, or water traffic

Once the attack tree is generated from the system configuration and goals, it is possible to generate paths from the graph to describe how an attacker can achieve those goals. Two paths are provided in this study: a wireless attack path, and a LAN attack path.

A Wireless Attack Path: The attacker starts with a wireless receiver/transmitter in (10), but no physical access to the system. The *wirelessController* is configured to listen for *move* commands issued from operator radios (11). The attacker determines that the control signal is analog without additional security and captures and later replays this transmission to issue the same *move* command to the *wirelessController* (12). An explanation of replay attacks and a taxonomy of other wireless attacks can be found in the work of Knight and Newlin (2017). If the transmission is captured and transmitted at an appropriate power, it is accepted by the *wirelessController* achieving the GOAL (8). The *wirelessController* is configured on the LAN to relay wireless movement commands (13) to the *plController* listening on TCP port 502 (7), following RULE (6). This results in achieving GOAL (4). Similarly, the *plController* is configured on the LAN to relay movement commands received over the Modbus protocol to the

motorController, per (3). The *plController* and *motorController* are in a Modbus master/slave configuration, so the *plController* can send *move* commands to the *motorController* (14). This follows RULE (2), achieving the overall goal (1).

A LAN Attack Path: The attacker starts with LAN network access in (23), which could be achieved via physical access to a network port or possibly through a remote code execution exploit against a vulnerable LAN system from the WAN (ignored in Figure 5.9-1). Scanning the network from the LAN allows the attacker to identify Modbus running on the *plController* on TCP port 502, per (22). The attacker has direct network access (21) to issue commands, satisfying GOAL (20). Using a passive listening methods on the LAN such as ARP spoofing (Liu *et al.*, 2015), an attacker can act as a man-in-the-middle to exploit a capture-replay vulnerability against the *plController*'s Modbus implementation (25). Modbus generally is not configured with confidentiality or integrity within an industrial control system; note that a partial formal security analysis of the Modbus protocol can be found in the work of Nardone *et al.* (2016). This exploit would allow the attacker to listen and replay/inject Modbus commands to the *plController* listening on TCP 502 (24), providing a remote exploit for Modbus (Arnold *et al.*, 2013) and satisfying GOAL (18). The *plController* and the *motorController* are in a Modbus master/slave configuration, where the *plController* can send *move* commands to the *motorController* (14). The *motorController* is configured to listen for Modbus on TCP 502 from the *plController* (16) and will provide status feedback to the *plController* (17). By understanding this configuration, the attacker can then replay some movement commands to the Modbus master *plController* which will issue a *move* command to the slave *motorController* (15), achieving the overall goal (1).

5.9.2 Attack-Fault Modeling

Definition of Failure for Attack-Fault Trees

A movable swing bridge is classified as a *binary dynamic and repairable system* as defined in the work of Chaux *et al.* (2013). It is considered *binary* because its failure is modeled as Boolean variables; *dynamic* because the order of the component failures impacts the system failures; *repairable* as faulty, degraded, or failed components can be replaced. By this classification, the swing bridge *failure* state can be defined as, *"a stopped and dysfunctional state of the swing bridge for some time period until a repair has occurred and normal functionality resumes."* If the bridge fails in either *opened* or *closed* states, it will prevent passage of overland or waterways traffic.

Referring to Figure 5.5-1, the *failure* state limits the use of the railroad operation and/or the waterway. Meaning, if the bridge failed while in the *opened* state, the bridge cannot close and lock the rails to allow a train to pass. If it fails in the *closed* state, watercrafts taller than the vertical clearance of the bridge would not be able to pass; it is possible that trains may still be allowed through the *closed* bridge.

If the bridge fails while moving, both transportation channels may be stopped. Resulting outages from such failures could last from a few hours to years, depending on factors such as the size of the failure, the size of the traffic impact, loss of revenue to concerned parties, and the cost of repairs. Failures can result in further destruction of property, injuries, or loss of life if the system is not assessed properly or issues are not communicated in a timely manner. A full bridge collapse is possible, but historical evidence suggests that it is very rare.

A Traditional Attack-Fault Tree

Both system faults and attacks can result in failure states. To show both types of failure in a single model, the swing bridge AFT is shown in Figure 5.9-5.

Obviously, with the specifics of a particular bridge application, a more precise model can be derived. The following section describes the functionality of a swing bridge at the subsystem level, and incorporates an analysis of the model's data and any assumptions made into the discussion of these components.

As a top-down failure analysis, AFT is a directed acyclic graph (DAG) that analyzes the top-level safety or security goal, and refines it into smaller sub-goals. In the case of this study's model, the top-level goal G_0 is labeled *prevent bridge movement,* relating back to the definition of failure. An AFT is composed of gates and leaves. The AND, OR, Functional Dependency (FDEP), Sequential AND (SAND), and SPARE gates used in the team's model are standard and dynamic fault tree gates, and their definitions and automatons are defined by Kumar and Stoelinga (2017). Figure 5.9-4 shows these gates graphically, in addition to the team's own extension described shortly. Leaves of the AFT are either basic component failures (BCF) or basic attack steps (BAS), representing faults and attacks.

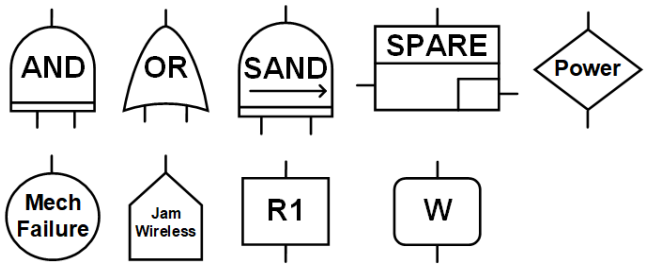


Figure 5.9-4 Illustration of Gates

Note: (left-right, by row): AND, OR, FDEP, SAND, SPARE, Intermediary, BCF, BAS, REPAIR, and NONREPAIR

Assumptions and Attack Paths in the Attack-Fault Tree Modeling

Researchers made the following assumptions about a generic swing bridge:

PLCs are used; both wireless networks and manual overrides are used for interconnections and operator control respectively; an AC-powered single electric motor and motor brake are used; a simple mechanical miter rail system that does not require separate electronic controls is used; it uses modern power systems.

Researchers identified five specific paths which faults and/or attacks could take to result in G_0:

G_2 – communication failures resulting in the inability of local or remote operators to move the bridge; **G_{32} –** the electric motor brake sticks preventing movement; **G_{68} –** the support system fails and prevents the motion system from functioning; **G_{54} –** the bridge substructure fails and results in a major bridge outage; **OR G_{64} –** the pivot pier, or superstructure, fails, also resulting in an outage. The following section defines the system and the faults and failures that make up the rest of the AFT.

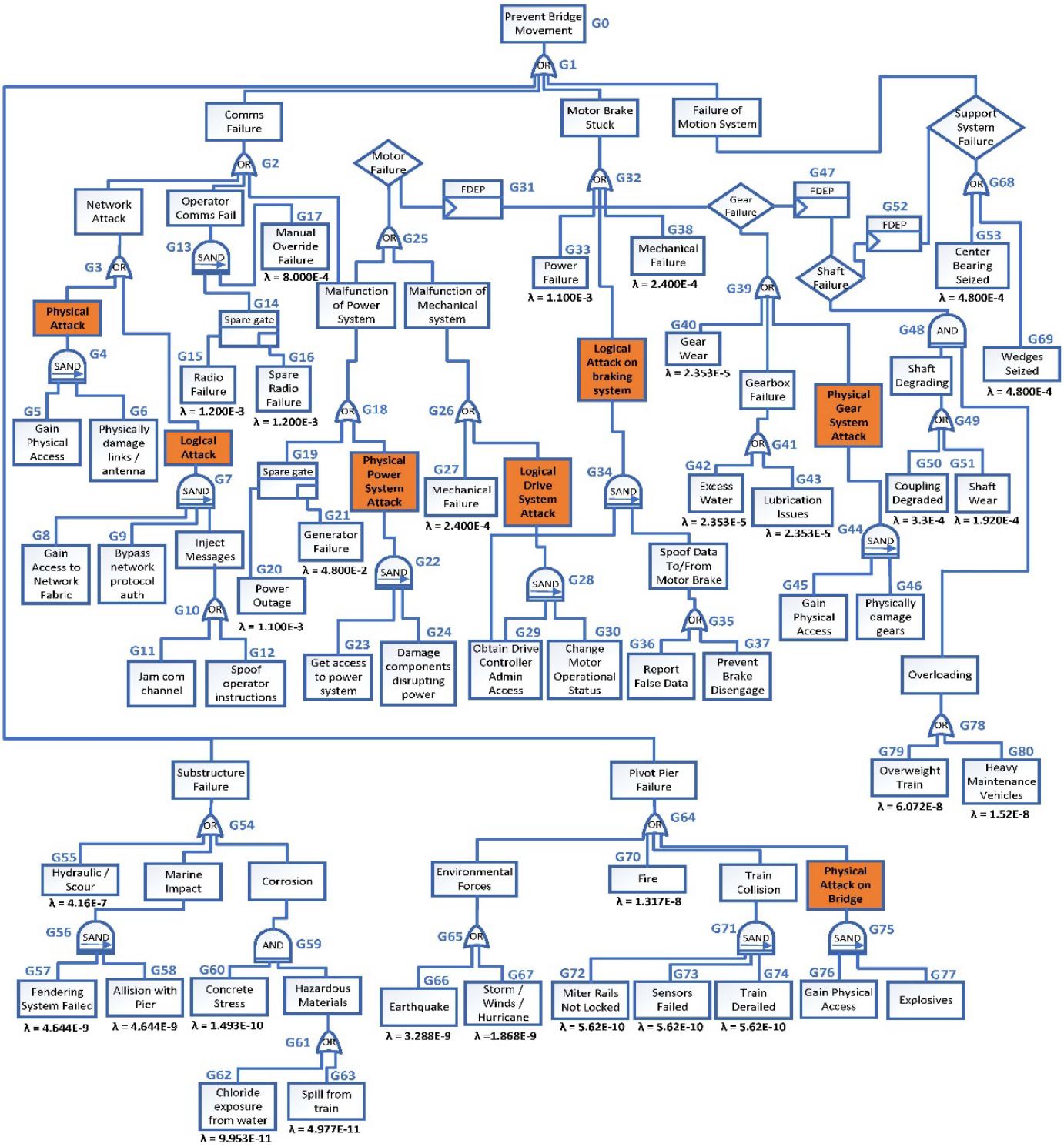


Figure 5.9-5 An Attack-Fault Tree Model of the Example Movable Bridge

Quantitative Evaluation of Cyber Risk using Attack-Fault Trees

For a quantitative analysis of this study's AFT, the research team used the stochastic model checking software UPPAAL SMC (64-bit v4.1.19, described by David *et al.* (2015a)) to turn the leaves of the AFT into automatons that simulate failures. This section describes the automatons and parameters that make up the BCFs and BASs used for the simulation in the next section.

Exponential probability distributions with mean λ to model failure rates are used where the probability of failure at time t modeled is $P(t)=1-e^{\lambda}$ P. The research team included the BCF λ-values (also written here as λ) with the AFT in Figure 5.9-5. To model the failure, a stochastic automaton was used to simulate the BCF as shown in Figure 5.9-6. In the automaton, λ was used as the exponential failure rate of failing nodes, and after that period of time, damage d occurs to the system, transitioning to a failed state and passing a message to a higher AFT gate declaring that the component failed. Each fault leaf in Figure 5.9-5 has its own automaton built as a part of the overall system, and the gates are stepped through during the UPPAL simulation. Table 5-1 lists the source of each λ- value included in the BCF that are converted to daily failure rates as shown in Figure 5.9-5, so that all faults and attacks in the simulation had consistent time values.

The resulting dynamic fault tree described in Section 5.9 is included in Figure 5.9-2. This focused on mechanical and electrical component failures, and then is used as the basis for our ATF. However, the ATF needs additional details regarding the system components that could fail to improve the quality of the stochastic model. The rest of this section augments the existing work with these details.

Figure 5.9-6 Stochastic Fault Leaf Automations of the Dynamic Fault-Attack Tree

Table 5-1 BCF Sources and Calculation Notes

BCF Leaf	Source	Notes
[G_{15}], [G_{16}], [G_{17}]	No Data	Assume 20,000 hours
[G_{20}]	(*13*)	
[G_{21}]	(*15*)	
[G_{27}], [G_{33}], [G_{38}]	(*6*)	AC Motor - Assume 10 failures per million hours @ 15-year renewal interval
[G_{40}], [G_{42}], [G_{43}]	(*4*)	Assume 40,000 hours based on L10 life at rated torque
[G_{50}]	(*6*)	Assume 8 failures per million hours at 15 year renewal interval
[G_{51}]	(*6*)	Assume 14 failures per million hours at 15 year renewal interval
[G_{53}]	(*6*)	Assume 20 failures per million hours @ 15-year renewal intervals
[G_{55}], [G_{57}], [G_{58}], [G_{66}], [G_{67}], [G_{70}], [G_{72}], [G_{73}], [G_{74}], [G_{79}], [G_{80}]	(*8*)	Taken directly or derived from included failure rates and divided by 365 to obtain per-day values
[G_{60}], [G_{62}], [G_{63}]	(*10*)	Derived from Concrete Stress and Corrosion - 1.09e-07 per annum
[G_{69}]	No Data	Assume 20 per million hours

The stochastic timed automaton used to model BAS leaves includes basic attack steps of an attack chain. Starting at the left *Initial* node in Figure 5.9-7, when the attack is activated, the attacker waits until s when he can afford to expend a cost value of f to proceed. Next, as the attacker proceeds, the attack is *potentially_undetected* with the probability of $w_1/(w_1 + w_2)$, or *potentially_detected* with the probability of $w_2/(w_1 + w_2)$. If being detected, the attack *Stops*, or is either *ongoing* or *activated* otherwise. If it is *ongoing*, the attack is detected while in progress with an exponential probability rate of λ at a cost of v per day to the attacker, and then the attack stops. If *activated*, the attack takes a time calculated by exponential probability rate λ at a cost of v per day to the attacker. Once *Executed*, the attack succeeds with probability $p/(p + q)$, causing damage d to the bridge operator/owner, or the attack fails with probability $q/(p + q)$. This probability is determined by the skills of the attacker, as outlined in the attacker profiles. The benefit of this approach is that one can determine a ratio of cost to the attacker against damage done to the bridge owner. A description of the attack paths and the configuration of leaf variables in our AFT is found in Table 5-2. The detection rates w_1 and w_2 in this table are configured at the *high* setting for reference in the discussion of the *WHAT-IF* scenario. In this configuration, assumption is made that the detection will occur at a higher rate while an attacker is trying to gain access but at a lesser rate post-exploitation. Attack labels (A_1, …, A_9) and the categorization of *logical* and *physical* attacks are relevant to attack profiles of this research. Dollar amounts for budgets, costs, and damage should be multiplied by 1,000.

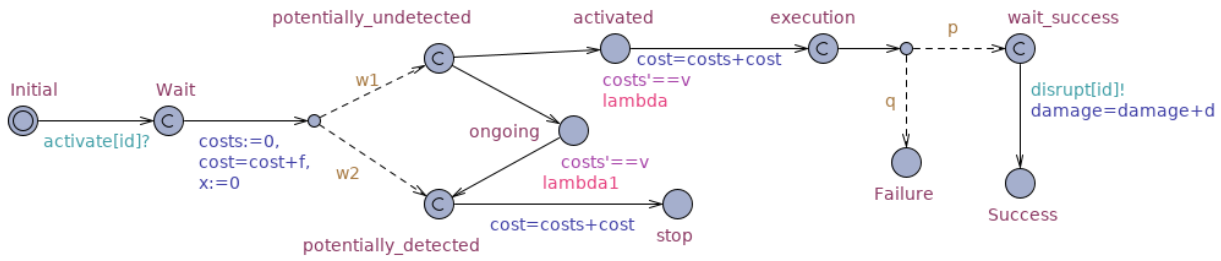


Figure 5.9-7 Stochastic Timed Automatons for BAS Leaves

Experimental Runs to Determine Risk

Then the researchers run attack simulations in UPPAAL using AS-IS and WHAT-IF scenarios. In the AS-IS case, detection capabilities are removed to establish a baseline for a successful attack based on attacker profiles. Then team researchers rerun the scenario using WHAT-IF settings that modifies the w_1 and w_2 detection rates so that they are on their *high* setting. This allows us to determine the effectiveness of detection mechanisms to prevent attacks.

A series of simulations were conducted to quantify the impact of faults and attacks on swing bridge operations. For each test, UPPAAL steps through a number of runs until the results become statistically significant (or insignificant) enough to provide feedback on the results. All runs were stopped and considered a *hit* if the goal G_0 was reached within the time frame noted in this analysis. If time expired without reaching G_0, the run was considered a *miss*.

Table 5-2 Configuration of BAS Leaf Variables

Attack Description	Label	Attack Path	Type	Description
Cut Network	A_1	$[G_5]$! $[G_6]$	Physical	$[G_5]$: $w1 = 60, w2 = 40, f = 20, v = 2, d = 5, lambda = 0.0011, lambda1 = 0.0011$ $[G_6]$: $w1 = 80, w2 = 20, f = 5, v = 1, d = 50, lambda = 0.00301, lambda1 = 0$
Jam Network Comms	A_2	$[G_8]$! $[G_9]$! $[G_{11}]$	Logical	$[G_8]$: $w1 = 60, w2 = 40, f = 20, v = 2, d = 5, lambda = 0.001188, lambda1 = 0.001188$ $[G_9]$: $w1 = 60, w2 = 40, f = 10, v = 1, d = 50, lambda = 0.0011, lambda1 = 0.0011$ $[G_{11}]$: $w1 = 80, w2 = 20, f = 10, v = 1, d = 100, lambda = 0.001, lambda1 = 0$
Inject Packets	A_3	$[G_8]$! $[G_9]$! $[G_{12}]$	Logical	$[G_{12}]$: $w1 = 80, w2 = 20, f = 30, v = 2, d = 250, lambda = 0.001, lambda1 = 0$
Cut Power	A_4	$[G_{23}]$! $[G_{24}]$	Physical	$[G_{23}]$: $w1 = 60, w2 = 40, f = 50, v = 3, d = 100, lambda = 0.00092, lambda1 = 0.00092$ $[G_{24}]$: $w1 = 80, w2 = 20, f = 10, v = 2, d = 350, lambda = 0.001, lambda1 = 0$
Drive Stop	A_5	$[G_{29}]$! $[G_{30}]$	Logical	$[G_{29}]$: $w1 = 60, w2 = 40, f = 40, v = 3, d = 100, lambda = 0.000596, lambda1 = 0.000596$ $[G_{30}]$: $w1 = 80, w2 = 20, f = 30, v = 2, d = 500, lambda = 0.0005, lambda1 = 0$
Brake Tamper	A_6	$[G_{29}]$! $[G_{36}]$	Logical	$[G_{36}]$: $w1 = 80, w2 = 20, f = 40, v = 4, d = 500, lambda = 0.0005, lambda1 = 0$
Brake Stop	A_7	$[G_{29}]$! $[G_{37}]$	Logical	$[G_{37}]$: $w1 = 80, w2 = 20, f = 25, v = 2, d = 500, lambda = 0.0005, lambda1 = 0$
Gear Break	A_8	$[G_{45}]$! $[G_{46}]$	Physical	$[G_{45}]$: $w1 = 60, w2 = 40, f = 20, v = 4, d = 5, lambda = 0.0011, lambda1 = 0.0011$ $[G_{46}]$: $w1 = 80, w2 = 20, f = 40, v = 8, d = 200, lambda = 0.001092, lambda1 = 0$
Explosion	A_9	$[G_{76}]$! $[G_{77}]$	Physical	$[G_{76}]$: $w1 = 65, w2 = 35, f = 50, v = 4, d = 5, lambda = 0.00037, lambda1 = 0.00037$ $[G_{77}]$: $w1 = 80, w2 = 20, f = 100, v = 10, d = 5000, lambda = 0.000178, lambda1 = 0$

Analyzing Simulation Results

The analysis is started by looking at the probability of disruption over time. Figure 5.9-8 shows the runs of five different scenarios to identify paths that cause the most disruption for the railroad bridge over a 10-year period. Note that low-detection attacks curve is very close to the fault curve due to two reasons: the first is that attacks with low-detection probability lets the attacker carry out the attacks without any mitigations as these attacks have a low probability of being detected, and hence they appear as if caused by a natural attack; second, the explicit parameter values chosen for this simulation also contributed to the curves and their proximity. The latter reason shows the need to use realistic data obtained from individual bridges, as moveable bridges are custom-made and hence no two bridges are identical.

At the 1-year limit, the *Only Faults* scenario resulted in fault probability $P(t < 365) = 0.747$. After 2 years, the Only Faults scenario had obtained a higher fault probability $P(t < 730) = 0.955$. *Attack* scenarios with *no*, *low*, or *high* detection rates at the second year were observed to be 0.197, 0.175, and 0.0815, respectively.

To identify the critical path within the fault tree, the simulation was rerun by disabling each of the BCF leaves found in the AFT at the 1-year intervals, where the *Only Faults* scenario resulted in a fault at $P(t < 365) = 0.747$. After testing all the BCF leaves, the percentage difference of the

new results with the baseline value is calculated. The results for this experiment are shown in Table 5-3 for all BCF leaves. This experiment shows that power-related BCF leaves pose the greatest risk to bridge failure. The G_{38} leaf representing a *motor brake power failure* created the highest differential at $P(t < 365) = 0.561$, a difference of -25.009 percent, followed by G21 (generator), with a difference of -21.455 percent, and G20 (power outage), with a difference of -19.601 percent. Note that G20 and G21 share the same critical path of failure, as the power generator should take over in the event of a power failure. Generators are not built to last forever and have a low exponential failure rate with $\lambda = 0.0042$. This may show a weakness in the design of the model. Without any repair capability to the power system, this defeats the purpose of a backup power system if it is not reliable as often as a power failure occurs.

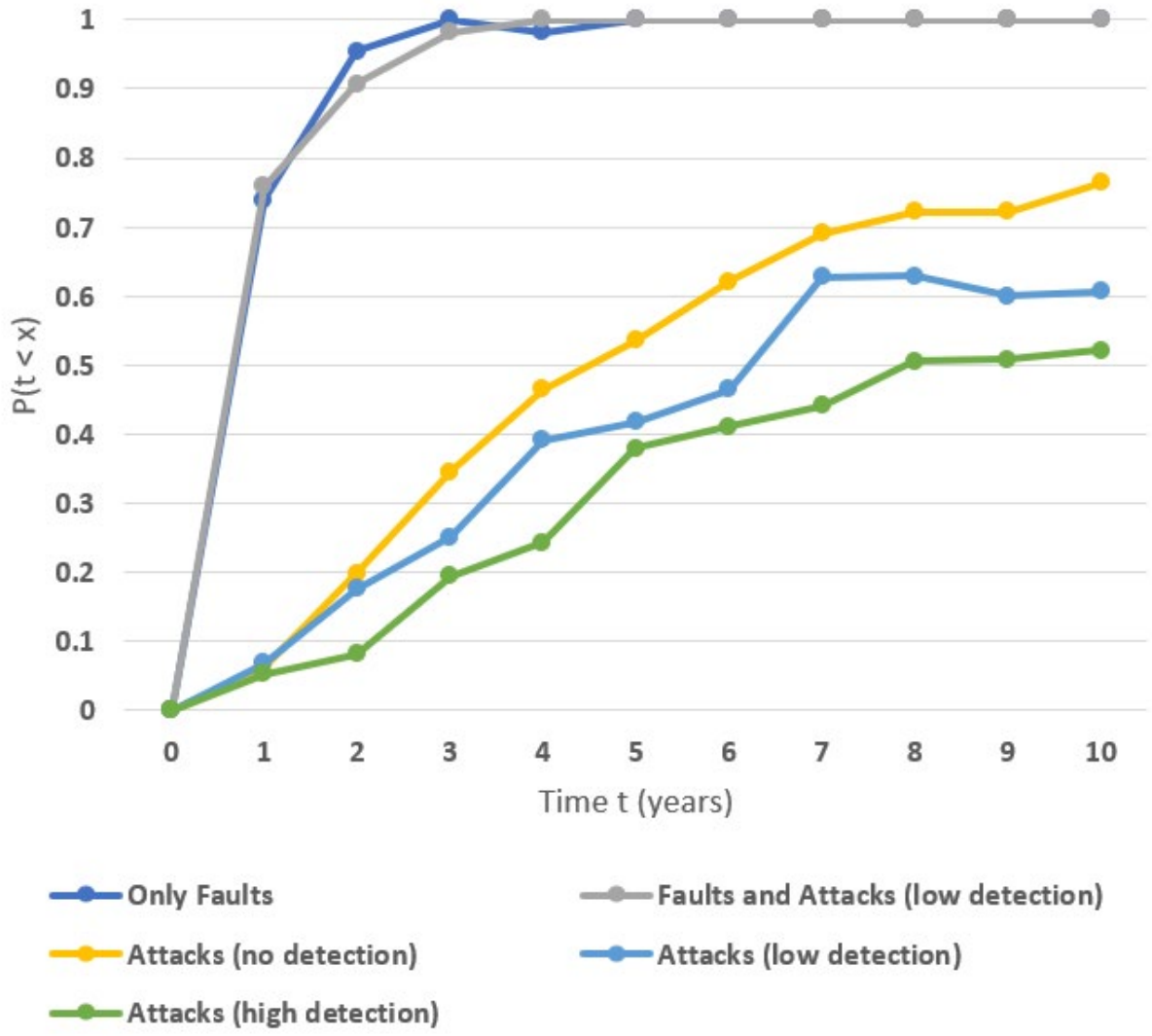


Figure 5.9-8 Probability of Disruption with Time

Table 5-3 Analysis of Fault Percent of Disruptions against All (74.757%)

Leaf	$P(t \leq 365)$	% Diff	Leaf	$P(t \leq 365)$	% Diff
G_{15}	0.720	-3.753%	G_{57}	0.748	0%
G_{16}	0.693	-7.333%	G_{58}	0.734	-1.88%
G_{17}	0.724	-3.162%	G_{60}	0.749	0.217%
G_{20}	0.601	-19.601%	G_{62}	0.716	-4.222%
G_{21}	0.587	-21.455%	G_{63}	0.748	0%
G_{27}	0.702	-6.088%	G_{66}	0.758	1.346%
G_{33}	0.561	-25.009%	G_{67}	0.728	-2.678%
G_{38}	0.699	-6.520%	G_{69}	0.689	-7.867%
G_{40}	0.718	-3.931%	G_{70}	0.749	0.21%
G_{42}	0.731	-2.183%	G_{72}	0.737	-1.368%
G_{43}	0.724	-3.162%	G_{73}	0.724	-3.152%
G_{50}	0.722	-3.459%	G_{74}	0.752	0.543%
G_{51}	0.708	-5.249%	G_{79}	0.722	-3.46%
G_{53}	0.697	-6.793%	G_{80}	0.735	-1.679%
G_{55}	0.735	-1.679%			

Table 5-4 AS-IS (Left) vs. WHAT-IF Attack Profiles (Right) over 10 Years

	Nate	Mallory	Chuck
P(t < 3650)	0.360	0.127	0.102
Mean E(t) in days	828.469	606.163	410.418
Mean E(costs) in US$	4158.215	2388.666	1706.83
Mean E(damage) in US$	1066.595	1058.763	442.77
Attacks Successful	133	22	14
Runs	371	182	150

	Nate	Mallory	Chuck
P(t < 3650)	0.226	0.0454	0.0515
Mean E(t) in days	982.201	628.984	971.847
Mean E(costs) in US$	4409.470	1650.969	1776.107
Mean E(damage) in US$	1361.609	752.78	670.127
Attacks Successful	65	4	5
Runs	287	88	97

Attacker Profile Analysis

AFTs were used to create attacker profiles for determining effective strategies against simulated adversaries. Three attacker profiles were devised to determine the effectiveness of adding security controls. Dollar amounts for budgets, costs, and damage in this section should be multiplied by 1,000.

- **Nate**: Nation-state attacker; budget = 10,000; p = 90 percent success rate for all attacks
- **Mallory**: Hacker with budget = 5,000; p = 80 percent success rate for *logical* attacks and p = 60 percent success rate for *physical* attacks
- **Chuck**: External threat; budget = 3,000; p = 80 percent success rate for *physical* attacks and p = 60 percent success rate for *logical* attacks

Table 5-4 shows the distinction between AS-IS and WHAT-IF results of running these three attack profiles against the AFT tree over 10 years. In the AS-IS scenario, Nate has a 35.963 percent chance of conducting a successful attack, compared with Mallory (12.730 percent) and Chuck (10.180 percent). Although Nate spends twice as much money on conducting a successful attack in the average case as Mallory ($4,158.21 vs. $2,388.67), they conduct roughly the same amount of average damage per attack ($1,066.60 vs. $1,058.76). This similarity initially suggests that more successful attacks are likely to be *logical* attacks, as Mallory has a higher probability of successful attacks. Meanwhile, Chuck spent an average of $1,706.83 per successful attack, resulting in an average of $442.77 in damage per successful attack. This again confirms *logical* attacks within the AFT are more likely to occur given the resources, as Chuck is more likely to succeed at *physical* attacks. A time comparison shows that Nate (828.47 days) takes longer average time than Mallory (606.163 days) and Chuck (410.42 days). As Nate has more resources to leverage to conduct a successful attack, he is able to spend more time waiting for an attack to succeed than either Mallory or Chuck, resulting in this higher average.

In the WHAT-IF scenario, detection values are reconfigured for w_1 and w_2, as shown in Table 5-2. Team researchers computed the percentages of successful attacks in the WHAT-IF scenario decline for Nate by -37.22 percent, Mallory by -64.25 percent, and Chuck by -49.51 percent, demonstrating the usefulness of detection against all attacker profiles. Nate saw an increase in average time by 18.56 percent and cost by 6.04 percent for his attacks, but presumably took greater risks with his additional resources, as the damage he inflicted also increased by 27.66 percent. The simulation was executed 10 additional times for Nate and received similar results to confirm this was not an anomaly. In contrast, Mallory saw an increase in the time required to conduct a successful attack by only 3.76 percent, but a decrease in the average cost by -30.88 percent and damage by -28.8 percent. Chuck saw a very large increase in the time required to conduct a successful attack by 136.79 percent, but only a slight increase in the average cost – 4.06 percent, but a large increase in damage – 51.35 percent. Based on these results, additional detection mechanisms appear to be more useful against a strictly *logical* attacker (Mallory) than those that are stronger at *physical* attacks (Nate and Chuck).

Table 5-5 Analysis of Attack Disruptions Measured Against

Attack	$P(t <= 3650)$	**% Diff**	**Attack**	$P(t <= 3650)$	**% Diff**
A_1	0.275	-19.365%	A_6	0.347	1.858%
A_2	0.343	0.8072%	A_7	0.349	2.38%
A_3	0.343	0.8072%	A_8	0.358	5.234%
A_4	0.341	0%	A_9	0.339	-0.5234%
A_5	0.330	-3.244%			

Based on the previous observation that attackers with strengths in *logical* attacks seemed disadvantaged, there is a need to identify critical attack paths that might exist in the graph to explain this behavior. To do so, the researchers reran the test for the attacks (no detection) previously described scenario, with Nate configured as the attacker. The tests were configured to run for 10 years without any detection mechanisms. The results for this experiment are shown in Table 5-5 for all the attack paths for this section. This experiment shows that the physical attack path A_1 focused on physically cutting network links is the critical path, as it had the highest differential, with a -19.365 percent drop in the probability of successful attacks. This explains

why *physical* attackers fared better in the *WHAT-IF* scenario. By applying detection methods of similar strength to both logical and physical attacks, the observation is that those stronger at physical attacks (Nate and Chuck) were still able to increase the amount of damage caused. This was due to their ability to complete A_1 to cut the bridge network links at a higher rate for a successful attack.

5.9.3 The AFTeR Model and Using It to Model Risks of Movable Rail Bridge

AFTeR is designed to use data available to the transportation authority to identify if some event was caused by a safety or security failure. It expands on the AFT model (Kumar & Stoelinga, 2017) for identifying possible safety and security failures by incorporating proactive system maintenance, reactive repairs, and incidence response into the qualitative and quantitative analysis. AFTeR was designed under the premise that by collecting and analyzing this data regarding a bridge's maintenance, faults, and repairs over time, it is possible to assign probability to some hazardous event as a fault or attack in order to determine the appropriate reaction. It was also designed to provide the system owner with a method to quantify reliability in order to justify the costs of proactive maintenance. Consequently, this research contributes a comprehensive identification and stochastic analysis of cyber attacks against a fail-safe movable bridge drive system and the AFTeR model, which brings the following contributions:

1. Incorporation of stochastic process models to calculate component failure rates when repairs leave the system in an as-good-as-new or as-bad-as-old states.
2. Statistical quantification demonstrating the reliability benefits of regular system maintenance towards addressing safety and security threats.
3. Incorporation of repairs after the failure of repairable and non-repairable components to allow for a trace analysis of probabilistic threat impacts over time.
4. Identification of scenarios where it is not possible to delineate between faults or attacks, giving an attacker's advantage.

The rest of the section is structured as follows. First, the research team provides background details on movable bridges, safety and reliability, CPS security, and the AFT model. The team next describes their enhancements in AFTeR to the original AFT model, followed by a qualitative and quantitative analysis of a fail-safe movable bridge system using AFTeR. The team concludes with a discussion on the AFTeR approach and a summary of findings.

In this section, the AFTeR model and its semantics are detailed, focusing on modifications made to the AFT model to incorporate reliability. Discussion regarding inherited AFT model components is limited; instead it is deferred to Koglin (2003) for a description on the inherited stochastic timed automata (STA), variables, behaviors, and testing safety and security metrics.

5.9.4 Qualitative Models

The qualitative AFTeR model is similar to AFT, leveraging similar gates as dynamic fault trees. two new intermediary gates are introduced, REPAIR and NONREPAIR, that visually indicate whether some system components that could fail or be attacked can be fixed during a maintenance cycle. For this modeling, the team also incorporates an intermediary node for readability of the model (although it does not have an STA), which the research team includes

here for completeness. All gates used in this section for qualitative analysis can be seen in Figure 5.9-4.

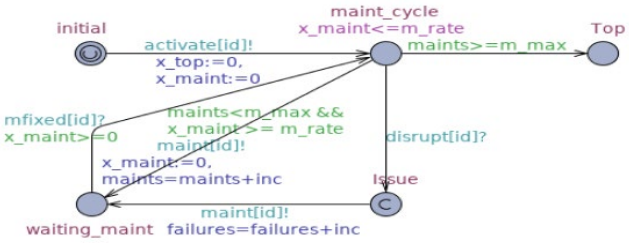
Modifications to Stochastic Timed Automata

Discussion here is limited to the modifications made to the AFTeR STA model semantics and how the team incorporated maintenance, repairs, and repairable and non-repairable components. For general UPPAAL SMC semantics, see David *et al.* (2015a).

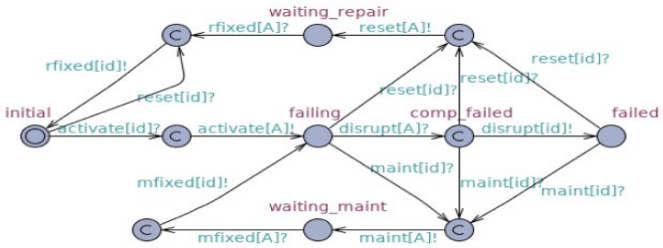
Maintenance/Repairs of Stochastic Timed Automata

To incorporate maintenance cycles into AFTeR, four broadcast channels were used to communicate maintenance status between parent and child nodes: *maint[id], mfixed[id], reset[id],* and *rfixed[id]*. As shown in the STA models of Figure 5.9-11, these channels form *maint* loops during maintenance cycles and *reset* loops to prevent deadlock from conditional nodes such as SAND and SPARE. Three global clocks were used to track maintenance cycle status: (1) *x_maint* is used to track the time inside the current maintenance cycle; (2) *maints* is a counter that tracks completed maintenance cycles, and (3) *failures* are used as a counter to track the number of top-level system failures that were repaired during the simulation run.

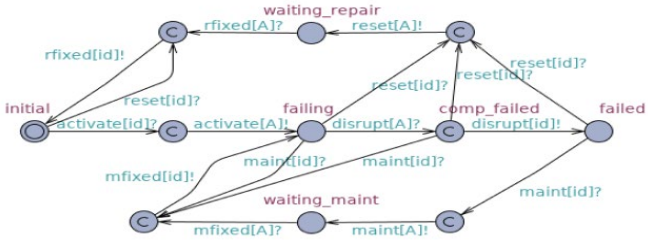
A separate clock to model MTTR was not incorporated, as the exponential failure rate invariants found in BCF and BAS leaves could lead to concurrent failures. Instead, probabilistic downtime due to repairs is computed using the number of failures and maintenance cycles in a given time period. An example query to obtain the constrained *failures* values using the WMTL query language in the UPPAAL SMC within time t and failures F would be $P[failures \leq F](<> top\_event.\ Top \wedge x\_top \leq t)$, where *top_event* is the name of the TOP model template and *x_top* is the global clock.



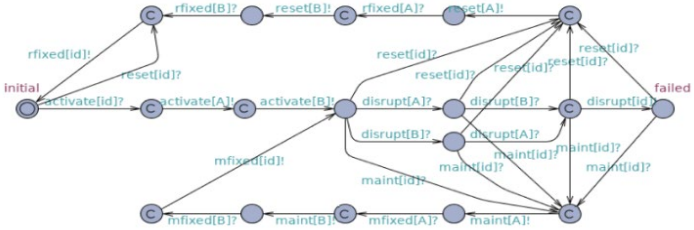
a.



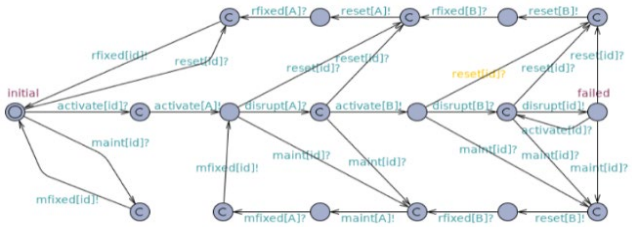
b.



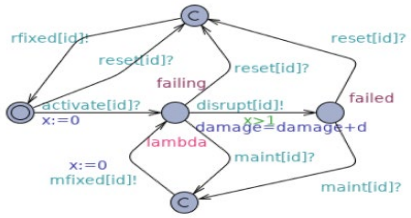
c.



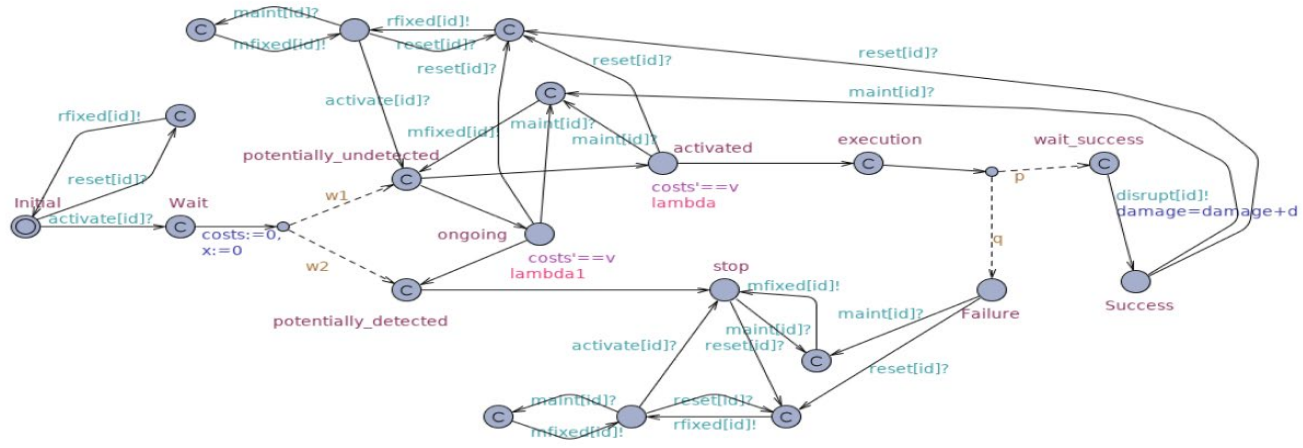
d.



e.



f.



g.

Figure 5.9-9 Stochastic Timed Automata of Each Model

Note: a) TOP, b) REPAIR, c) NONREPAIR, d) AND, e) SAND/SPARE, f) BCF, g) BAS

The TOP Model

The TOP model (Figure 5.9-9 2a) incorporates three global clocks to manage maintenance cycles. It takes two variables to constrain the number of maintenance cycles as input: 1. *m_rate* – the length of the cycle in terms of time and 2. *m_max* – the maximum number of cycles to step through before transitioning to the Top. When *x_maint* clock exceeds the maintenance cycle window, the system transitions to *waiting_maint*. If a system-wide failure occurs while waiting for maintenance, the child passes **disrupt[A]!** and the TOP transitions to the *Issue* state before triggering the maintenance cycle. To probabilistically determine if a failure occurs at all in a time period, the WMTL query should check if *top_event.Issue* has been reached.

REPAIR and NONREPAIR Gate Models

Both the REPAIR (Figure 5.9-9 2b) and NONREPAIR (Figure 5.9-9 2c) models serve as a top-level component STA used to filter maintenance cycles from repairing or replacing the specific component. Initially, both models start in the left-most state, waiting for activation from their parent node. At any point in the failing stage, *maint* or *reset* cycle could be triggered and the difference in the two models is how they react to the **maint[id]?** signal. In the REPAIR model, even if the component has not failed, it immediately responds with a **maint[A]!**, signaling its child automaton to begin its maintenance cycle. In the NONREPAIR model, unless the component has failed, the component immediately responds with a **mfixed[id]!** signal to let its parent know the maintenance loop is complete and returns to the *failing* state.

Existing AFT Gate and Basic Component Failure (BCF) Models

The AND model (Figure 5.9-9 2d) OR model (similar *maint* and *reset* to AND), SAND / SPARE (Figure 5.9-9 2e)/(Figure 5.9-9 2f) and BCF model (Figure 5.9-9 2g) were modified to incorporate the *maint* and *reset* loops. After receiving a *maint* or *reset* signal, AND and OR models signal **maint[x]!** or **reset[x]!** and wait for each of their x children to conduct their loops. SAND / SPARE models differ in that when they receive a *maint* signal, they signal **reset[x]!** to their children except for the left-most child to ensure that the model remains in a non-deadlocked state. FDEP, PAND, and iFAIL models in Kumar and Stoelinga (2017) could be modified similarly.

Basic Attack Step (BAS)

The BAS model modification serves two purposes: (1) to give the attacker a chance to regain access or reattempt their attack if it is currently underway or was previously successful; and (2) to ensure that no deadlocks occur due to *maint* or *reset* cycles. If an attack was previously successful or currently underway when the model received a **maint[id]?** or **reset[id]!** signal, the attacker would return to the *potentially_undetected* state. It is possible that system maintenance could install security patches or make a configuration change to fix the vulnerability where the attacker exploited to gain access, so the attacker might lose some capability after *maint* or *reset* requiring another attempt. If an attack was previously detected or failed, assumption was made that the attacker would not spend additional resources to reattempt the attack.

5.9.5 Qualitative Analysis

In this section, the team researchers use AFTeR to provide a qualitative analysis of a fail-safe movable bridge control system. The reference model of the team is shown in Figure 5.9-10 based on the fail-safe control system described in VanDeRee (2016).

Reference Model Definition

Networked electronic components were the focus, as they are susceptible to cyber attacks. Fail-safe bridge controls require redundancies to ensure that the bridge remains operational despite a component failure. The drive system leverages a PLC, *P1,* programmed using ladder logic to take operator control orders and sensor data as input and convert the instructions and the perceived system state into physically actuating the bridge. The variable speed drive (VSD), *V1*, converts instructions from the PLC into motor actuation using a *pulse width modulation (PWM)* signal. The PLCs and VSDs are both configured with warm spares (*P2* and *V2,* respectively) to ensure that the system continues to function in the event where their primaries fail. All these components communicate over the LAN, leveraging protocols such as MODBUS for input and output. The LAN is configured with redundant Ethernet switches, *L1* and *L2,* and network interfaces from the PLCs and VSDs are aggregated across both switches to ensure communication in the event of a switch failure.

Operator controls are also built with redundancies. Field operators use radios, *R1* and *R2,* to send open and close commands to a wireless controller. If the operator is physically inside an operator closet, they could leverage a human machine interface (HMI), *H,* to also control the bridge. Both the wireless controller and HMI pass control instructions to the PLC, which then leverages its ladder logic to determine if it is safe to move the bridge.

Modern drive systems leverage an electric motor, *M,* to convert electrical energy to mechanical energy that moves the bridge. As part of the control logic, an electric brake, *B,* is closed to prohibit movement and released when the VSD provides current instructing the motor to move. To protect the motor from being overloaded by the current, overload protection relays, *O,* are mechanical components that monitor the current to the motor and open the relay contacts when the current remains high for an extended time. Sensors are used to monitor the states of the relays, current, brakes, and motor, which provide feedback to the control system. In the AFTeR analysis, a motor temperature sensor *S* is incorporated.

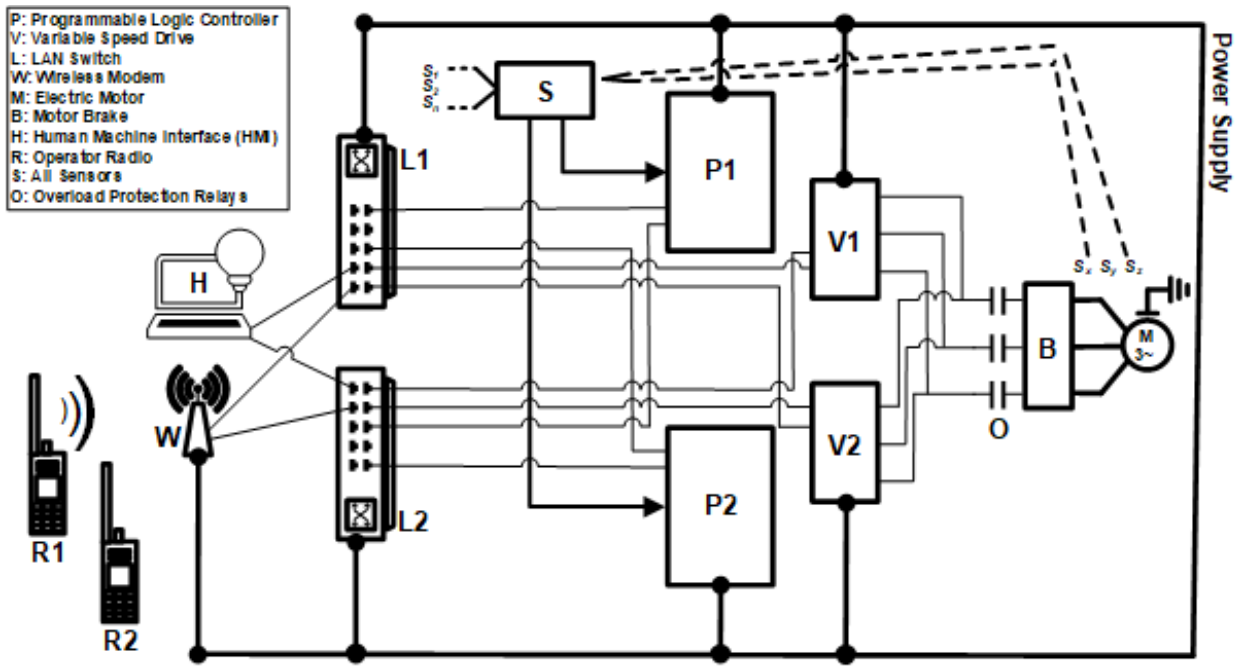


Figure 5.9-10 Wiring Diagram of a Fail-Safe Movable Bridge System

AFTeR Model Definition

The AFTeR model in Figure 5.9-11 qualitatively shows how component faults or cyber attacks against the fail-safe system could result in a *Bridge Halted* state (G_0). The gates and leaves, labeled G_0-G_{66}, are referenced individually in the discussion and analysis of this report. The team classifies PLCs, VSDs, and radios as *repairable* components using a SPARE gate, as the redundancy and warm/cold spare relationship would allow for maintenance when one member of the cluster fails, or for system upgrades with no downtime. Remaining components are treated as *nonrepairable,* either due to their mechanical nature, or because their product manuals/reviews classify them as such. The research team also treats the redundant networked switches as nonrepairable, as it is often possible for individual switch ports to fail, many times without being detected because of the redundancy provided by aggregated network ports across multiple networking devices. The rest of this section provides the configuration details for the quantitative analysis. Background information on BAS values and constraints, attacker profiles, and analysis is provided in depth by M. Jablonski (2019).

Faults

Due to a lack of data on finer grained component failures in movable bridges, faults were limited to individual component failures. One can calculate the MTBF *(repairable)* and MTTF *(nonrepairable)* for each component with granularity in days using assumptions from product reviews (unless otherwise noted), and by converting the value to λ that are included in Table 5-2. Both λ and the noted d value, representing damage costs X 10^3, are variables used by the BCF leaves for the quantitative analysis.

- B (G_4): Assume 10 percent of brakes fail at 1,000,000 cycles, with 60 cycles/day; MTTF = 1,000,000/(0.1*60) = 166,667 days; d = 100

- *M* (G_8): MTTF = 65y = 23,725 days; *d* = 300
- *S* (G_{12}): MTTF = 100y = 36,500 days; *d* = 5
- (G_{14}): MTTF = 1,000,000h = 41,667 days; *d* = 6
- *V1*/*V2* (G_{20}/G_{22}): MTBF = 300,000h = 12,500 days; *d* = 40
- *R1*/*R2* (G_{29}/G_{30}): MTBF = 20,000h = 833.33 days; *d* = 2
- *W* (G_{34}): MTTF = 90,000h = 3,750 days; *d* = 10
- *H* (G_{38}): MTTF = 50,000h = 2,083.33 days; *d* = 25
- *L1*/*L2* (G_{47}/G_{50}): MTTF = 10y = 3,650 days; *d* = 15
- *P1*/*P2* (G_{60}/G_{63}): MTBF = 40,000h = 1,666.67 days; *d* = 80

Attacks

The research team leveraged SAND gates in Figure 5.9-11 to show the serial steps represented by BAS leaves of an attacker while they step through their kill chain to disrupt or control the system. The resulting kill chains, labeled A_1-A_7, for the reference model (detailed in Table 5-6) were derived from a review of Stuxnet and other real-world SCADA attacks that are applicable to movable bridge systems (Zhu *et al.*, 2011). Jamming attacks (A_1) against the wireless network did not have a multi-step kill chain as such an attack could physically occur some distance from the bridge. The remaining kill chains require the attacker to obtain network access (G_{52}) and possibly either HMI (G_{40}) or PLC (G_{65}) access. To gain an initial network foothold, an attacker could use a variety of methods such as implanting a physical device on the network or installing malware on an operator's maintenance laptop. The specifics of gaining network access are not shown here but should be considered when conducting security assessments of movable bridge systems. Attack goals vary from denying service (A_1, A_4, A_6) to controlling bridge movement (A_2, A_3, A_4, A_7).

Modeled Attacks were estimated to take no more than 1–2 years to execute or be detected prior to execution, represented by λ and $\lambda 1$, respectively. The listed w_1 and w_2 values represent high detection values for the WHAT-IF analysis (it should be assumed that w_1 is higher and w_2 is lower for the AS-IS analysis to represent low defensive detection capabilities). Cost value *f* is defined based on assumptions of costs to research and develop the attack step. Cost value *v* is defined based on possible daily costs to an attacker to maintain persistence while undertaking the attack step. Cost value *d* is defined based on assumptions of costs for incidence response and/or component damages. In the adopted model, attackers did not accrue any ongoing costs ($v = 0$) during attacks G52, G40, and G65, so that attackers would not get penalized for repeat access attempts after maintenance cycles. Instead, the research team opted for upfront costs for access attacks, and then assigned a v value to the final attack in the kill chain.

Table 5-6 Definition of Fail-Safe Movable Bridge Kill Chain

Attack Name	Kill Chain	Type	Leaf	BAS Values
A_1 - Jam Wireless	G_{35}	Network	G_{35}	w_1=80, w_2=20, f=5, v=3, d=25, λ=0.015, λ_1=0.015
A_2 - Control HMI	G_{52}→G_{40}→G_{41}	SCADA	G_{52}	w_1=70, w_2=30, f=30, v=0, d=5, λ=0.0093, λ_1=0.0093
			G_{40}	w_1=80, w_2=20, f=60, v=0, d=10, λ=0.065, λ_1=0.065
			G_{41}	w_1=80, w_2=20, f=10, v=2, d=50, λ=0.08, λ_1=0.014
A3 - Packet Injection	G_{52}→G_{43}	Network	G_{43}	w_1=70, w_2=30, f=30, v=2, d=30, λ=0.0095, λ_1=0.02
A4 - DoS LAN	G_{52}→G_{53}	Network	G_{53}	w_1=70, w_2=30, f=10, v=1, d=125, λ=0.035, λ_1=0.04
A5 - Inject PLC Logic	G_{52}→G_{65}→G_{56}	SCADA	G_{65}	w_1=80, w_2=20, f=40, v=0, d=15, λ=0.025, λ_1=0.025
			G_{56}	w_1=80, w_2=20, f=12, v=2, d=225, λ=0.045, λ_1=0.011
A6 - DoS PLC	G_{52}→G_{65}→G_{66}	SCADA	G_{66}	w_1=80, w_2=20, f=10, v=1, d=175, λ=0.07, λ_1=0.095
A7 - Inject Sensor Data	G_{52}→G_{65}→G_{16}	SCADA	G_{16}	w_1=80, w_2=20, f=20, v=2, d=400, λ=0.065, λ_1=0.01

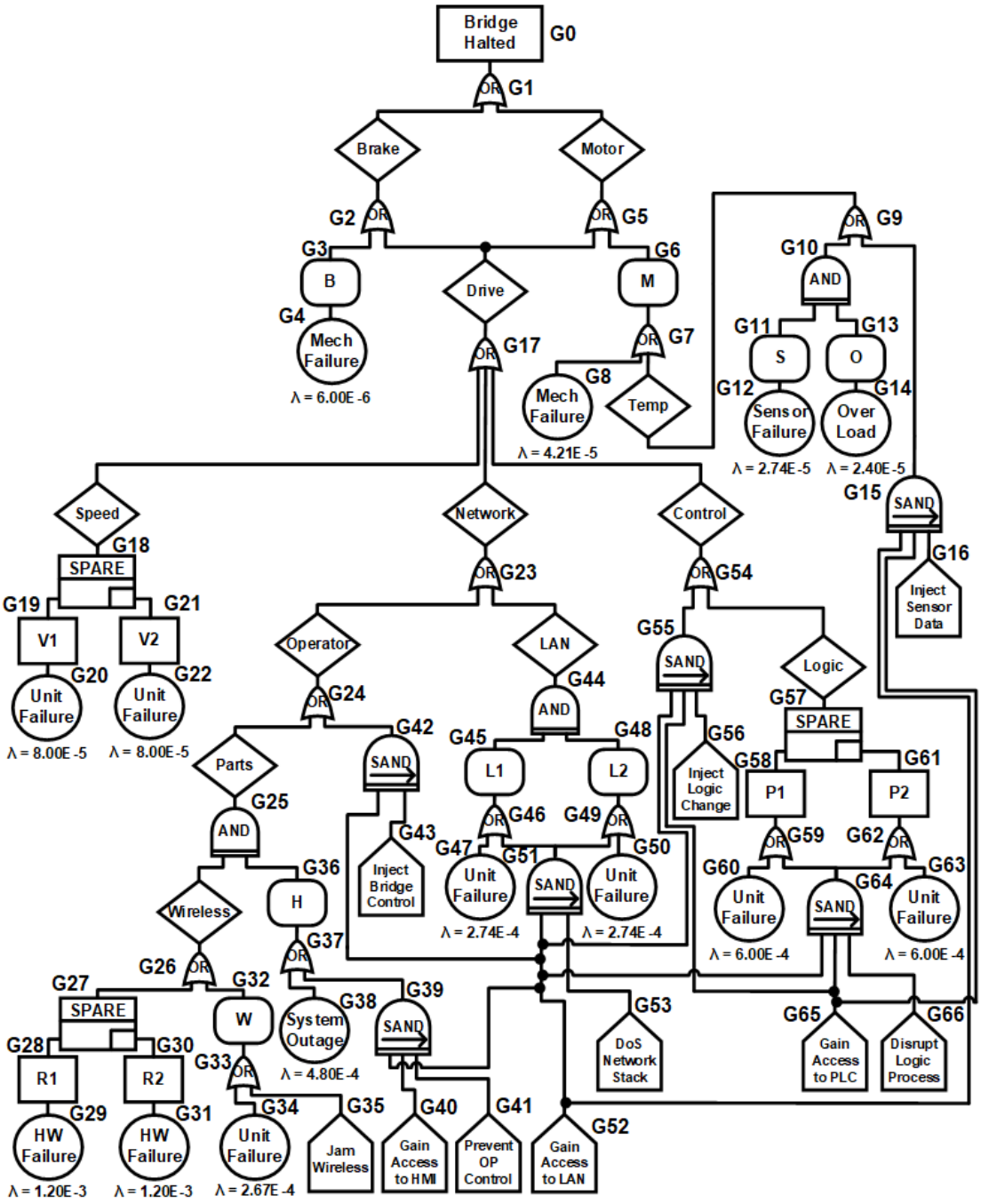


Figure 5.9-11 Qualitative AFTeR Model of Fail-Safe Movable Bridge

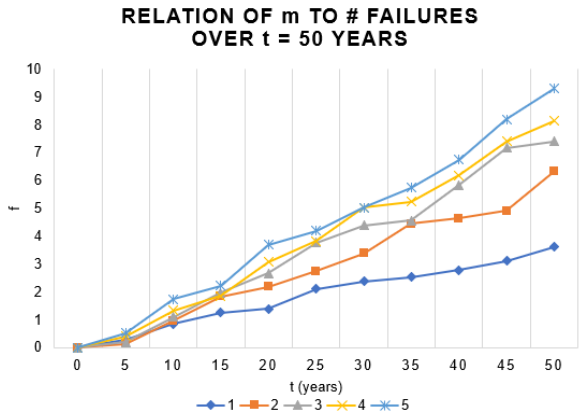
Attacker Profiles

BAS leaves were categorized as *SCADA* or *Network* in Table 5-6 to allow for the creation of attack profiles for quantitative analysis in the following section. APTs exist with expertise in either or both categories and the quantitative analysis would indicate offensive skillsets required for a successful attack. Attacker profiles are defined below with their budgetary (*cost*$ x 10^3) and probability of success (*p*) constraints.

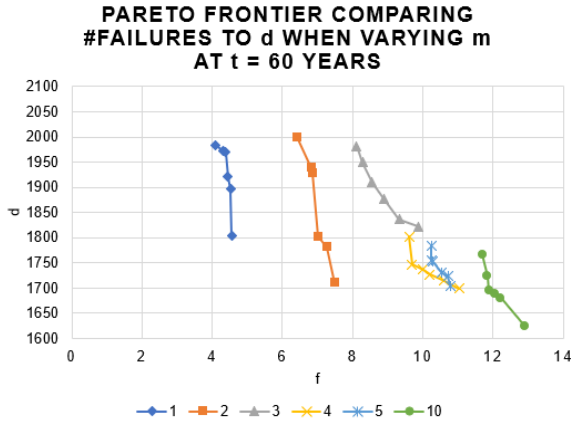
- ***Nicole***: Nation-state attacker; *cost* = 1,000; *p* = 90 percent
- ***Ike***: Network specialist; *cost* = 300; p_{net} = 80 percent and p_{scada} = 60 percent
- ***Josh***: SCADA specialist; *cost* = 300; p_{scada} = 80 percent and p_{net} = 60 percent

5.9.6 Quantitative Analysis

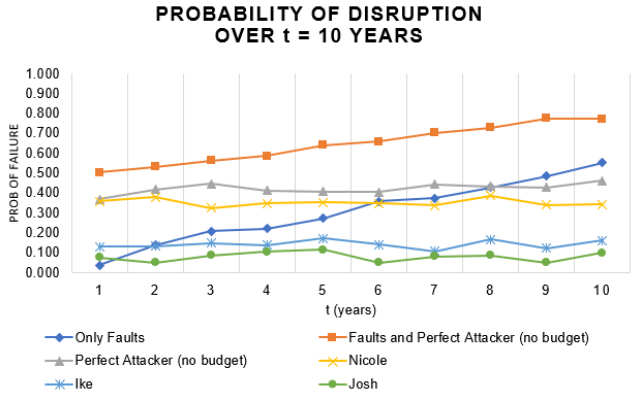
As discussed previously, AFTeR quantitative analysis allows for the statistical analysis of faults and attacks within the model using UPPAAL SMC. The experiments were selected to showcase AFTeR's maintenance and reparability contributions and to provide statistical details regarding faults and attacks in the bridge control system. For all experiments, let *m* represent the length of a maintenance cycle in years; *d* represents damage in \$ x 10^3; *c* represents attacker cost in \$ x 10^3; *f* represents the number of failures; t represents the length of the test scenario. All tests were run using UPPAAL SMC 64-bit version 4.1.19, in a Fedora 28 VM configured with 4 GB RAM and 4 Intel Core i5-8400 virtual CPUs.



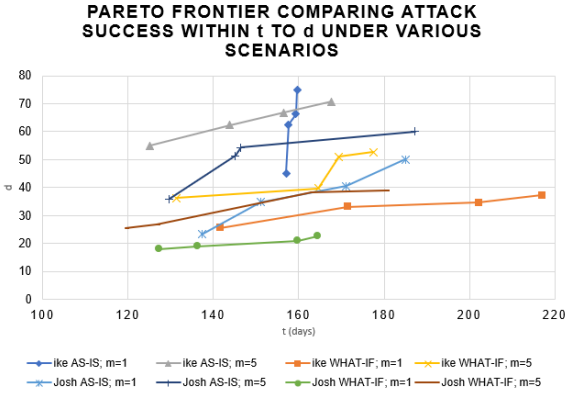
a. **Comparing m={1-5} to failures**



b. **Comparing failures to d under varying m**



c. **Comparing faults and attacks under varying scenarios**



d. **Comparing attack success under varying scenarios**

Figure 5.9-12 Quantitative Analysis Comparisons

Analysis of System Maintenance Cycles on Fault Rates

For m∈{1,2,3,4,5}, the research team ran the simulation at 5-year intervals over 50 years to identify the mean number of failures for each *m* at *t*. The results are shown in Figure 5.9-12 (a). By varying the maintenance interval, one can identify a linear relationship where the slope is related to the value of *m*. Within 10 years, $\bar{f}_{m=1,t=10} = 0278 \pm 0.154$ failures and $\bar{f}_{m=1,t=10} = 0.527 \pm 0.286$ failures, resulting in an 89.568 percent growth when varying *m*. After 50 years, $\bar{f}m=1,t=50 = 3.611 \pm 0.59$ failures and $\bar{f}_{m=5,t=50} = 9.306 \pm 0.646$ failures, resulting in a 157.713 percent growth. All values are within the 95 percent CI. Annual inspections, as required in the U.S. by law (Movable Bridge Locking Inspection, 33 CFR §236.387, 1984), clearly have the intended effect of limiting failure under AFTeR.

A second experiment was conducted at $t = 60$ years to compare *d* of component failures m∈{1,2,3,4,5,10}, by rerunning each value of *m* through the simulator six times and collecting *d* and *f*. A Pareto frontier representing the results are in Figure 5.9-12 (b). Again, the relationship of *m* to $\bar{f}$ holds at *t* = 60 years. The mean of the runs result in $\bar{f}_{m=1,t=60} = 4.384$ and $\bar{d}_{m=1,t=60} = 1924.759$ for $m = 1$, $\bar{f}_{m=5,t=60} = 10.467$ and $\bar{d}_{m=5,t=60} = 1741.995$ for $m = 5$, and $\bar{f}_{m=10,t=60} = 12.102$ and $\bar{d}_{m=10,t=60} = 1696.208$ for $m = 10$. These results indicate greater *d* costs over time for smaller values of *m*. This relationship seems paradoxical, but it is due to the design and use of component redundancy in the fail-safe bridge system. In AFTeR, non-repairable redundant components have their failures detected more frequently under smaller *m* values, so they are replaced faster resulting in more component failures over time. The tradeoff is that the system does not fail as frequently.

Table 5-7 Percentage of Disruptions

BCF	P(x<=10)	percentDiff	Leaf	P(x<=10)	percentDiff
G_4	0.505	-8.85	G_{31}	0.456	-17.69
G_8	0.437	-21.12	G_{34}	0.439	-20.76
G_{12}	0.521	-5.96	G_{38}	0.358	-35.38
G_{14}	0.507	-8.48	G_{47}	0.429	-22.56
G_{20}	0.498	-10.11	G_{50}	0.469	-15.34
G_{22}	0.529	-4.51	G_{60}	0.386	-30.33
G_{29}	0.437	-21.12	G_{63}	0.382	-31.05

a. Fault Percentage of Disruptions Measured Against $P(t \leq 10) = 0.554$

Attack	P(t<=10)	percentDiff
A_1	0.420	-9.29
A_2	0.417	-9.94
A_3	0.413	-10.80
A_4	0.382	-17.50
A_5	0.410	-11.45
A_6	0.452	-2.38
A_7	0.450	-2.81

b. Attack Percentage of Disruptions Measured Against $P(t \leq 10) = 0.463$

Combined Attack-Fault Analysis

The research team conducted additional experiments to identify the relationships of attacks and faults at the optimal maintenance interval, where *m* = 1 year. For t∈{1,2,⋯,10}, the research team calculated the probability of the system failure before time *t*, $P(x \leq t)$, under various combinations of faults and attacks, as shown in Figure 5.9-12 (c). For attack profiles, the research team leverage *Nicole, Ike,* and *Josh,* along with a *perfect attacker* that does not have budgetary constraints to demonstrate peak attack success in a fail-safe bridge model. The system is configured without any security detection mechanisms for this experiment. The growth of $P(x \leq t)$ due to faults in this experiment is linear over time, as shown under both the *Only Faults* and

Faults and Perfect Attacker models. At $t = 10$, *Only Faults* resulted in $P(x \leq 10) = 0.554$ and *Faults and Perfect Attacker* resulted in $P(x \leq 10) = 0.774$, a 32.63 percent increase in risk for a fail-safe bridge under threat of attack.

To identify the critical fault path in the fail-safe movable bridge system, the research team reran the *Only Faults* model 14 more times, each time removing 1 fault leaf to observe the difference in results from $P(x \leq 10) = 0.554$. The results are shown in Table 5-7 (a). The table is a useful indicator of the relationships of component failures to overall failure in a fail-safe movable bridge design. The G_{38} leaf, representing an *HMI failure*, created the highest differential at $P(x \leq 10) = 0.358$ with a difference of -35.38 percent. Figure 5.9-12 demonstrates the reasoning for this finding, as the HMI is the only networked interface for operator control. A recommendation for the fail-safe bridge model would be to add additional hard-wired interfaces for operators in the event where the wireless system is unavailable.

For the attack-only models, Figure 5.9-12 show that attack success rate remains near constant over time for each of the attack models. This is primarily due to the low λ-value definitions, which the team defined based on their own research in networking and SCADA attacks against movable bridge systems. *Nicole,* the nation-state attacker with $c = 1{,}000$, performs very close to the *Perfect Attacker,* with $P(x \leq 10) = 0.343$ and $P(x \leq 10) = 0.463$. This indicates that the budget for a nation state could have a high success rate if they target a bridge system. When the team directly compare *Ike* (the network attacker with 0.162) and *Josh* (the SCADA attacker with $P(x \leq 10) = 0.101$), hypothesis is made that network attacks have the greatest chance of success when targeting a fail-safe movable bridge system.

To test the hypothesis, the research team conducted an additional experiment to find the critical attack path, taking a similar approach to finding the critical fault path. The team reran the *Perfect Attacker* scenario seven times, each time disabling the last leaf in each of the seven kill chains. The results are shown in Table 5-7 (b). Attack path A_4, representing the *network denial-of-service (DoS)* kill chain, created the highest differential at $P(x \leq 10) = 0.382$ with a difference of -17.50 percent. It is also observed that SCADA attacks A_6 and A_7, where an attacker attempts a PLC DoS attack or a sensor injection attack, have the lowest probability of success.

Additional Security Experiments

The team also determined if there was any relationship between attack success and variances in the maintenance interval. Using $m = 1$, the team compared the *Ike* (network) and *Josh* (SCADA) modes under the AS-IS low detection scenario and then under the WHAT-IF high detection scenario. As an additional variable, the test was repeated for $m = 5$. The results are shown as a Pareto frontier in Figure 5.9-12 (d), At $m = 1$, *Ike* took longer to conduct a successful attack in AS-IS, $\bar{t} = 158.417$, versus WHAT-IF, $\bar{t} = 183.079$ (a 15.56 percent difference). At $m = 5$, *Ike* again took longer to conduct a successful attack in AS-IS, $\bar{t} = 148.308$, versus WHAT-IF, $\bar{t} = 160.713$ (an 8.36 percent difference). *Ike*'s attacks took less time when $m = 5$ for both scenarios when compared against the same scenario in $m = 1$. *Josh*'s attacks resulted in similar comparisons for $\bar{t}$.

When directly comparing d for both AS-IS and WHAT-IF scenarios at $m = 1$, both *Ike* and *Josh* produced less damage to the bridge, as shown in Figure 5.9-12 (d). When comparing *Ike* at $m = 1$ AS-IS ($\bar{d} = 62.188$) versus $m = 5$ AS-IS ($\bar{d} = 63.715$), there is a 2.46 percent increase in damage. However, when comparing *Josh* at $m = 1$ AS-IS ($\bar{d} = 37.153$) versus $m = 5$ AS-IS ($\bar{d} = 50.451$),

there is a 35.46 percent increase in damage. This possibly indicates that SCADA attacks become more probable as the system is maintained less frequently. When directly comparing *Ike* to *Josh*, results show that attacks focusing on the network result in more damage than SCADA attacks in the fail-safe movable bridge system.

5.10 Conclusions and Mitigation Strategies

This section describes three increasingly complex models used to model the attacks and faults that could impact the functionality and performance of movable bridges. Given that risk and consequence analysis of cyber-physical systems due to faults and/or cyber attacks depends on the model chosen to represent the object or system under study, the consequences that can be drawn from the models vary. Therefore, the consequences drawn from the three models are presented as follows.

5.10.1 Conclusions Drawn from the Attack and Fault Trees

Many low coastal areas and areas with long waterways have been providing passageways to waterway traffic and rail traffic by using movable rail bridges. These bridges, considered as heavy movable structures, are custom-made to satisfy recommendations of AREMA and federal safety mandates. The movable components are carefully designed and controlled by a set of custom-made distributed controllers. Considered cyber-physical system-of-systems, movable bridges are subject to failures and attacks on their control systems.

5.10.2 Conclusions Drawn by Applying the Attack-Fault Model

In the interconnected twenty-first century, much work is being done to automate and connect movable bridge components into a network, which adds a new layer of risk. In this part of the research, the research team leveraged attack-fault trees to create a model that combines the physical risks of operating a railroad swing bridge with the newer logical risks against control systems.

Having analyzed the AFT approach, the team concluded with some thoughts on the stochastic timed automaton approach for this particular application. The approach was useful for mapping out all faults and attacks into a single model and allowed us to run a statistical analysis to identify critical paths in the graph. For the model, it is observed that power faults and physical network attacks are the best course for stopping a movable swing bridge. Although not discussed in the analysis section, by stepping through this model, it is observed that faults against the *substructure* and *superstructure* systems are statistical anomalies as far as a combined attack-fault model is concerned, and future research should focus on the electro-mechanical attack surface and its failures.

One can conclude that the AFT approach is good for identifying critical attack and fault paths at a high level. For the swing bridge case, it is believed that the model falls short in many ways. With the swing bridge, many faults could possibly occur only while the bridge is moving, or similarly only when the bridge is closed. The state of the system is not incorporated in the AFT model. For example, mechanical components like electric motors and gears have failure rates that are established only when the system is in use. For movable bridges, the system is only in motion for a few minutes at a time, and the mechanical components spend the majority of their time at rest. Also, the AFT approach allows for the incorporation of attack chains, but it does not

necessarily take into account specific system configurations included in previous attack tree models that this model was conceptually built upon. The AFT model also abstracts security control solutions into a simple detection mechanism to stop attacks, reducing its practical application against real-world environments.

5.10.3 Conclusions Drawn from the AFTeR Model

An analysis of a fail-safe movable bridge system led to several general conclusions regarding its safety and security risks. A computer simulation model has been developed, which can support "what-if" scenario analysis, the identification of a critical fault path, and a security path. Also, the model could be used to probabilistically differentiate between a fault and a cyber attack if the cause is not immediately known. It is also noteworthy that bridge designs vary case-by-case. Provided with specific data, the model can quantify the risk depending on questions of interest.

6. Selected Use Case – State-of-the-Art Research and Potential Research Directions of PTC Cyber Security Risk Management

The objective of this section is to discuss the connected rail aspect of PTC systems that railroads have been implementing nationwide. This section first presents an overview and ConOps for PTC, followed by an overview of the security requirements and threats to PTC, and then an approach for the identification of vulnerabilities and potential cyber attack scenarios by exploiting these vulnerabilities. The research team then illustrate the application of this approach for one specific component, and explore possible mitigation strategies.[1] Finally, this section is concluded with potential future research directions associated with this mitigation approach.

6.1 Overview and ConOps of PTC Systems

American railroads are implementing PTC systems in most railroads and hope to complete implementation by December 2020.[2] Neither Federal law nor regulations specify a particular technical approach for PTC. Railroads have designed and implemented multiple systems to satisfy the safety objectives of the PTC mandate. The most widely adopted systems in the United States are ACSES II, the Incremental Train Control System (ITCS)[3], I-ETMS, and Enhanced Automatic Train Control (EATC).[4]

Regardless of the specific technical approach adopted, all PTC system consists of four major subsystems with their associated communication networks. The first is the WIU network, which provides interface to critical infrastructure, such as switches as well as an interface to the signaling network, and is responsible for communication permissions for trains to occupy track segments and enforce speed limits. The second is the back office network that receives input from the dispatcher for temporary speed restrictions and then delivers them to the train over the data radio network as the train polls for WIU information. The back office network also receives critical information about the train consist and crew from the railroad's information technology systems and provides that to the onboard system. The third network is the onboard system, which receives and processes the information from the wayside and back office, along with state and

[1] It is important to emphasize that this is a **selective** study. An analysis approach can be: i) threat-oriented; ii) asset/impact-oriented; or iii) vulnerability-oriented. Each analysis approach takes into consideration the same risk factors and thus entails the same set of risk assessment activities, albeit in different order. Differences in the starting point of the risk assessment can potentially bias the results, causing some issues not to be identified. The specific approach taken is driven by different organizational considerations (e.g., the quality and quantity of information available with respect to threats, vulnerabilities, and impacts/assets; the specific orientation carrying the highest priority for organizations; availability of analysis tools emphasizing certain orientations; or a combination).

[2] With limited exceptions and exclusions (see 49 CFR §236 Subpart I), PTC is required to be installed and implemented on Class I railroad main lines (i.e., lines with over 5 million gross tons annually) over which any poisonous- or toxic-by-inhalation hazardous materials are transported, and on any railroad's main lines over which regularly scheduled passenger intercity or commuter operations are conducted.

[3] A GPS- and communications-based system used by Amtrak on its Michigan Line, authorized for passenger train speeds up to 110 mph.

[4] A system that uses an underlying automatic train control (ATC) system integrated with underlying cab signal systems (CSS) and centralized traffic control (CTC) systems, used by Capital Metro in Austin, Texas.

status information of the consist. Together these provide the required information necessary for the train to travel in a way that ensures safety requirements have been met.

The specifics of this process are dependent upon the system implemented. For example, in the I-ETMS system all trains must communicate with the back office servers (BOS) every few seconds. This can be done over the data radio system via cell modems on the locomotive. The BOS serves several purposes. First, before each train begins its trip, the engineer must initialize the system by communication to the BOS. The BOS contains information about the engineer and his/her qualifications. If the engineer is not qualified to operate the train, the system will not initialize. Next, the BOS contains the subdivision data files. The engineer enters the train destination and the BOS checks to see if the locomotive has the database onboard for all the track segments that the train will travel over. If the database is missing or if it is not the current version, the BOS will download the correct database to the train.

The BOS interfaces with the dispatching system, allowing the dispatcher to issue train movement authority directly to the train. This includes temporary speed restriction information, roadway worker zone limits and restrictions, highway-rail crossing restrictions, and other movement authorities such as movement in "dark territory" where there is no signal system to govern train movements. A train will initialize with its home railroad BOS. It is required to maintain constant communication with the BOS (every few seconds). If it is routed over another railroad as part of its journey, it will be required to communicate with that railroad's BOS as it approaches its boundary while it is on that railroad.

All railroads utilizing the I-ETMS system, for example, have a BOS.[1] The BOSs are connected over a federated link so that they can pass information among BOSs. This federated link may be privately owned and operated by the railroad, or provided by commercial internet service providers such as AT&T and Verizon. Multiple redundant and diverse communications paths are established between railroads.

The onboard PTC controller assesses information supplied by the two external and one internal networks continuously. If informed about a threat, the PTC controller displays it to the train engineer using a display unit on board the locomotive. This warning indication is provided with sufficient time for the engineer to understand the risk and allow the engineer to control the consist braking. The onboard PTC controller monitors if the engineer/train operator applies brakes. If the engineer does not apply brakes in a timely manner, the PTC controller will automatically do so to control the train speed. One example consequence of not following speed restrictions is the Amtrak Train No.188 derailment in Philadelphia in May 2015. The train was traveling at more than twice of the mandated speed, which caused an overspeed derailment.[2] In systems without automated control, the engineer is obligated to follow operational rules, including adherence to speed limits.

---

[1] This may either be a BOS implemented by the railroad owning the track, a BOS owned by the tenant railroad, or a BOS operated by a third party with contractual service level agreements with the host and/or tenant railroad.

[2] The Amtrak 188 incident was "PTC preventable." PTC was not operational at the time, so the automatic braking enforcement was not possible.

Rail tracks are divided into linear track segments referred as (static) blocks. Under signaled territory, any train is allowed to enter and occupy blocks for a permitted period of time, usually referred to as being granted the movement authority. Movement authority granting is based on the concept that only one train can occupy a single block at one moment of time and travel in a specified direction.[1] In pre-PTC era, these authorities were obtained and granted using voice radios between the operator and the so-called back office staff who operate trains that travel on tracks owned by the same company or, alternatively, using signal aspects from the CTC system. One of the design objectives of PTC is to replace this error prone "read-manual copy readback" voice communication process. This functionality is moved into a fully automated digital computer-to-computer exchange of authorities between the dispatcher and the train crew.

In addition to abiding by movement constraints placed by vehicular dynamics and movement authorities, there are two other significant critical movement constraints:

First are turnouts that open and close pathways when tracks merge or split.[2] Only one track path is allowed to operate through a switch at a moment. To travel through a switch, the train must travel below a specified speed limit, and the last car should exit the safe switching position for clearance.

The second functionality comes from the devices, usually referred to as wayside devices. These are special-purpose sensors placed on the track to detect conditions of the track (e.g., broken rail detectors, track occupancy detectors) or interfaced with the wayside signaling system (e.g., slide fence detectors, high-water detectors and others). Some PTC systems such as ITCS utilize WIUs installed at grade crossing to ensure that approaching trains are operating at an appropriate speed given the activation status of the warning system as detected by the WIU.

The signal system conveys information via light signals and/or cab signals. Most freight railroads employ a radio message system for hot box detectors and dragging equipment detectors. As a train passes the detector, the detector is activated and then a voice radio message is broadcast to the train indicating whether any defects were detected. A message is always broadcast, and the engineer is required to respond. The voice message can be heard by the engineer, other trains in the area, and the dispatcher. If there is a defect, the detector can often tell the engineer which axle or car and what side of the car the defect is from. If there is no defect, the detector will broadcast a message that there are no defects. Figure 6.1-1 provides a full architecture summary of PTC applications in the context of RIoT.

[1] This is a general rule. Under certain operational situations, joint authorities may be issued by the dispatcher.

[2] Turnout refers to the entire assembly: the points, frog, guard rails, all the fixed rails, and the machine; switch refers to the moveable parts only: the points and machine.

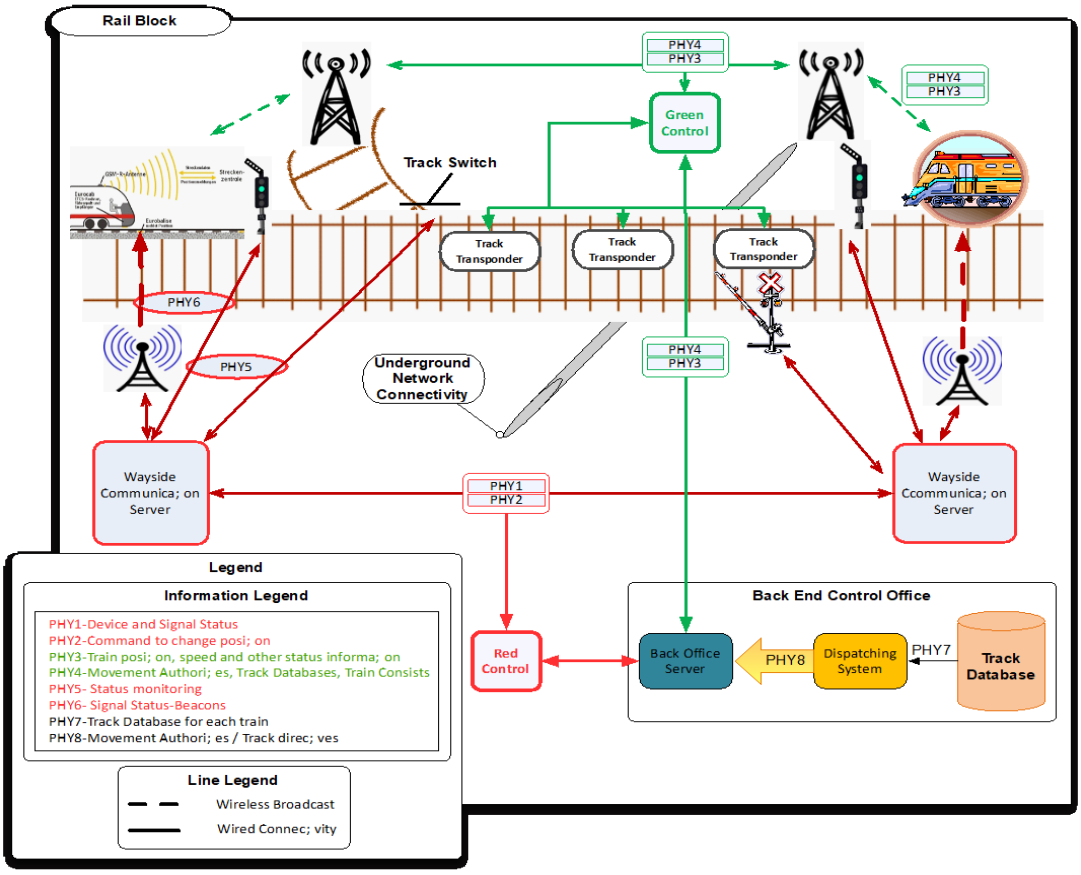


Figure 6.1-1 PTC in the Context of RIoT/Connected Railways

Adapted from R.G. Mark Hartong, and Duminda Wijesekera (2011); Mark Hartong (2012); R.G.a.D.W. Mark Hartong (2011)

6.2 Cyber Security Requirements of PTC Systems

PTC systems are CPSs.[1] Traditionally, cyber security objectives are categorized as confidentiality ("C": that information is shared only with authorized users), integrity ("I": that changes to the information is done by authorized entities only) and availability ("A": that information is available on demand by legitimate entities) of the system. Table 6-1 shows the security objectives required of PTC systems to enable providing the mandated safety objectives (Bandara, Kolli*, et al.*, 2017; Hartong, 2009). However, unlike traditional information technology systems which do not interact strongly with their physical environment, PTC as a CPS places greater emphasis on integrity and availability.[2]

[1] CPS is a generic term for a variety of other control systems (such as SCADA (Supervisory Control and Data Acquisition) systems and ICSs [Industrial Control Systems]) that integrate computational resources, communication capabilities, and sensing to monitor and control physical processes.

[2] In fact, for PTC, there is no mandatory federal regulatory requirement for confidentiality. See 49 CFR §236.1033.

Table 6-1 Cyber Security Requirements and Their Relationship to PTC Safety Mandates

Systems	Security Requirements	Enabled PTC Safety Requirements
Train and onboard system	C, I, A	Speed enforcement + Wayside worker safety
Back office system	C, I, A	Speed enforcement + Wayside worker safety
Dispatching system	C, I, A	Speed enforcement + Wayside worker safety
IT Train scheduler	C, I, A	Speed enforcement + Wayside worker safety
Control system for track movement and switching	C, I, A	Speed enforcement control
Color signal system	I, A	Speed enforcement + Wayside worker safety
Wayside devices	I, A	Speed enforcement + Wayside worker safety
Signaling to locomotive communication	C, I, A	Speed enforcement + Wayside worker safety
Wayside to locomotive radio communication	I, A	Speed enforcement + Wayside worker safety
Transponder/balise system	C, I, A	Speed enforcement
GPS signals	I, A	Speed enforcement + Wayside worker safety
Radio bandwidth	A	Speed enforcement + Wayside worker safety

As seen from Table 6-1, different components of PTC systems have different security requirements. Based on the usage scenarios of these components, potential misuses and their prevention and/or detection methods differ. This section discusses sample requirements from selected components.

6.2.1 Sources of Threats

PTC is a complex, computer-based system of systems (SoS). Increasing safety of train operations, it also increases (cyber) attack surfaces. There are a number of cyber and physical interfaces vulnerable to intrusions from both local and remote adversaries. Threat classification allows detecting, understanding, and evaluating threats in order to propose appropriate security and resilience solutions. This type of classification helps to accurately assess and evaluate cyber threat impacts. It is necessary to shift from reactive methods to systematic proactive methods with consideration of assessing potential cyber threats and taking necessary protection measures against them.

Table 6-2 summarizes the results of the first step of the process as applicable to PTC presented in Section 3. This table identifies the critical threats, attacks, and vulnerabilities that the system designers and implementers must consider when designing PTC subsystems and components.

Table 6-2 PTC Cyber Taxonomy

Threats		Attack		Vulnerability
Threat Origin/Actors	**Threat Type Categories**	**Attack Actions**	**Attack Target**	**Vulnerability Type**
• Individual Attackers • Bot-network Operators • Criminal groups • Foreign Intelligence Services • Insiders • Phishers • Spammers • Spyware/Malware Authors • Terrorists/Industrial Spies • Supply Chain	• Spoofing • Data Tampering • Data Disclosure • Elevation of Privilege • Denial-of-Service	• Probe • Terminate • Scan • Flood • Authenticate • Bypass • Spoof • Eavesdrop • Misdirect • Read/Copy • Execute • Modify • Delete	• Client • Server • Network	• Lack of Availability • Lack of Integrity • Lack of Confidentiality

Given the importance of the railroads as a critical element of the US national infrastructure, the threat can be assumed as being an APT. An APT either directly or indirectly subsumes the capabilities of any of the other potential threat origins with a higher level of capability, motivation and possess *"sophisticated levels of expertise and significant resources allowing it… [to] pursue its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives"* (USEAC, 2017). The architect, engineers, and system implementers can therefore assume that any of the potential threat types, attack scenarios, attack targets, and associated vulnerabilities will be open to potential exploitation and must design and implement the system accordingly. Identification of individual threat origins, while of "interest," is a secondary concern. By assuming the existence of an APT, questions related to threat capability and motivation can be safely ignored.

6.2.2 Use Cases

The preceding defines the required attributes of critical use cases to elicit non-functional requirements that assure PTC continues to perform its mission-essential functions even when under cyber attack. For services that are mission-essential, or that require high or uninterrupted availability, cyber resiliency should be built into the design of PTC systems, subsystems, and components that provide or support those services. Cyber-resilient systems can withstand a cyber attack and can continue to operate even in a degraded or debilitated state carrying out mission-essential functions. Most systems already have some existing resilience features, methods, and requirements to counter unexpected events ranging from extreme weather to operator errors and can be utilized and then expanded to provide resilience against events originating in cyberspace (cyber events).

Figure 6.2-1 graphically shows the usage scenarios and their misuses (i.e., attacks) in term of use cases and misuse cases. The formalized definition of misuse cases presented also adopts the standard Unified Modelling Language (UML 2.0) Use case multiplicities of the actors, mal-actors, use cases, and misuse cases. Multiplicities are marked on the lines indicating the associations.

Figure 6.2-1 also graphically illustrates office/dispatch, wayside, and mobile unit operators as PTC actors in use cases. Potential mal-actors are abstracted to single attackers in misuse cases and show how the misuse cases affect the use cases of Processing Wayside Status Data, Processing Consist Data, and Processing Track Warrant. All actors (including attackers) communicate by exchanging messages via the PTC system. The actual message formats found in the PTC systems are dependent on system design and implementation.

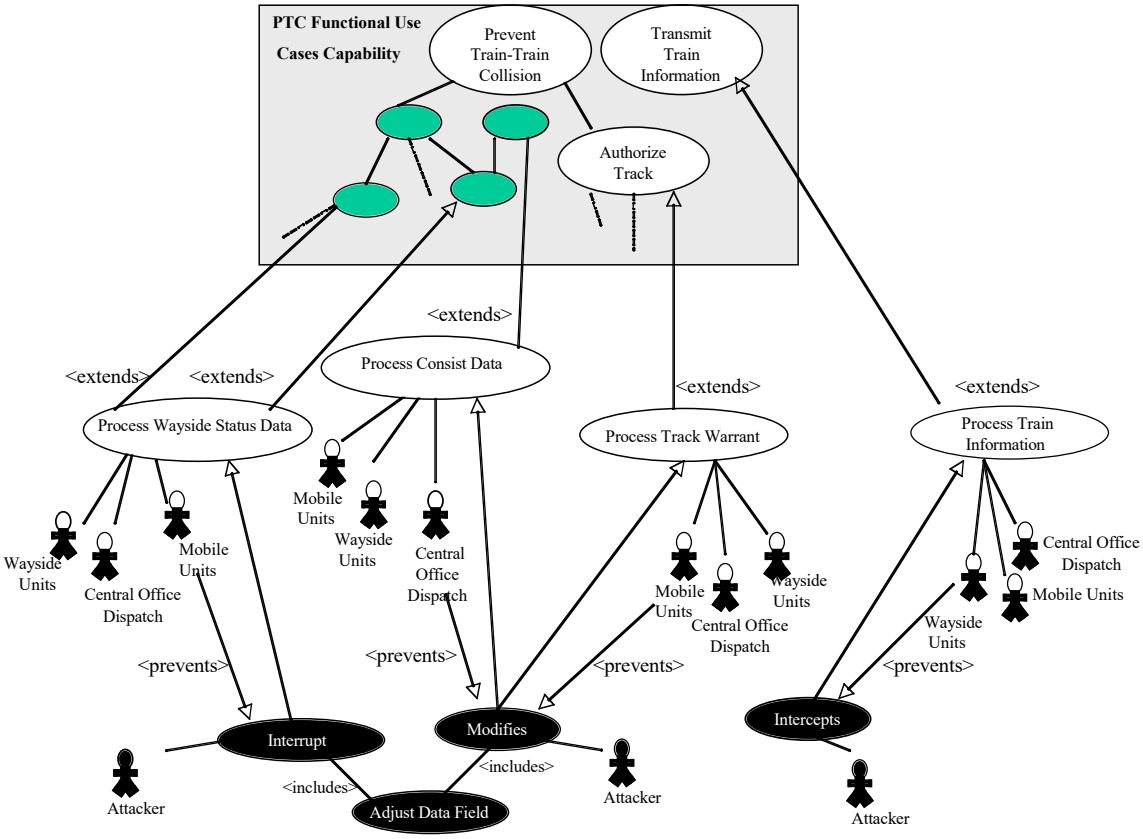


Figure 6.2-1 Use Cases and Misuse Cases for PTC

A secure PTC system ensures that the safety services provided for the various PTC functions are available even in an exploitable communications environment. The repeated applications of use-misuse case analysis to Prevent Train to Train Collision, for example, first yields the traditional aggregate requirements of confidentiality, integrity, availability, authentication, accountability, and identification.

One specific misuse case, representing a specific security breach in a PTC environment, is the Modify Track Warrant, and for this breach, the associations between the actors and mal-actors are graphically represented in Figure 6.2-1. Figure 6.2-1 does not specify all the implications of the misuse case on the Process Track Warrant use case. It is only when all of the associated use

relationships are also graphed, for example Process Track Warrant <<extends>> Authorize Track <<used by>> Prevent Train-Train Collision, that the consequences of the misuse become apparent.

A crucial challenge is to preserve extra-functional properties of individual components when composing the overall architecture. A composition of secure and resilient components should not result in an insecure and brittle architecture. Simply implementing individual cyber defense and resiliency concepts does not guarantee a secure or resilient system. Thus, dependent upon the objectives and the abstraction level, suboptimal elements and constituent systems that integrate synergistically may yield greater security and resilience. Key to this is understanding the boundary for the system and then making appropriate tradeoffs that holistically optimize cyber security in light of the system objectives.

For example, redundancy can work for resilience. Homogenous alternate paths may work well for non-malicious disruptions, but an intelligent adversary gains an advantage from this setup: potential uniformity of attack surface, and thus uniformity of vulnerabilities across the system. Homogeneity makes patching, versioning, and life cycle management easier, thus contributing to baseline threat mitigation. However, a vulnerability, especially a "zero-day" vulnerability, will now be present across the entire system, turning redundant paths and systems into extra vectors. Conversely, increased heterogeneity provides adversaries with more vulnerabilities to target. Furthermore, heterogeneity adds complications to the enterprise and its managers. Thus, system architects must make the tradeoff appropriate to deliver a measured application of heterogeneity across networks and constituent systems for a given context.

Understanding and making these tradeoffs requires clear definition of the system and its potential use cases and contexts, as well as the associated threats and vulnerabilities. Not all assemblies of humans, systems, and objectives necessitate the implementation of all defense and resilience techniques, and adding some or all may not be possible given constraints of cost, time, and subsystem capability. Without first understanding the adversary – system-specific threats (and their rapid agility) – it is difficult, if not impossible, to defend against them. Understanding and modeling the threat becomes a critical prerequisite for developing a resilient architecture. The threat model must consider that vulnerabilities and threats are not static, and that their attacks and behaviors periodically change. Another important factor is that attacks might not only come from outside the system but also from inside. The knowledge that insiders possess often gives them unrestricted access to steal or modify data in the system or to deactivate that system.

To cover all of these potential avenues of attack in cyber, an analysis must address the entire lifecycle of the platform from construction to decommissioning. Questions like the following must be answered for all mission and non-mission states:

- Who has access to the platform and its systems? Depending on the stage in the lifecycle, this can include hardware engineers and software developers, train crew, maintainers and support personnel, visitors, users on networks to which the platform is connected. Anyone with access, i.e., hands-on or remote (network or RF), can potentially tamper with a system in a way that affects its cyber security and resilience.
- What types of access are available? To understand cyber security and resilience, access is not limited to computer networking, e.g., TCP/IP. It must also include electromagnetic access, physical access, supply chain access, and possibly other forms of access. One of

the key results of a cyber security analysis is determining all of the access vectors by which an adversary can exploit the system or have a cyber effect. Moreover, the analysis must identify the types of access inherently available on the platform, as well as potential ways that an adversary can introduce access vectors.

- What vulnerabilities do the various systems have? This is partially answered by the risk management framework (RMF) (NIST, 2018) process, but there are vulnerabilities created as artifacts of design decisions that it does not cover. For example, a broadcast network with no authentication, encryption, or integrity checks does not necessarily violate RMF control requirements, but may offer a number of exploit and attack opportunities to an adversary.
- What effects constitute a "mission kill" or other debilitating effects on the platform? Disabling a system may be one such effect, but the analysis must determine if there are less obvious means of accomplishing the same goal. This must be performed from the adversary's perspective and what they need to accomplish is to reduce/neutralize the effectiveness and threat (to the adversary) of the platform.

The preceding list is by no means comprehensive, but hopefully clarifies the true scope of a cyber analysis. To perform an effective analysis, the team doing so must include not only cyber experts, but operators (crew), maintainers, developers, and whomever else would be affected by the platform not being able to fulfill its mission requirements. Conducting such an analysis is a complex undertaking, requiring consideration of aspects of which include, but are not limited to: the threat space, vulnerabilities, missions/business functions, mission/business processes, enterprise and information security architectures, information technologies, personnel, facilities, supply chain relationships, organizational governance/culture, procurement/acquisition processes, organizational policies/procedures (organizational assumptions, constraints, risk tolerance, and priorities/tradeoffs).

6.3 Sample Vulnerability Analysis and Mitigation

To illustrate the application of the preceding, this study presents an abbreviated analysis and mitigation for a specific component. Security vulnerabilities appear at various stages in the individual component and their system lifecycle.

The onboard PTC system is connected to other multiple systems inside a locomotive:

1. Interfaces to the radio antennas for transmitting and receiving information from the signaling and WIU networks and communicating with the back office server
2. Receiving inputs from the engineer's console and updating status information to the engineer and the conductor
3. Interfaces to multiple braking systems

All these interfaces convey vital information and therefore require cyber security solutions to ensure that they are secure. The main security requirements of these interfaces are message timeliness and non-interference (where integrity, sequencing and non-injection of spurious messages are some of the requirements of non-interference). The most significant kind of misuses against these requirements is interference of communications between the components. These communications happen using internal networks and/or bus structures within a

locomotive. Hence any interfering process (usually referred to as malware) needs to be inserted into the communication link or either end of the link. Although not known publicly in rail sector, such attacks inside vehicular or other control systems are known to happen. As a risk mitigation technique, internal networks can use hashing and/or encryption techniques for internal inter-subsystem communications inside vehicles. Most such communications also use parity bits to identify systems faults that may cause integrity issues. Distinguishing between a fault and an attack is a major issue for time-sensitive inter-system communication. When cryptography is used for securing inter-system communications, the attacking script usually attempts to steal the seeds or the keys used to set up the communications. Some of these communications use known boards and or bus systems that are used in other SCADA-alike systems with their known vulnerabilities and patches against the systems.

Another aspect of onboard processing is the real-time requirement of the onboard executions, as any delay in executing a command may result in delayed enforcement of a safety requirement. As a solution, a real-time operating system such as VxWorks or RTLinux (a preferred source now) used as a base operating system with multiple processors that carry out the same computation and then vote on the final outcome on a per-command basis. These systems are subjected to the same software vulnerabilities that are found in normal computing systems such as buffer overflow attacks, heap-spray, and stack manipulation attacks – in addition to lower layer hardware attacks. While most of these attacks have known mitigation techniques that can be applied during the software development lifecycle, they do not preclude the possibilities of zero-day attacks[1] arising from an inherent flaw in the software code or in the way a piece of software interacts with other software that is yet to be discovered.

6.3.1 Wayside Interface Units

Wayside interface networks connect WIUs to either a server[2] or directly to a transmitting radio to broadcast the status of the wayside. WIUs are usually placed in a signal cabinet, bungalow, or a signal case, and interface with track circuits to detect the presence of a train, position of switches, inputs from other trackside sensors, and aspects of signal system so that the onboard computer can enforce compliance with the signal. It also monitors other information that may be required.

One design objective of PTC is to provide wayside information. In I-ETMS and ITCS, this is accomplished in the form of radio signals using a network of SDRs. The WIU broadcasting transmissions are expected to provide authenticity and integrity, but not confidentiality. To provide authenticity and integrity, WIU broadcast messages are transmitted with a limited

[1] A zero-day attack (also referred to as “day zero”) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of or had insufficient time to address.

[2] The server aggregates the inputs from one or more individual WIUs for communication to the dispatch office, or conversely disseminates inputs from the dispatch office to one or more WIUs.

lifespan[1] and a hash that covers the message content. In addition, some WIUs also provide a request response transmission from the trains.

6.3.2 Wayside Interface Unit Vulnerability

A replay, message corruption, or guessing attack on the WIU beacon could result in trains stopping when it should not be due to the fail-safe nature of the onboard system design. Similarly, these attacks on a WIU could result in a train failing to stop when it should.[2]

One of the sample vulnerabilities is the use of a 32-bit SHA-1 HMAC algorithm that is specified by an I-ETMS wayside message. The HMAC field is used to detect any tampering attempts. It further uses a 4-bit time stamp to avoid replay attacks. But since the HMAC is unseeded and the 4-bit time stamp repeats every 16 seconds (i.e., because the range of the time stamp is from 0000(0) to 1111(15)), an attacker can replay a status message every second until it matches with the correct time stamp. For example, when the train is expecting a WIU message, a WIU message with a FAULTY status would normally result in stopping the train. If, however, an attacker can replay an earlier message with NO-FAULT status, the attacker can cause the train to fail to stop in time.

The second kind of attack would be a bandwidth exhaustion (including jamming) attack or a lack of sufficient radio bandwidth in the 220 MHz spectrum allocated to PTC radio.

6.3.3 Mitigation Strategies

There is a limited amount of space provided for the WIU packets in I-ETMS. Therefore, in order to provide comparable security using the same space, one possible approach is using an enhanced hash key schema (instead of a static hash key) and a PTC specific IDS to detect potentially malicious packets received through the radio system. Another functionality provided by the cryptographic cognitive engine is analyzing threats to the radio spectrum. Figure 6.3-1 shows the threat detection procedure of the current threat module. This study's threat analysis module uses the CRC and hash validation to identify attacks. For each message, the threat analysis module checks the CRC and the hash value. If both the CRC and the hash values are correct, the message is identified as a correct message. If either the CRC or the hash value is incorrect, it checks the message with the previous messages to determine a potential for a replay attack.

[1] The lifespan policy establishes a contract for the amount of time allowed between messages. For subscribers, it establishes the maximum amount of time allowed to pass between receiving messages. For publishers, it establishes the maximum amount of time allowed to pass between sending messages.

[2] The consequences of such a successful attack could range from merely annoying (delay of the train) to catastrophic (collision, derailment).

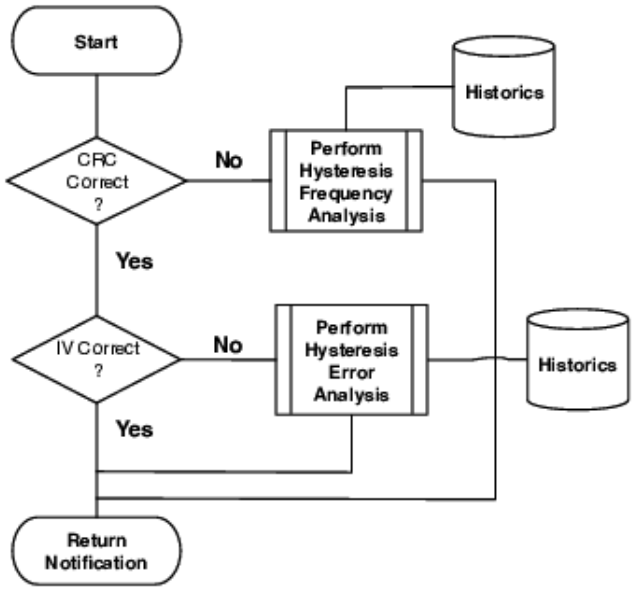


Figure 6.3-1 Threat Detection Process of Current Module

Enhanced Hashing Technologies

Changing the seed of the hash function frequently can minimize the replay attack. Researchers have done so by using an extension to the TESLA protocol (Perrig *et al.*, 2002). The original TESLA protocol generates a chain of keys using a forward hash algorithm and the keys are used in the backward direction. This protocol is enhanced in this study's work, as shown in Algorithm 1. The enhanced TESLA algorithm changes both the seed and the hash generation algorithm randomly with the time.

1. $Signal_{Net} \rightarrow WIU, Loco : \{MAC | Algo_{PRN} | t_{int}\}$
2. $WIU., Loco.$: Divides Total Communication Time t_{int}
3. $WIU., Loco : K_i, Algo \rightarrow t_{int}$
   Assign a Key K_i and Algorithm to each time interval t_{int}
4. $Loco \rightarrow WIU : \{t_{loco}\}$
5. $WIU \rightarrow Loco : \{t_{WIU}\}$
6. $WIU., Loco.$: Calculates Δ
7. $WIU \rightarrow Loco : \{Message\}$
   At this point messages are being transmitted and verified with K_i. The Wayside Interface Unit (WIU) and the Locomotive rotates integrity algorithms and Keys K_i without disclosure.
8. $WIU, Loco. : MAC_{new} = hash(Seed_1 \oplus Seed_n)$
   A new MAC is generated for continuous communications. The new MAC is then used to create new salts

Algorithm 1 Enhanced TESLA for Secure WIU Broadcast to the Locomotive

One can use Algorithm 1 twice and produce two hashes, say $Hash_{app}$ and $Hash_{phy}$ to be used at the application layer (i.e., on the data packet) and to watermark the radio stream at the physical layer, respectively.

Attack Detection Technologies

Type 1 – Replay Attack Detection

In a replay attack, the attacker captures a previously sent message and then transmits it to the intended receiver. According to the original PTC specification, it is difficult to detect a replay attack because of the usage of a static salt value for the hash function. Because in the proposed cognitive radio architecture, one changes the cryptographic seed value with time, the replay attempts can be identified more efficiently.

$$ReplayDetected : (CRC = VALID)\&(hash = INVALID)\& \\ M_{OldTimestamp}\&(M = SyntacticallyCorrect)$$

Equation 1

As shown in Equation 1, a message is identified as a potential replay if the message is syntactically correct and has a valid CRC value, but the hash value does not match the hash value corresponding to the key that the system uses at the time of message reception. Further, one can check the timestamp of the message to verify that the message is generated at an earlier time.

Type 2 – Message Corruption Detection

In the message corruption attack, the attacker captures a message, changes and transmits it back to the intended recipient. If the attacker does not do it in an intelligent way, this will lead to CRC corruption.

$$MessageCorruption : (CRC = INVALID)\&(hash = IN|VALID) \\ \&Current|OldTimestamp\&(M = Corrupted)$$

Equation 2

As shown in Equation 2, the message corruption is detected by an invalid CRC. The current message corruption detection algorithm does not have sufficient intelligence to distinguish between intentional and unintentional message corruption.

Type 3 – Guessing Attack Detection

A message-guessing attacker is more complex than the previous situations. One can assume that such an attacker has information about the key generation algorithms, but does not have the initial seed value to generate the key chain. Therefore, the attacker guesses the initial key, generates key chains, and transmits messages. Because the attacker has the knowledge about all the algorithms, she or he can generate a syntactically correct message. But since the cryptographic cognitive engine changes the keys frequently, it is difficult for the attacker to guess the key used at that time period. This will lead to hash failures. The logic used to detect this kind of attacks are shown in Equation 3.

$$MessageCorruption : CRC = VALID \& IV = INVALID \\ \& CurrentTimestamp \& M = SyntacticallyCorrect$$

Equation 3

Key Management

At startup, the cryptographic seeds for hash generation are loaded to the train database. When a train approaches a WIU or a control point, it uses the corresponding seed that is recognized using identification of the WIU or the control point. This behavior is illustrated in Algorithm 2. If the pre-loaded seed values are compromised for a particular WIU or control point, the new seed value is generated as shown in Algorithm 3. In this scenario, the back office will generate an emergency seed value, encrypted by a back office private key associated with the specific WIU or geographical region, and transmit it to the compromised entity. Once an emergency rekey event is securely broadcasted using the signaling network, the public key is sent to locomotive to decrypt the message authentication code (MAC). In the normal activation of a MAC for a particular WIU, the following message exchanges shown in Algorithm 2 are expected.

Locomotive (L) enters the block and performs a GetWIUStatus Request (G) or Timed Beacon Request (T)for a Beacon (B) and sends a message (M) and Status (S).

a. $L \rightarrow B : \{CRC | IV_{Algo,Salt} | M\{G,T | WIU_{ID}\}\}$
   The WIU_{ID} is used internal by the Locomotive to lookup the MAC
b. $B \rightarrow L : \{CRC | IV_{Algo,Salt} | M\{S\}\}$
   The WIU has its MAC provided to it from the Signaling network

Algorithm 2 Normal Protocol Exchange: GetWIUStatus

a. $S \rightarrow L : \{CRC | IV | R\{WIU_{ID} | WIU_{PublicKey} | Time_{Activate}\}\}$
   The Signaling network sends the Locomotive the specific WIU to rekey as well ad the public key to decrypt the encrypted MAC and the activation time to start using the salts.
b. $S \rightarrow B : \{CRC | IV | \{M\{Salts | Times\}\}$
   The Signaling Network sends the Beacon the salts and times associated with the salts.
c. $L \rightarrow S : \{CRC | IV | \{M\{Time_{Activated}\}\}$
   The Locomotive sends the signaling network that the MAC has been activated at the exact time according to the Locomotive.
d. $S \rightarrow B : \{CRC | IV | \{M\{Time_{L_{Activated}}\}\}$
   The Signaling network sends the Locomotive activation time to the beacon.

Algorithm 3 Emergency Reseed Event

6.4 Potential Research Directions

6.4.1 Dynamic Spectrum Management

The ACSES system uses spectrum in the 217 to 219 MHz band. Amtrak operates in the 217 MHz band and some of the commuter railroads operate in the 218 MHz band. Filters are utilized to prevent interference from the I-ETMS band of frequencies since I-ETMS operates at higher power levels and constantly communicates with the BOS. ACSES trains only communicate over

these RF frequencies with the WIU as they approach an interlocking to obtain information from the WIU at the interlocking. The train also obtains temporary speed restriction (TSR) information as it communicates with the WIU. The TSR server downloads any TSRs in the next three track blocks[1] ahead each time a train approaches an interlocking. They poll the WIU every 6 seconds. Upon initial contact with the base radio at the WIU location, the train is assigned with a time slot by the base radio to prevent collisions with other transmissions by other trains. Once a train passes the interlocking, the radio goes silent until it approaches the next interlocking. The WIU only transmits information when requested by an approaching train. In the I-ETMS architecture, WIUs beacon information all the time[2], not just when being approached by a train equipped with the I-ETMS system.

American railroads are allocated the spectrum from 217 MHz–219 MHz (for the uplink) and 221 MHz–222 MHz (for the downlink) to operate PTC. In addition to the 220 MHz spectrum, railroads also can use 160 MHz and 900 MHz ranges as assigned by FCC. This bandwidth should be properly shared between the WIU network and the signaling network. With the limited bandwidth availability, proper channel management architecture is required to adequately handle trains. Improper management of channels can lead to interference between allocated channels. Interference will decrease the signal-to-noise ratio (SNR) in the received signal and increase the bit error rate (BER). The information contained in the packets can be distorted. Therefore, improper channel management introduces a higher risk to train operations. Denying spectrum to train communications and/or creating jamming signals are a major security threat to PTC communication. In addition, creating incorrect unauthenticated messages also causes potential safety hazards for PTC operations.

One of the major cyber security objectives of spectrum access is availability. One of the enabling techniques for provisioning spectrum access is proper cell planning and dynamic access to available spectrum.

Problem: The problem addressed in this section is to find a safe and secure way of optimally using the limited bandwidth available for railroads. Given that the rail traffic is mixed (i.e., high-speed but shorter passenger trains and lower-speed but longer freight trains have to use the same spectrum. Some areas, such as the Northeast Corridor, San Francisco Bay area and Chicago area, have known spectrum shortages (Vieira *et al.*, 2018); bandwidth utility must be maximized for a wide variety of traffic. In addition, given that radio transmissions are exposed to any receiver, the possibility of a cyber attack is not trivial.

Outcome: George Mason University previously designed a cognitive radio network (Bandara, Kolli*, et al.*, 2017) that runs over the Meterorcomm's SDR network, which provides intelligent spectrum usage and cyber security against potential attacks in a way that addresses the moving target of strengthening the cyber security in anticipation of enhancing attacker capabilities. The developed dynamic spectrum management would include dynamic channel allocation, using extra bandwidths available from the 160 MHz and 900 MHz ranges based on need, and dynamic

[1] A design implementation decision.

[2] Beaconing is the continuous, repeated broadcasting of a radio signal containing identifier and associated system information.

modulation that packs a varying number of symbols to a radio wave (to avoid interference and jamming), and dynamic power adjustment.

Benefits: The design enhancement proposed here, if implemented, would solve two main issues of dynamic bandwidth allocation, whereby trains in need will get their bandwidth based on their individual needs (as opposed to a one-size-fits-all solution), and also address cyber security issues at the application layer (i.e., data packet) as well as the physical layer.

Given the diversity and variability of train schedules and the complexity of track geometries, a variable amount of spectrum is required in a timely manner to provide designed-in safety objectives of PTC. To do this, the intelligence has to be built to the radio network. In addition to efficient spectrum sharing, this cognitive radio will also detect spectrum abuse, any potential cyber threats to PTC operations and improve security of radio communication between the PTC nodes.

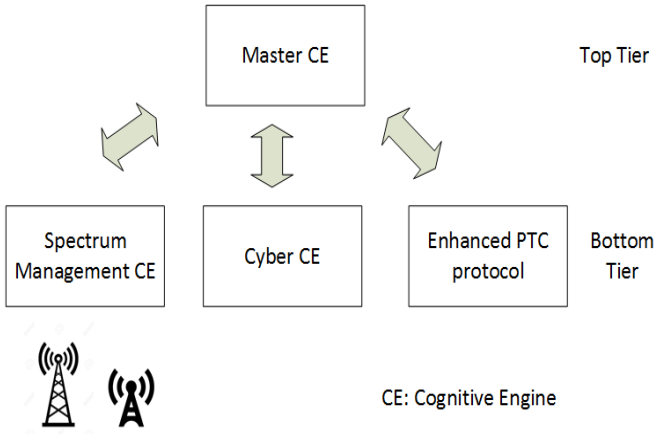


Figure 6.4-1 Internal Architecture of a Cognitive Radio

Adapted from Bandara and Kolli, et al. (2017)

As shown in Figure 6.4-1, each cognitive radio in the proposed network is designed to have two tiers. The bottom tier consists of sub-cognitive engines designed for spectrum management and cyber security management. The spectrum management cognitive engine is responsible for measuring the deviations of SNR and BER, and informs it to the top-tier master cognitive engine. Based on the decisions of the master cognitive engine, the spectrum management cognitive engine changes the frequency, power, and modulation schemas dynamically. The cyber cognitive engine is responsible for ensuring the communications between the PTC entities are secure. To do so, this sub-engine changes cryptographic keys periodically to protect the broadcast messages from malicious attacks and analyzes messages to detect any potential impostures. If it detects suspicious activities, it will report it to the master cognitive engine that holistically evaluates the operational risk, decides actions to mitigate them, and communicates them to the bottom tiers. The master cognitive engine considers the Doppler effect, the environmental conditions (e.g., precipitation, foliage), and multi-path effects with historical information when making decisions. In addition, the master cognitive engine shares appropriate information among peers. Taking together these cognitive radios creates a radio-based IDS for PTC systems.

6.4.2 Cell Planning for WIUs

If trains do not operate regularly in a route, the WIUs can operate in *on demand* mode. When the WIU is operating in *on demand* mode, an approaching train has to request the device status from the WIU. Upon receipt of a request, the WIU starts beaconing until a pre-set timer expires. Therefore, a WIU operating in *on demand* mode requires an extra channel for receiving the beacon request message. Because the beacon request messages are not sent very regularly, one assumes that it is reasonable to have one channel for all the WIUs.

Channels should be allocated for wayside devices so that co-channel and adjacent channel interference is avoided. To do so, one could potentially divide the channels allocated for the WIU network into two groups. Then, the system connects wayside interface units located very close to a single transmitter to transmit the status of these devices using more than one channel. This will allow the transmitter to use fewer channels to transmit the status of many wayside devices, and hop between the frequencies among the allocated channels to avoid interference. To do so, the research team clusters the transmitters along the route based on the distance and assign frequencies from one set to one cluster interchangeably. This is done in a way similar to how channels are allocated for CPs, but based on the number of wayside devices located in a region. Therefore, the wayside unit clusters and the control point location can be independent of each other.

Table 6-3 Summary of Intended Solutions and Corresponding Features

Requirements	Solution	Limitations	Possible improvements
Improve throughput Noise immunity	SIRT: Dynamic modulation change	Three modulation schemes; modulation oscillation (18dB–35dB), synchronization difficulties at higher modulations	Hardware-level spectrum measurements, add more higher-level modulations – may require to redesign the sync algorithms
Jamming immunity	SIRT: Frequency hoping	Channel-specific jamming	Hardware-level spectrum measurements
Cyber threat withstanding	SIRT: Integrity validation and threat detection	Require more precise timing.	
Congestion management	SIRT: Dynamic channel allocation, comprehensive frequency analysis, WIU network planning	Does not consider the type of WIU into account.	Add more details to WIU cell planning.

6.4.3 Practical Challenges in Incorporating Proposed Bandwidth Management Enhancements

If the proposed use of a 160 MHz or 900 MHz spectrum for PTC purposes (to supplement or replace existing PTC-related 220 MHz spectrum) is the case, the following challenges have to be addressed:

1. Utilization of the railroad allocated frequencies within these bands is currently high, with the trend to further increase this utilization over time. In many U.S. metropolitan areas, there currently is very little unused railroad allocated spectrum available, if any, in these bands.
2. Given (1) above, adding railroad users to this band will very likely require obtaining of additional spectrum. From past experiences, even when the railroads act as a single entity (e.g., PTC 220 LLC), this process has proven to be both time-consuming and expensive.
3. The propagation properties of 900 MHz compare unfavorably to 220 MHz. Therefore, if 900 MHz were to be used for PTC purposes, additional transmitter sites would very likely be needed to match PTC coverage currently being provided in the 220 MHz band.
4. When adding transmitter frequencies in a given area (such as on the roof of a locomotive), special consideration must be given to matters such as receiver de-sensing, as well as mitigating any type of RF interference that might have been created by these additions. Use of any new frequencies (including 900 MHz) would require testing to determine what measures would be required (if any) to ensure continued reliability of all the systems which utilize transmitters located on the locomotive. Measures would likely include items such as use of filters along with new antenna designs/configurations and orientations.

6.5 Conclusion of PTC Research Review

In summary, academic research on extending cognitive radios for PTC has suggested several enhancements that could address several envisioned PTC cyber security-related issues.

Many railroads and their suppliers are proposing newer techniques to cyber-strengthen the systems that are being proposed and mostly implemented. Each new testing and analysis stage continues to bring in new additions that could strengthen and secure the system against failures and potential attacks. Given the progress of the PTC enforcement and trial runs, no publicly disclosed cyber incidents have been reported by the rail industry at the time of writing this report.

One possible direction that may be taken further to advance PTC systems is to migrate the PTC signaling systems into 5G-based communications (as being considered in the vehicle-to-everything, i.e., V2X systems). This will address some limitations of the allocated bandwidth for PTC. The disadvantage of this is that the radio system being prototyped will need to replace existing QPSK-based modulations by GFDM modulations. Given that the majority of the PTC

radios are software defined, it may not require substantial changes, but it may be cost prohibitive.[1]

[1] Costs include, but are not limited to design, implementation, acquisition, testing, certification, installation, and maintenance of the new software; training and associated personnel costs; configuration management; and control costs.

7. Conclusion

Each RIoT application may have its own security loopholes and breach points, which require specific risk management strategies. The proposed methodology recommends a streamlined procedure for conducting cyber security risk assessment for each specific use case. This report selects three representative use cases to demonstrate the application of the risk methodology. These use cases include ATCS, remote controlled movable rail bridges, and PTC. The following sub-sections include some primary findings and conclusions for each use case.

7.1 ATCS

The ATCS radio code line system is widely adopted over North American railroads. The multi-layer, fail-safe design over the ATCS-related systems can prevent most unsafe train movements and thus catastrophic collisions. However, this research identified one potential safety risk case over the ATCS radio code line system, as explained in the Blue Block case scenario. Such risk is minimized by safeguards that are currently incorporated into the design of ATCS communications between the base station and wayside locations, and further augmented by the fact that current designs provide visibility at the back office when unknown factors prevent normal ATCS communication interactions. Since the introduction to PTC technologies, upgrading the legacy ATCS network for better security is no longer deemed as cost-effective. Although the ATCS-targeted attack precedents were rare in the past and could be minimized by its original design, the authors still recommend attention to this potential risk source and ensure that multiple operational verifications are required besides the sole dependency on the ATCS system itself. As for denial-of-service (DoS) attacks (another identified non-safety risk), better resource allocation is needed for optimal counteractions, such as radio channel monitoring and protection, workforce of communication and signaling (C&S) maintenance, flexibility of operation plans, etc.

7.2 Remote-Controlled Movable Rail Bridges

An analysis of a fail-safe movable bridge system led to several general conclusions regarding its safety and security risks. A computer simulation model has been developed, which can support "what-if" scenario analysis, the identification of a critical fault path, and a security path. Also, the model could be used to probabilistically differentiate between a fault and a cyber attack if the cause is not immediately known. It is also noteworthy that bridge designs vary case-by-case. Provided with specific data, the model can quantify the risk depending on questions of interest.

7.3 PTC

PTC has evolved over the last 15 years. Many railroads and suppliers are proposing or developing advanced technologies to further secure current PTC systems. One potential future research area on this subject is pointed out: considering the migration from the PTC signaling systems into 5G-based communication systems (as being considered in the vehicle-to-everything, i.e., V2X systems). This will address the limitations of the allocated bandwidth for PTC. The disadvantage of this approach is that the prototyped radio system will need to replace existing QPSK-based modulations with GFDM modulations.

7.4 Epilogue

It is practically impossible to draw a universal conclusion over cyber security vulnerability and profile for all possible systems in the U.S. Instead, use-case-specific risk analysis built upon a consistent methodological framework could be helpful for government, academia, and industry to work collaboratively to manage the cyber security risk associated with connected railroad technologies.

8. References

AAR. (1997). American Railroad Association Manual for railway Engineering, latest ed. Washington, DC.

AAR. (2005). Manual of Standards and Recommended Practices Section K-II: Railway Electronics. Washington, DC.

Abrahams, M. (2000). Bridge Engineering Handbook. Ed. Wai-Fah Chen and Lian Duan. Boca Raton: CRC Press.

Abrahams, M. (2000). Movable bridges. In e. B. R. W.-F. Chen and L. Duan, FL. (Eds.), Bridge Engineering Handbook, 1–26.

Adin, I., Mendizabal, J., & del Portillo, J. (2012). Impact of electromagnetic environment on reliability assessment for railway signalling systems. Railway Safety, Reliability, and Security: Technologies and Systems Engineering: *Technologies and Systems Engineering,* 151.

Aissa, M. J. L. B. A. R. A. B. (2014). Classification of Security Threats in Information Systems. Paper presented at the 5th International Conference on Ambient Systems, Networks and Technologies.

AlEroud, A., & Karabatis, G. (2012). A contextual anomaly detection approach to discover zero-day attacks. Paper presented at the Cyber Security (CyberSecurity), 2012 International Conference on.

Alnifie, G., & Simon, R. (2007). A Multi-channel Defense Against Jamming Attacks in Wireless Sensor Networks. Paper presented at the Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, Chania, Crete Island, Greece.

Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013). Cyber security of Water SCADA systems Part 1: Analysis and Experimentation of Stealthy Deception Attacks. *IEEE Transactions on Control Systems Technology, 21*(5), 1963–1970.

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). Scalable, graph-based network vulnerability analysis. Paper presented at the Proceedings of the 9th ACM Conference on Computer and Communications Security.

Andre'B, A. (2014). Combining operational and spectrum characteristics to form a risk model for positive train control communications. George Mason University,

Apostol, K. (2012). Brute-force attack.

Arnold, F., Belinfante, A., Van der Berg, F., Guck, D., & Stoelinga, M. (2013). DFTC alc: a tool for efficient fault tree analysis. Paper presented at the International Conference on Computer Safety, Reliability, and Security.

Baker, G. (Producer). (2019, July 26). Schoolboy Hacks into City's Tram System. The Telegraph.

Baklouti, A., Nguyen, N., Choley, J.-Y., Mhenni, F., and Mlika, A. (2017). Free and Open Source Fault Tree Analysis Tools Survey. Systems Conference (SysCon), 2017 Annual IEEE International, IEEE, 1–8.

Baldini, G., Fovino, I. N., Masera, M., Luise, M., Pellegrini, V., Bagagli, E., . . . Senesi, F. (2010). An early warning system for detecting GSM-R wireless interference in the high-speed railway infrastructure. *International Journal of Critical Infrastructure Protection, 3*(3-4), 140-156.

Bandara, K. R. D. S., Kolli, S., & Wijesekara, D. (2017). Secure Intelligent Radio for Trains (SIRT). Paper presented at the 2017 Joint Rail Conference.

Bandara, K. R. D. S., Melaragno, A., Wijesekera, D., & Costa, P. (2017). A Case Study of Cognitive Radio Networks: Secure Spectrum Management for Positive Train Control Operations. Spectrum Access and Management for Cognitive Radio Networks, 121-152. doi:10.1007/978-981-10-2254-8_5

Bandara, K. R. D. S., Melaragno, A. P., Wijesekara, D., & Costa, P. (2016). Multi-Tiered Cognitive Radio Network for Positive Train Control Operations. *Proceedings of the Asme Joint Rail Conference*.

Bantin, C., & Siu, J. (2011). Designing a secure data communications system for automatic train control. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 225*(4), 395-402.

Bardsley, R. E. a. M. (2002). Electrical reliability analysis for transit applications. ASME/IEEE Joint Railroad Conference, 81–86.

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1.

Bastow, M. D. (2014). Cyber security of the railway signalling & control system. Paper presented at the 9th IET International Conference on System Safety and Cyber Security, Manchester, UK.

Baumeister, T. (2010). Literature Review on Smart Grid Cyber Security.

Bayuk, J. L., & Mostashari, A. (2011). Measuring cyber security in intelligent urban infrastructure systems. Paper presented at the Emerging Technologies for a Smarter World (CEWIT), 2011 8th International Conference & Expo.

BBC (Producer). (2010). Swing bridge reopens in Whitby after gearbox failure.

Bezzateev, S., Voloshina, N., & Sankin, P. (2013). Joint safety and security analysis for complex systems. Paper presented at 13th Conference of FRUCT (Finnish–Russian University Cooperation in Telecommunications) Association.

Bhattacharya, S., & Başar, T. (2010). Game-theoretic analysis of an aerial jamming attack on a UAV communication network. Paper presented at the American Control Conference (ACC), 2010.

Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*.

Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. Paper presented at the International Conference on Reliability, Safety and Security of Railway Systems.

Bloomfield, R., Bloomfield, R., Gashi, I., & Stroud, R. (2012). How secure is ERTMS? Paper presented at the International Conference on Computer Safety, Reliability, and Security.

Bondavalli, A., Ceccarelli, A., Grønbæk, J., Iovino, D., Kárná, L., Klapka, Š., . . . Salzo, A. (2009). Design and Evaluation of a Safe Driver Machine Interface. *International Journal of Performability Engineering, 5*(2).

Boudali, H., Crouzen, P., & Stoelinga, M. (2007). Dynamic fault tree analysis using input/output interactive markov chains. Paper presented at the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.

Bouissou, L. P. t.-C. d. s. a. M. (2010). Modeling Safety and Security Interdependencies with BDMP (Boolean Logic Driven Markov Processes). Paper presented at the 2010 IEEE International Conference on Systems, Man and Cybernetics.

Boyd, M. A. (1992). Dynamic fault tree models: Techniques for analysis of advanced fault tolerant computer systems (Doctoral dissertation). University of North Carolina.
Bridge Lighting and Other Signals, 33 CFR § 118 (1986).
Burgett, M. J. (2016). The Engineering Basics of CTC. Retrieved from http://www.ctcparts.com/about.htm
CBC (Producer). (2017). Delays at Swing Bridge in Little Current Due to Repairs.
Chang, S.-Y., Cai, S., Seo, H., & Hu, Y.-C. (2016). Key Update at Train Stations: Two-Layer Dynamic Key Update Scheme for Secure Train Communications. Paper presented at the International Conference on Security and Privacy in Communication Systems.
Chang, S.-Y., Tran, B. A. N., Hu, Y.-C., & Jones, D. L. (2015). Jamming with power boost: leaky waveguide vulnerability in train systems. Paper presented at the Parallel and Distributed Systems (ICPADS), 2015 IEEE 21st International Conference on.
Chaux, P.-Y., Roussel, J.-M., Lesage, J.-J., Deleuze, G., & Bouissou, M. (2013). Towards a unified definition of minimal cut sequences. *IFAC Proceedings 46*(22), 1-6.
Cheminod, M., Durante, M., & Valenzano, A. (2018). Review of Security Issues in Industrial Networks. IEEE Transactions on Industrial Informatics, 9(1), 277-293.
Chen, B., Schmittner, C., Ma, Z., Temple, W. G., Dong, X., Jones, D. L., & Sanders, W. H. (2014). Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective. Paper presented at the International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands.
Chen, L.-j., Shan, Z.-y., Tang, T., & Liu, H.-j. (2011). Performance analysis and verification of safety communication protocol in train control system. *Computer Standards & Interfaces, 33*(5), 505-518.
Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A Review of Cyber Security Risk Assessment Methods for SCADA Systems. *Computers & Security, 56,* 1-27.
Chernov, A. V., Butakova, M. A., & Karpenko, E. V. (2015). Security incident detection technique for multilevel intelligent control systems on railway transport in Russia. Paper presented at the Telecommunications Forum Telfor (TELFOR), 2015 23rd.
Cho, J.-S., Yeo, S.-S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer Communications, 34*(3), 391-397.
Chothia, T., Ordean, M., de Ruiter, J., & Thomas, R. J. (2017). An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*.
Chu, P. C., & Beasley, J. E. (1998). A genetic algorithm for the multidimensional knapsack problem. *Journal of Heuristics, 4*(1), 63-86.
CNSS. (2015). Committee on National Security Systems (CNSS) Glossary.
Coast Guard, Department of Homeland Security, 33 CFR § 1, (1986).
Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. *Proceedings of the 39th Annual Hawaii International Conference*.
ConnDOT. (2014). Connecticut DOT Br. No. 04288r Walk Bridge over Norwalk River.
Cook, W. (2013). Bridge failure rates, consequences, and predictive trends.
Corp., N. S. (Producer). (2010, June 07). Norfolk Southern and GE Announce Success of Breakthrough Technology To Help Railroads Move Freight Faster and Smarter.

Craven, P. V. (2004). A brief look at railroad communication vulnerabilities. *Proceedings of the 7th International IEEE Conference*.
Craven, P. V. (2008). Architecture of an ATCS Network Simulator. Paper presented at the 2008 IEEE International Conference on Electro/Information Technology.
Craven, P. V., & Craven, S. (2005). Security of ATCS Wireless Railway Communications. *Proceedings of JRC 2005,* Pueblo, CO.
Czescik, R., & Siemianowski, T. (2014). "Invisible" Threats to the Railway Infrastructure-an Attempted Analysis. *Internal Security, 6*(1), 71.
Dablain, K. (2017). Cyber Threats Against Critical Infrastructures in Railroads. Utica College,
David, A., Larsen, K. G., Legay, A., Mikučionis, M., & Poulsen, D. (2015a). Uppaal SMC tutorial. *International Journal on Software Tools for Technology Transfer, 17*(4), 397-415.
David, A., Larsen, K. G., Legay, A., Mikučionis, M., & Poulsen, D. (2015b). *Uppaal SMC Tutorial, 17*(4), 397-415.
de Ruiter, J., Thomas, R. J., & Chothia, T. (2016). A formal security analysis of ERTMS train to trackside protocols. Paper presented at the International Conference on Reliability, Safety and Security of Railway Systems.
Dingler, M. H., Lai, Y.-C. R., & Barkan, C. P. L. (2009). Impact of Train Type Heterogeneity on Single-Track Railway Capacity. *Transportation Research Record: Journal of the Transportation Research Board, 2117*(1), 41-49.
Douthit, H. (1988). The Use and Effectiveness of Sabotage As a Means of Unconventional Warfare: An Historical Perspective From World War I Through Viet Nam. (M.S.), School of Systems and Logistics, Air Force Institute of Technology, Wright Patterson Air Force Base, Dayton, OH.
Drago, A., Marrone, S., Mazzocca, N., Tedesco, A., & Vitto, V. (2013). Model-Driven Estimation of Distributed Vulnerability in Complex Railway Networks. Paper presented at the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, Vietri sul Mere, Italy.
Du, S., Li, X., Du, J., & Zhu, H. (2014). An attack-and-defence game for security assessment in vehicular ad hoc networks. *Peer-to-Peer Networking and Applications, 7*(3), 215-228.
Elliot, S. (2013). Hierarchical state machines in the automation process.
ENISA (Producer). (2004). European Union Agency for Cybersecurity (ENISA).
Ericson, C. A. (1999). Fault tree analysis. Paper presented at the System Safety Conference, Orlando, Florida.
F-Secure. (2014). BLACKENERGY & QUEDAGH: The Convergence of Crimeware and APT Attacks. Helsinki, Finland.
Feuser, J., & Peleska, J. (2010). Security in Open Model Software with Hardware Virtualisation–The Railway Control System Perspective. Electronic Communications of the EASST, 33.
FHWA. (1992). Systems Engineering for Intelligent Transportation Systems. What is Systems Engineering?
Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86,* 13-23.
Fink, G., Best, D., Manz, D., Popovsky, V., & Endicott-Popovsky, B. (2013). Gamification for measuring cyber security situational awareness. Paper presented at the International Conference on Augmented Cognition.

Flammini, F., Marrone, S., Mazzocca, N., & Vittorini, V. (2006). Modelling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks. Paper presented at the Proc. European Safety and Reliability Conference, ESREL.

Fovino, I. N., Masera, M., & De Cian, A. (2009). Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety, 94*(9), 1394-1402.

Fraga-Lamas, P., Fernández-Caramés, T. M., & Castedo, L. J. S. (2017). *Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways, 17*(6), 1457.

Franekova, M., & Chrtiansky, P. (2009). Key Management System in ETCS. *Archives of Transport System Telematics, 2,* 12-16.

Franeková, M., Rástocný, K., Janota, A., & Chrtiansky, P. (2011). Safety analysis of cryptography mechanisms used in GSM for railway. *Annals of the Faculty of Engineering Hunedoara, 9*(1), 207.

Franeková, M., & Výrostko, M. (2012). Approaches to a Solution of Key Management System for Cryptography Communications within Railway Applications. Paper presented at the International Conference on Transport Systems Telematics.

Franekova, M., Vyrostko, M., & Luley, P. (2013). Determination of error probability of cryptography and safety codes for safety-related railway applications. *Advances in Electrical and Electronic Engineering, 11*(2), 94.

GCOR. (2015). Railroad Radio and Communication Rules. In GCOR General Code of Operating Rules, 2-2.

Grønbæk, J., Madsen, T. K., & Schwefel, H. P. (2008). Safe wireless communication solution for driver machine interface for train control systems. Paper presented at the Systems, 2008. ICONS 08. Third International Conference.

Gürcan, O., Yakymets, N., Tucci-Piergiovanni, S., & Radermacher, A. (2015). Multi-Agent Optimization for Safety Analysis of Cyber-Physical Systems: Position Paper. Paper presented at the 2nd International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems, part of Cyber-Physical Systems Week, Seattle.

Handbook, M. S. J. R. P. o. E. E., US Department of Defense. (1995). MIL-HDBK-217F.

Harshan, J., Chang, S.-Y., Kang, S., & Hu, Y.-C. (2017). Securing balise-based train control systems using cryptographic random fountains. Paper presented at the Communications and Network Security (CNS), 2017 IEEE Conference.

Hartong, M., Goel, R., & Wijesekera, D. (2006a). Communications security concerns in communications based train control. *WIT Transactions on The Built Environment, 88*.

Hartong, M., Goel, R., & Wijesekera, D. (2006b). Key management requirements for positive train control communications security. Paper presented at the ASME/IEEE 2006 Joint Rail Conference.

Hartong, M., Goel, R., & Wijesekera, D. (2006c). Mapping misuse cases to functional fault trees in order to secure positive train control systems. *Applications of Advanced Technology in Transportation*, 394-399.

Hartong, M., Goel, R., & Wijesekera, D. (2007). Securing positive train control systems. Paper presented at the International Conference on Critical Infrastructure Protection.

Hartong, M., Goel, R., & Wijesekera, D. (2008a). Security and the US rail infrastructure. *International Journal of Critical Infrastructure Protection, 1,* 15-28.

Hartong, M., Goel, R., & Wijesekera, D. (2008b). Trust-based secure positive train control (PTC). *Journal of Transportation Security, 1*(4), 211-228.

Hartong, M., Goel, R., & Wijesekera, D. (2010). Security and Dependability in Train Control Systems. *Vehicular Networking: Automotive Applications and Beyond, 2,* 129.
Hartong, M. W. (2009). Secure Communications Based Train Control (CBTC) Operations. George Mason University,
Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2017). Real-time management of railway CPS secure administration of IoT and CPS infrastructure. Paper presented at the Embedded Computing (MECO), 2017 6th Mediterranean Conference on.
Heddebaut, M., Deniau, V., Rioult, J., & Copin, G. (2015). Method for detecting jamming signals superimposed on a radio communication application to the surveillance of railway environments. Paper presented at the Electromagnetic Compatibility (EMC), 2015 IEEE International Symposium.
Heddebaut, M., Deniau, V., Rioult, J., & Gransart, C. (2016). Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train. *IEEE Transactions on Electromagnetic Compatibility, 59*(3), 845-852.
Heddebaut, M., Mili, S., Sodoyer, D., Jacob, E., Aguado, M., Zamalloa, C. P., . . . Deniau, V. (2014). Towards a resilient railway communication network against electromagnetic attacks. Paper presented at the TRA-Transport Research Arena.
Henrie, M. (2013). Cyber Security Risk Management in the SCADA Critical Infrastructure Environment. *Engineering Management Journal, 25*(2), 38-45.
Hitachi. (2017). ASTS USA Railway Signaling Equipment (RSE) Catalog Rev. 2-17. In: Ansaldo STS USA, A Hitachi Group Company.
Horace, M. (1969). A Summary and Analysis of Bridge Failures. Iowa State University, Ames, IA.
House, T. W. (2003). The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
Houy, D. (Producer). (2010). ATCS Monitor – Potential for Misuse.
Huang, P.-C., & Milius, B. (2016). Operational Security–A Coming Evolution of Railway Operational Procedures Under the IT Security Threat. Paper presented at the International Conference on Reliability, Safety and Security of Railway Systems.
Hughes, J., & Cybenko, G. (2014). Three Tenets for Secure Cyber-Physical System Design and Assessment. Paper presented at the Cyber Sensing 2014.
IEEE. (1998). IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document. *IEEE*.
IEEE. (2005). IEEE 1474.1-2004 - IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.
Ji, X., Yu, H., Fan, G., & Fu, W. (2016). Attack-defense trees based cyber security analysis for CPSs. Paper presented at the Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2016 17th IEEE/ACIS International Conference.
Kertis, T., & Prochazkova, D. (2017). Cyber security of underground railway system operation. Paper presented at the Smart City Symposium Prague (SCSP).
Knight, M., & Newlin, M. (2017). Radio exploitation 101. In: DEFCON.
Koglin, T. L. (2003). Movable Bridge Engineering.
Kohli, S. (2016). Developing Cyber Security Asset Management framework for UK rail. Paper presented at the Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) International Conference, London.

Kolli, S., Lilly, J., & Wijesekera, D. (2018). Providing Cyber Situational Awareness (CSA) for PTC Using a Distributed IDS System (DIDS). *Proceedings of the Asme Joint Rail Conference, 2018*.

Kordy, B., Pouly, M., & Schweitzer, P. (2012). Computational aspects of attack–defense trees. *Security and Intelligent Information Systems,* 103-116. Springer.

Koutsoukos, X., Neema, H., Martins, G., Bhatia, S., Sztipanovits, J., Stouffer, K., . . . Candell, R. (2016). Performance evaluation of secure industrial control system design: A railway control system case study. Paper presented at the Resilience Week (RWS).

Krotofil, M., and Larson, J. (2015). Rocking the Pocket Book: Hacking Chemical Plants for Competition and Extortion. DEFCON 23.

Kumar, R., & Stoelinga, M. (2017). Quantitative security and safety analysis with attack-fault trees. Paper presented at the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE).

Lakshminarayana, S., Teng, T. Z., Tan, R., & Yau, D. K. (2017). Modeling and Detecting False Data Injection Attacks against Railway Traction Power Systems. arXiv preprint arXiv:1709.07574.

Lakshminarayana, S., Teo, Z.-T., Tan, R., Yau, D. K., & Arboleya, P. (2016). On false data injection attacks against railway traction power systems. Paper presented at the Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference.

Langensiepen, D. A. X. M. C. (2015). Analysis of Security Protocols using Finite-State Machines. *International Journal of Advanced Research in Artificial Intelligence, 4,* 46-53.

Langner, R. (2013). To kill a centrifuge. Arlington, VA: The Langer Group.

Lee, M. A. a. R. (2015). The Industrial Control Systems Cyber Kill Chain.

Lim, H. W., Temple, W. G., Tran, B. A. N., Chen, B., Kalbarczyk, Z., & Zhou, J. (2017). Data Integrity Threats and Countermeasures in Railway Spot Transmission Systems. arXiv preprint arXiv:1709.05935.

Lipol, L. S., & Haq, J. (2011). Risk analysis method: FMEA/FMECA in the organizations. *International Journal of Basic & Applied Sciences, 11*(5), 74-82.

Liu, P., Yang, L., Gao, Z., Li, S., & Gao, Y. (2015). Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Safety Science, 79,* 344-357.

Lopez, I., & Aguado, M. (2015). Cyber security analysis of the european train control system. *IEEE Communications Magazine, 53*(10), 110-116.

Lu, Z., Lu, X., Wang, W., & Wang, C. (2010). Review and evaluation of security threats on the communication networks in the smart grid. Paper presented at the MILCOM, Military Communications Conference, San Jose, CA.

Luckett, P., McDonald, J. T., & Glisson, W. B. (2017). Attack-graph threat modeling assessment of ambulatory medical devices. arXiv preprint arXiv:1709.05026.

M. Jablonski, Y. W., C. Yavvari, Z. Wang, X. Liu, K. Holt and D. Wijesekera. (2019). An Attack-Fault Analysis of Movable Railroad Bridges. Paper presented at the Critical Infrastructure Protection X 13th IFIP WG 11.10 International Conference, ICCIP 2019, Arlington, VA.

Mansson, D., Thottappillil, R., Backstrom, M., & Lunden, O. (2008). Vulnerability of European rail traffic management system to radiated intentional EMI. *IEEE Transactions on Electromagnetic Compatibility, 50*(1), 101-109.

Mark Hartong, R. G., and Duminda Wijesekera. (2011). Secure Interchange Routing. *Journal of Transportation Technologies, 1,* 21-29.
Mark Hartong, R. G., Duminda Wijesekera. (2012). In R. S. Javier Lopez, Stephen D. Wolthusen LNCS (Ed.), Critical Infrastructure Protection - Information Infrastructure Models, Analysis, and Defense (Vol. 7130, pp. 330-355).
Mark Hartong, R. G. a. D. W. (2011). Positive Train Control (PTC) Failure Modes. *Journal of King Saud University,* 1-11.
Marrone, S., Rodríguez, R. J., Nardone, R., Flammini, F., & Vittorini, V. (2015). On synergies of cyber and physical security modelling in vulnerability assessment of railway systems. *Computers & Electrical Engineering, 47,* 275-285.
Masson, É., & Gransart, C. (2017). Cyber Security for Railways – A Huge Challenge – Shift2Rail Perspective. Paper presented at the 12th International Workshop of Communication Technologies for Vehicles, Toulouse, France.
Mauw, S., and Oostdijk, M. (2005). Foundations of Attack Trees. Paper presented at the International Conference on Information Security and Cryptology ICISC 2005. LNCS 3935, Springer.
McGeehan, P. (2014, Sept. 25). Critical 104-year-old Link Poses $900 Million Problem. *The New York Times.*
McGoogan, C., & Willgress, L. (Producer). (2016, July 12). UK rail network hit by multiple cyber attacks last year.
Melaragno, A., Bandara, K. D. S., Fewell, A., & Wijesekera, D. (2016). Rail radio intrusion detection system (RRIDS) for communication based train control (CBTC). Paper presented at the Intelligent Rail Transportation (ICIRT), 2016 IEEE International Conference on.
Mili, S., Deniau, V., Sodoyer, D., Heddebaut, M., & Ambellouis, S. (2015). Jamming Detection Methods to Protect Railway Radio Communication. *Methods, 4*(7).
Mili, S., Sodoyer, D., Deniau, V., Heddebaut, M., Philippe, H., & Canavero, F. (2013). Recognition process of jamming signals superimposed on GSM-R radiocommunications. Paper presented at the Electromagnetic Compatibility (EMC Europe), 2013 International Symposium.
Moayedi, B. Z., & Azgomi, M. A. (2012). A game theoretic framework for evaluation of the impacts of hackers diversity on security measures. *Reliability Engineering & System Safety, 99,* 45-54.
MODICON, I. (Producer). (1996). Modicon Modbus Protocol Reference Guide. Retrieved from http:// modbus.org/docs/PI_MBUS_300.pdf
Morscher, A. H. (Producer). How to set up ATCS monitoring, based upon my recent experiences.
Movable Bridge Locking Inspection, 33 CFR § 236.387, (1984).
Movable Bridge, Interlocking of Signal Appliances with Bridge Devices, 49 CFR § 236.312, (1984).
Nardone, R., Rodríguez, R. J., & Marrone, S. (2016). Formal security assessment of Modbus protocol. Paper presented at the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).
Nguyen, H. H., Tan, R., & Yau, D. K. (2015). Impact of signal delay attack on voltage control for electrified railways. Paper presented at the TENCON 2015-2015 IEEE Region 10 Conference.

NIST. (2018). *Risk Management Framework for Information Systems and Organizations. 800,* 37.
Nowakowski, W., Bojarczak, P., & Łukasik, Z. (2017). Performance analysis of data security algorithms used in the railway traffic control systems. Paper presented at the Information and Digital Technologies (IDT), 2017 International Conference on.
NTSB. (1994). Derailment of Amtrak Train No. 2 on the CXST Big Bayou Cannot Bridge.
NTSB. (2012). Railroad Accident Brief: DCA-13-FR-001. Retrieved from Washington, D.C.:
Ojamaa, A., Tyugu, E., & Kivimaa, J. (2008). Pareto-optimal situaton analysis for selection of security measures. Paper presented at the Military Communications Conference, 2008. MILCOM 2008. IEEE.
Ou, X. (2013). Mulval project at Kansas State University.
Ou, X., Boyer, W. F., & McQueen, M. A. (2006). A scalable approach to attack graph generation. Paper presented at the Proceedings of the 13th ACM conference on Computer and communications security.
Paine, G. T. (2018). Telemetry from the Code Line.
Paul X. O'Neil, & Ostrovsky, A. (2002). Failure and quick recovery of movable bridge on the Acela line. Paper presented at the Heavy Movable Structures, Inc. 9th Bienniel Symposium.
Perrig, A., Canetti, R., Tygar, J. D., & Song, D. J. R. C. (2002). *TESLA Broadcast authentication Protocol, 5*(2), 2-13.
Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems, 16*(2), 546-556.
Pinedo, C., Aguado, M., Lopez, I., Higuero, M., & Jacob, E. (2016). A multi bearer adaptable communication demonstrator for train-to-ground IP communication to increase resilience. Paper presented at the International Workshop on Communication Technologies for Vehicles.
Protin, H. F., & McGuire, M. (2004). End Lift Machinery for Swing Bridges (There's More than One Way to Lift a Span). Paper presented at the Inc. 10th Biennial Symposium, Orlando, FL.
R. Lee, J. Slowik, B. Miller, A. Cherepanov, & Lipovsky, R. (2017). INDUSTROYER / CRASHOVERRIDE: Zero Things Cool About a Threat Group Targeting the Power Grid. Paper presented at the Black Hat USA 2017, Las Vegas, NV.
Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega, 40*(1), 79-88.
Rao, N. S., Ma, C. Y., He, F., Zhuang, J., & Yau, D. K. (2014). Cyber-physical correlations for infrastructure resilience: A game-theoretic approach. Paper presented at the Information Fusion (FUSION), 2014 17th International Conference on.
Rao, N. S., Poole, S. W., Ma, C. Y., He, F., Zhuang, J., & Yau, D. K. (2016). Defense of Cyber Infrastructures Against Cyber‐Physical Attacks Using Game‐Theoretic Models. *Risk Analysis, 36*(4), 694-710.
Ren, D., Du, S., & Zhu, H. (2011). A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. Paper presented at the 2011 IEEE International Conference on Communications (ICC).
Rimmer, M. (2010). Somerleyton swing bridge report by waterways strategy officer.

Robert Lee, M. J. A., & T., C. (2016). Analysis of the cyber attack on the Ukrainian power grid. Paper presented at the Electricity Information Sharing and Analysis Center and SANS, Washington, DC.
Rodríguez-Piñeiro, J., Fraga-Lamas, P., García-Naya, J. A., & Castedo, L. (2012). Long term evolution security analysis for railway communications. Paper presented at the Proceedings of the IEEE Congreso de Ingeniería en Electro-Electrónica, Comunicaciones y Computación, Asunción, Paraguay.
Rodriguez, L., Pinedo, C., Lopez, I., Aguado, M., Astorga, J., Higuero, M., . . . Mendizabal, J. (2016). Eurobalise-Train communication modelling to assess interferences in railway control signalling systems. *Network Protocols and Algorithms, 8*(1), 58-72.
Ross, R., McEvilley, M., & Oren, J. (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Retrieved from
Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Retrieved from
Ross, R. S., Katzke, S. W., & Johnson, L. A. (2006). Minimum security requirements for federal information and information systems.
Roy, A., Kim, D. S., & Trivedi, K. S. (2010). Cyber security analysis using attack countermeasure trees. Paper presented at the Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research.
Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances 49 CFR § 236, (2010).
Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems, 55*(1), 156-164.
Schlehuber, C., Heinrich, M., Vateva-Gurova, T., Katzenbeisser, S., & Suri, N. (2017). A Security Architecture for Railway Signalling. Paper presented at the International Conference on Computer Safety, Reliability, and Security.
Schmittner, C., Ma, Z., Schoitsch, E., & Gruber, T. (2015). A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive cyber-physical systems. Paper presented at the Proceedings of the 1st ACM Workshop on Cyber-Physical System Security.
Schneier, B. (1999). Attack Trees. *Dr. Dobbs Journal, 24*(12), 21–29.
SECRET. (2015). White Paper: Security of Railways against Electromagnetic Attacks (SECRET) (978-2-7461-2465-3).
SECUR-ED. (2014). White Paper for Public Transport Stakeholders – Based on the Lessons Learned in SECUR-ED.
Shiva, S., Roy, S., & Dasgupta, D. (2010). Game theory for cyber security. Paper presented at the Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research.
Siemens. (2014). Installation: Base Station Communications Package II (BCP) 53410. Rancho Cucamonga, CA.
Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management, 34*(6), 733-740.

Sinson, H. (2016). Gasparilla island swing bridge replacement. Paper presented at the Heavy Movable Structures, Inc. 16th Biennial Symposium.
Sondi, P., Berbineau, M., Kassab, M., Wahl, M., Gransart, C., Lemaire, E., . . . Schon, W. (2014). Virtual lab based on co-simulation to include impairments of wireless telecommunication such as GSM-R in the evaluation of ERTMS. Paper presented at the TRA-Transport Research Arena.
Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75,* 49-62.
SS-CCS, A. (2010). Securing Control and Communications Systems in Rail Transit Environments.
Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety Science, 49*(2), 292-297.
Stouffer, K., Falco, J., & Scarfone, K. J. N. s. p. (2011). Guide to Industrial Control Systems (ICS) *Security, 800*(82), 16-16.
Stouffer, K., Zimmerman, T., Tang, C., Lubell, J., Cichonski, J., & McCarthy, J. (2017). Cybersecurity Framework Manufacturing Profile.
Symantec. (2014). Dragonfly: Cyberespionage Attacks Against Energy Suppliers. Dover, DE.
Tan, X., & Ai, B. (2011). The issues of cloud computing security in high-speed railway. Paper presented at the Electronic and Mechanical Engineering and Information Technology (EMEIT), International Conference, Harbin, China.
Temple, W., Li, Y., Tran, B. A. N., Liu, Y., & Chen, B. (2016). Railway System Failure Scenario Analysis. Paper presented at the International Conference on Critical Information Infrastructures Security, Paris.
Temple, W., Tran, B. A. N., Chen, B., Kalbarczyk, Z., & Sanders, W. H. (2017). On Train Automatic Stop Control Using Balises: Attacks and a Software-Only Countermeasure. Paper presented at the Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium.
Ten, C.-W., Liu, C.-C., & Govindarasu, M. (2007). Vulnerability assessment of cybersecurity for SCADA systems using attack trees. Paper presented at the 2007 IEEE Power Engineering Society General Meeting.
Teo, Z.-T., Tran, B. A. N., Lakshminarayana, S., Temple, W. G., Chen, B., Tan, R., & Yau, D. K. (2016). SecureRails: towards an open simulation platform for analyzing cyber-physical attacks in railways. Paper presented at the Region 10 Conference (TENCON), 2016 IEEE.
Tsudik, G. (1992). Message authentication with one-way hash functions. Paper presented at the INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE.
The UPPAL Model checker. www.uppal.org
USEAC. (2017). Common Cybersecurity Terminology.
VanDeRee, M. (2016). Fail-Safe Control Systems for Heavy Movable Structures. Paper presented at the Heavy Movable Structures, Inc. Sixteenth Biennial Symposium, Tampa, FL.
Vieira, P., Paudel, Y., Catral, J., Eruvuru, S., & Gonzalez-Ruiz, A. (2018). PTC Radio Frequency Network Design for Dense Urban Areas.

Výrostko, M., Lüley, P., Ondrašina, T., & Franeková, M. (2012). Probabilistic error analysis of encrypted transmission for safety-related railway applications. Paper presented at the ELEKTRO, 2012.
W. Vesely, F. Goldberg, N. Roberts, & Haasl, D. (1981). Fault Tree Handbook. Paper presented at the Nuclear Regulatory Commission, Washington, DC.
Wang, M.-y., Wang, H., & Liu, Z.-g. (2014). Reach on fault tree analysis of train derailment in urban rail transit. *International Journal of Business and Social Science, 5*(8).
Wang, W., & Lu, Z. (2013). Cyber Security in the Smart Grid: Survey and Challenges. Computer Networks, 57(5), 1344-1371.
Wang, Z., Liu, X., Wang, Y., Yavvari, C., Jablonski, M., Wijesekera, D., . . . Holt, K. (2019). Cyber Security Analysis for Advanced Train Control System (ATCS) in CTC Systems: Concepts and Methods. Paper presented at the Proceedings of the 2019 Joint Rail Conference, Snowbird, UT.
Wolf, J. T. D. (2009). History of Connecticut's Short-Term Strain Program for Evaluation of Steel Bridges.
Wu, Y., Weng, J., Tang, Z., Li, X., & Deng, R. H. (2017). Vulnerabilities, attacks, and countermeasures in balise-based train control systems. *IEEE Transactions on Intelligent Transportation Systems, 18*(4), 814-823.
Xie, F., Lu, T., Guo, X., Liu, J., Peng, Y., & Gao, Y. (2013). Security analysis on cyber-physical system using attack tree. Paper presented at the Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference.
Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010). Using Bayesian networks for cyber security analysis. Paper presented at the Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference.
Xu, Z., & Zhu, Q. (2017). A game-theoretic approach to secure control of communication-based train control systems under jamming attacks. Paper presented at the Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles.
Y. Wang, M. J., C. Yavvari, Z. Wang, X. Liu, K. Holt and D. Wijesekera. (2019). Safety and Security Analysis For Movable Railroad Bridges. Paper presented at the 2019 ASME/IEEE Joint Rail Conference.
Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials, 14*(4), 998-1010.
Zhang, Z., Liu, X., & Bian, Z. (2018). Analysis of restricted-speed accidents using Fault Tree Analysis. Paper presented at the 2018 Joint Rail Conference.
Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. Paper presented at the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing.
Zhu, L., Yu, F. R., Tang, T., & Ning, B. (2016). An integrated train–ground communication system using wireless network virtualization: Security and quality of service provisioning. *IEEE Transactions on Vehicular Technology, 65*(12), 9607-9616.
Zones, P. C. (2013). Securing Control and Communications Systems in Rail Transit Environments.

Abbreviations and Acronyms

ACRONYM	EXPLANATION
AAR	Association of American Railroads
AASHTO	American Association of State Highway and Transportation Officials
AC	Alternating Current
ACSES	Advanced Civil Speed Enforcement System
ACSES II	Advanced Civil Speed Enforcement System (second generation)
AES	Advanced Encryption Standard
AFT	Attack Fault Tree
AFTeR	Attack-Fault Trees with Reliability
APR	absolute position reference
APT	advanced persistent threat
AREMA	American Railroad Engineering and Maintenance-of-Way Association
ARES	Advanced Railroad Electronics System
ARINC	Aeronautical Radio Inc.
ARP	Address Resolution Protocol
ATACS	Advanced Train Administration and Communications System
ATC	Automatic Train Control
ATCS	Advanced Train Control System
BART	Bay Area Rapid Transit
BAS	Basic Attack Steps
BCD	Binary Coded Decimal
BCF	Basic Component Failure
BCM	Base Communication Managers
BCP	Base Communication Package
BER	Bit Error Rate
BOS	Back Office Server
C&S	Communication and Signaling
CBTC	Communications-Based Train Control
CC	Cluster Controllers
CDMA	Code Division Multiple Access
CI	Confidence Interval
ConOps	Concept of Operations
CP	Control Point
CPs	Control Points
CPS	Cyber-Physical System
CRC	Cyclic Redundancy Check
CTC	Centralized Traffic Control
CTCS-3	Level 3 of Chinese Train Control System
DAG	Directed Acyclic Graph

ACRONYM	EXPLANATION
DC	Direct Current
DFT	Dynamic Fault Tree
DoS	Denial of Service
DTMF	Dual Tone Multi Frequency
EMI	Electro Magnetic Interference
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDEP	Functional Dependency
FEC	Forward Error Correction
FEP	Front End Processors
FMVEA	Failure Mode Vulnerabilities and Effects Analysis
FHWA	Federal Highway Administration
FRA	Federal Railroad Administration
FSM	Finite State Machine
FTA	Federal Transit Administration
GFDM	Generalized Frequency Division Multiplexing
GSM-R	Global System for Mobile Communications – Railway
hACLs	Host Access Control lists
HDLC	High-level Data Link Control
HIPS	Host Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HMI	Human machine interface
I-ETMS	Interoperable Electronic Train Management System
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IFAIL	Instant Failures
IoT	Internet of Things
IPS	Intrusion Prevention System
ISP	Internet Service Provider
ITCS	Incremental Train Control System
JR-East	East Japan Railway Company
LAN	Local Area Network
LEU	Lineside Equipment Unit
MA	Movement Authorities
MAC	Message Authentication Code
MCP	Mobile Communication Package
MIS	Management Information System

ACRONYM	EXPLANATION
MOW	Maintenance-of-Way
MSRP	Manual of Standards and Recommended Practices
MTBF	Mean-time-between-failure
MTTF	Mean-time-to-fail
MTTR	Mean-time-to-repair
MulVAL	Multi-host, Multi-stage Vulnerability Analysis Language
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIST	National Institute of Standards and Technology
NTSB	National Transportation Safety Board
OSI	Open Systems Interconnection
PA	Public Address
PAND	Priority AND
PLC	Programmable Logic Controller
PTC	Positive Train Control
PWM	Pulse Width Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RIoT	Rail Internet of Things
SAND	Sequential AND
SCADA	Supervisory Control and Data Acquisition
SCR	Silicon Controlled Rectifier
SDR	Software Defined Radio
SFTP	Secure File Transfer Protocol
SMC	Statistical Model Checking
SNR	Signal to Noise Ratio
STA	Stochastic Timed Automata
TCP/IP	Transmission Control Protocol (TCP)/Internet Protocol (IP)
TDMA	Time-Division Multiple Access
TESLA	Timed Efficient Stream Loss-tolerant Authentication
TMDS	Traffic Management and Dispatching System
TSR	Temporary Speed Restriction
UML	Unified Modeling Languages
US&S	Union Switch and Signal Company
VHF/UHF	Very High Frequency/Ultra High Frequency
VSD	Variable Speed Drive
WAN	Wide Area Network
WCP	Wayside Communication Package
WIU	Wayside Interface Unit