Communications in Transportation Research 2 (2022) 100078

Contents lists available at ScienceDirect

Communications in Transportation Research

journal homepage: www.journals.elsevier.com/communications-in-transportation-research

Full Length Article

# Cyber security of railway cyber-physical system (CPS) – A risk management methodology

Zezhou Wang, Xiang Liu [*]

*Rutgers University, 500 Bartholomew Road, Piscataway, 08854, NJ, USA*

ARTICLE INFO

*Keywords:*
Cyber security
Rail-CPS
Risk management
Advanced train control system (ATCS)

ABSTRACT

Along with the increasing application of different cyber-physical systems (CPSs) to connect various components in the rail industry, rising connectivity through communication technologies has also introduced cyber threats against rail-CPSs, causing failures with huge consequences. Implementations of rail-CPSs demand proactive identification, clear-cut definition, and proper handling of their cyber security risks. In this paper, we formulate a risk management methodology for cyber security in rail-CPSs and conduct a retrospective case study on the Advanced Train Control System (ATCS) that has been deployed in many U.S. freight railways. The methodology provides two alternative approaches to fill knowledge gaps in contingency preparation, threat prevention, consequence analysis, and security risk mitigation. In the case study, we demonstrate two cyber threats of ATCS, using attack sequence modeling and consequence analysis, and provide recommendations for risk mitigation. By practicing the methodology with the case study, this work can be used as a general reference to conduct cyber risk management and cyber-robustness evaluations for other existing systems.

## 1. Introduction

Nowadays, critical infrastructure (CI) continues to adopt advanced cyber technologies to enhance its level of automation and digitization, and the modern rail industry is no exception. To upgrade operational safety and efficiency, an increasing number of railway physical components have become connected by different CPSs through communications, creating the new paradigm of “Rail Internet of Things”. The trend towards CPS integration has also led to an ever-growing dependency of the rail industry on cyber and IoT technologies, exposing the risk of cyber threats. Embarrassingly, in favor of business growth and cost control, well-thought-out cyber security considerations of CPSs in many industries often occur much later than their actual deployments (Habibzadeh et al., 2019). Therefore, the rail industry is also subject to cyber risks ingrained in its CPS deployments, especially in those legacy ones, laying “ticking bombs” (threats) based on ulterior motives.

For cyber-attacks aimed at the critical infrastructure (CI), the integrity of physical components in the cyber-physical systems (CPSs) of CI is usually the “ultimate goal”, e.g., to sabotage train operations in the rail industry. Technically, impostors infiltrate through the CPS cyber components to spoil the physical components. Unfortunately, the CPS cyber components provide not only the desired connectivity but also a medium for attackers to achieve malicious goals. Generic cyber technologies are often shared across CPSs in different industries, and their fundamental security designs have been well-studied by technical iterations and IT-domain research (Yampolskiy et al., 2015). Therefore, it is the distinctions of the CPS physical components that magnify the consequences of CPS-targeted cyber-attacks.

To efficiently study cyber risks on rail-CPSs, we prototype a generalized risk management methodology in this paper. The methodology can help distinguish between cyber components and physical components, focusing on their functional interactions. Alternatively, it can also use parameterized risk consequences to epitomize the outcome of cyber threats. It aims to help railway stakeholders categorize and prioritize cyber risks on rail-CPSs to better connect threats with their associated components, and to take effective action before diving too deep into the overwhelming fundamentals of cyber technologies.

The paper is organized as follows: first, we review the subject background and related works. Based on the reviewed literature, we abstract the need for a generalized methodology for rail-CPS cyber security risk management. To illustrate the application of the methodology with a concrete example, we present a case study of an existing rail-CPS: the Advanced Train Control System (ATCS) used in U.S. freight railways. At the end of this paper, we summarize the case study conclusions, prospects

[*] Corresponding author.
*E-mail address:* xiang.liu@rutgers.edu (X. Liu).

https://doi.org/10.1016/j.commtr.2022.100078
Received 27 April 2022; Received in revised form 17 July 2022; Accepted 18 July 2022
Available online xxxx

for the methodology, and the general contributions of our work.

## 2. Literature review: rail-CPS security background and current studies

The significance of railway can make successful cyber-attacks "fruitful," leading to varied consequences, ranging from operational disruptions to safety breaches. Specifically, serious safety breaches can cause equipment damage, injuries, or even fatalities. Over the years, cyber-attacks against rail-CPSs have not been uncommon. On the one hand, spontaneous attacks spread around the world and can be traced back to the early 21st century. In 2003, the malware "Sobig" knocked down the signaling system of CSX, a major U.S. freight rail operator, causing 6+ hours of halted operations in the eastern U.S. rail network (Temple et al., 2017a, 2017b); in 2008, a schoolboy hacked a Polish tram system and created derailments and injuries (Leyden, 2008); in 2011, the signaling system of an unnamed U.S. rail operator in the Pacific Northwest was infiltrated by foreign attackers, with disruptions clocked over two days (Sternstein, 2012); and between 2015 and 2016, four major cyber-attacks were launched on UK rail network (McGoogan and Willgress, 2016). On the other hand, systemic cyber-attacks have also been launched on rail systems among hostile parties. For example, the Iranian railway was allegedly hit multiple times by adversaries in 2019 and 2021 (Bergman, 2021). Additionally, a burst of cyber-attack activities has been reported on many railways in different nations during the Russo-Ukrainian War, including the Italian railway (Reuters, 2022) and the Belarusian railway (Gallagher, 2022).

Over the years, plentiful studies have been conducted on CPS cyber security subjects in the rail domain, and their topic coverage continues to expand. In Table 1, we present a collection of state-of-the-art rail-CPS cyber security research. The studies are categorized by individual system types and threats analyzed. Each paper has provided pertinent solutions to specific rail-CPS cyber security issues.

Classically, most concurrent papers choose to use case studies to address rail-CPS security issues on individual systems. They focus on cyber technical details, consequence analyses, and security modeling to resolve specific security problems. However, the reasoning for their subject selection is mostly subjective or empirical, posing a gap in materializing the urgency for selected security subjects. For example, Chen et al. (2015) juxtaposed the communications-based train control (CBTC) system and passenger mobile APP as two case studies for railway cyber-physical security research. Although their technical analysis and security evaluations on each system are both contributive, these two systems are incommensurate and have completely different operational roles. Meanwhile, the commonly used technologies (e.g., wireless communication technologies) may share loopholes across different systems. Different cyber-physical interactions may either attenuate or amplify their threats. Therefore, such facts have created a delicate situation for prioritizing resources to handle the most emergent cyber threats for railway administrators. An effective method is needed to cross-compare threats and their associated rail-CPS systems from a security perspective.

## 3. Risk management methodology

Cyber security problems in CPS are never purely cyber problems (Mo et al., 2012). Instead, the uniqueness and significance of their physical outputs and cyber-physical interactions jointly define the damage level caused by successful cyber-attacks (Yampolskiy et al., 2015). In miscellaneous CPS operations, the cyber technological complexity of a breach is not necessarily correlated to the consequences. In other words, deliberate CPS cyber-attacks on non-critical physical components may only result in minor disruptions; lethal attacks may not require sophisticated knowledge to achieve either (e.g., the Polish schoolboy derailed the trams with simple infrared modifications (Leyden, 2008)). Therefore, we should be aware of and move away from "cyber technological entrapment", where the CPS cyber security studies fall too obsessed with technological complexity, yet contribute little to the substantial threats.

**Table 1**
Summary of recent cyber security research on rail-CPS, categorized by CPS and threats.

| Rail-CPS Subjects | Analyzed Threats | References |
|---|---|---|
| New-gen train control systems (e.g., ERTMS, ETCS, PTC, CBTC) | Multiple attacks including electromagnetic interference, jamming, denial of service (DoS), message modification and unauthorized access, etc. | Bezzateev et al., 2013; Bloomfield et al., 2012; Chernov et al., 2015; Craven, 2004; Masson and Gransart, 2017; Pinedo et al., 2016; Rodríguez-Piñeiro et al., 2012 |
| | Electromagnetic interference, jamming attack | Andre'B, 2014; Bandara et al., 2017; Chang et al., 2015; Heddebaut et al., 2015; Mili et al., 2015; Xu and Zhu, 2017 |
| | Brute force attacks, unauthorized access to the network, and message modification | Bantin and Siu, 2011; Chang et al., 2017; Chen et al., 2011, 2015; Chothia et al., 2017; de Ruiter et al., 2016; Melaragno et al., 2016; Temple et al., 2017a, 2017b |
| | Passive eavesdropping, active denial of control, and assumption of control | Emmelmann et al., 2010; Hartong et al., 2008, 2012 |
| Traditional railway signaling systems | Unauthorized access to the network, denial of service, and message modification | Bastow, 2014; Schlehuber et al., 2017 |
| | Electromagnetic interference | Adin et al., 2012 |
| Balise data transmission | Compromise the availability or integrity of the balises' data, jamming, electromagnetic interference | Harshan et al., 2017; Lim et al., 2019; Temple et al., 2017a, 2017b |
| Railway traction power, voltage control systems | False data injection attacks, message modification, and unauthorized access to the network | Lakshminarayana et al., 2016, 2018; Nguyen et al., 2015; Teo et al., 2016 |
| Human-machine interface | Multiple attacks including denial of service, message modification, unauthorized access, etc. | Bondavalli et al., 2009; Grønbæk et al., 2008 |
| Public address (PA) or public information display systems | Unauthorized intrusions | Chen et al., 2015 |
| Railway trackside/ lineside system | Both physical and cyber intrusion into lineside shelter protection system | Marrone et al., 2015 |

In the mainstream of rail-CPS security risk studies, many have expounded on the significance of physical components. Ali et al. (2018) have stated the need for a declaration of "valuable assets" prior to risk characterization. Neuman (2009) advocated for the enforcement of "domain-specific" knowledge during CPS security design. Burmester et al. (2012) introduced CPS physical-layer modeling to compensate for its absence in traditional cyber threat models. On the path to cyber resilience, it is always desirable to prioritize resources and efforts on the most emergent security issues, which are often the ones with the worst impact (DiMase et al., 2015). In proactive/preventive efforts, topic-specific studies (e.g., the specialized ones from Table 1) are most useful when a rail-CPS security problem is clearly confirmed and crystallized. Referring to Fig. 1 (for illustrative purposes only, not exhaustive), different cyber technologies are intensively shared by various rail-CPS components. The criticality and vitality of each component may not be consistent. In cyber security risk management, tracing "upstream" from the cyber technologies may end up reaching a non-critical system. Therefore, an effective methodology shall approach "downstream" from the direction of physical components in rail-CPS, in order to explicitly formulate the security problem at an early stage.

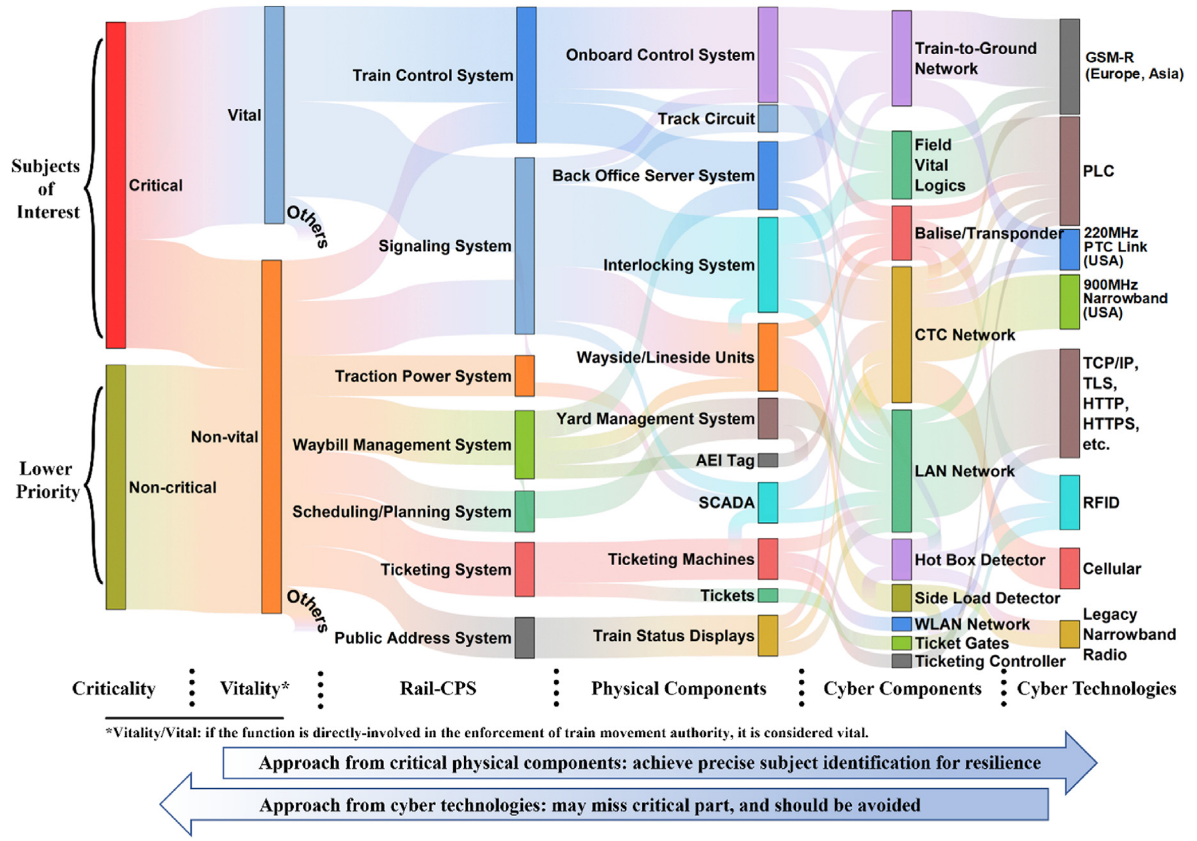
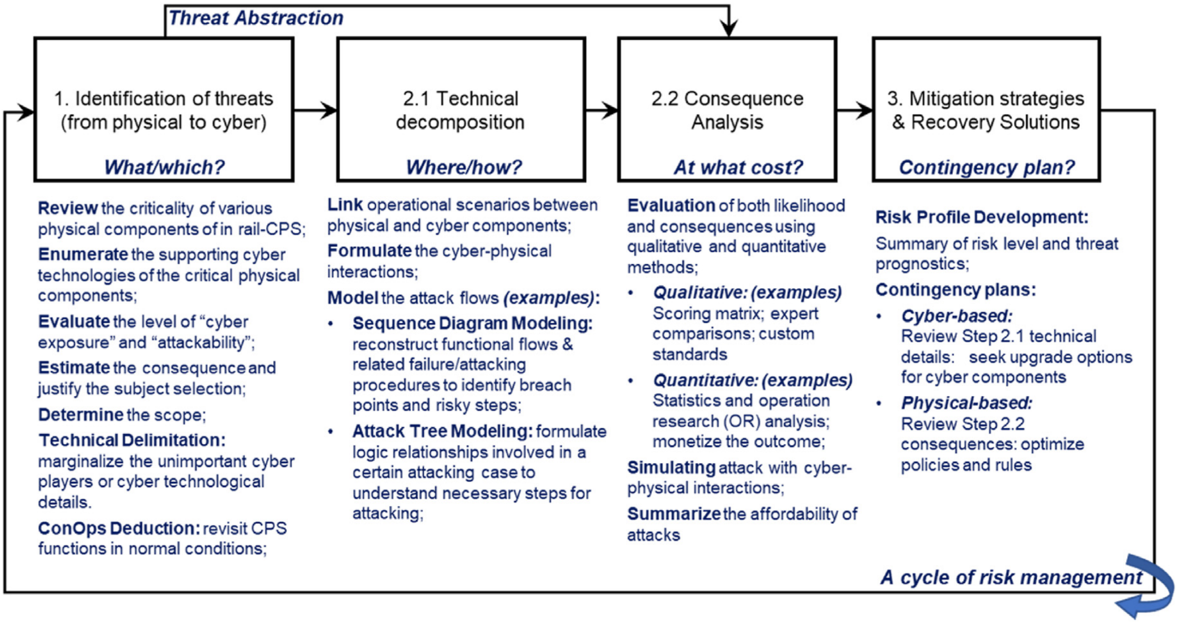


**Fig. 1.** Schematic of the interwoven relationships between physical and cyber components in rail-CPS.

Based on the U.S. National Institute of Standards and Technology (NIST) security model (Ross and McEvilley, 2016), we propose a risk management methodology for rail-CPS consisting of a stepwise loop. Each cyber security subject is determined from the "downstream" approach after the evaluation of criticality and vitality. The execution flow of the proposed methodology is illustrated in Fig. 2. It outlines a set of progressive procedures for cyber risk management for railway stakeholders, suitable for most rail-CPSs with miscellaneous development processes and cyber technologies.

Each round of procedures begins with threat identification, initiated from the review of physical components of rail-CPS. Criticality assessment and enumeration of the cyber components are needed from the selected physical components. Justifications of subject selection are required during the threat identification, in order to prioritize the efforts


Threat Abstraction
1. Identification of threats (from physical to cyber)
What/which?
2.1 Technical decomposition
Where/how?
2.2 Consequence Analysis
At what cost?
3. Mitigation strategies & Recovery Solutions
Contingency plan?
A cycle of risk management

**Review** the criticality of various physical components of in rail-CPS;
**Enumerate** the supporting cyber technologies of the critical physical components;
**Evaluate** the level of "cyber exposure" and "attackability";
**Estimate** the consequence and justify the subject selection;
**Determine** the scope;
**Technical Delimitation:** marginalize the unimportant cyber players or cyber technological details.
**ConOps Deduction:** revisit CPS functions in normal conditions;

**Link** operational scenarios between physical and cyber components;
**Formulate** the cyber-physical interactions;
**Model** the attack flows ***(examples)***:
- **Sequence Diagram Modeling:** reconstruct functional flows & related failure/attacking procedures to identify breach points and risky steps;
- **Attack Tree Modeling:** formulate logic relationships involved in a certain attacking case to understand necessary steps for attacking;

**Evaluation** of both likelihood and consequences using qualitative and quantitative methods;
- ***Qualitative: (examples)*** Scoring matrix; expert comparisons; custom standards
- ***Quantitative: (examples)*** Statistics and operation research (OR) analysis; monetize the outcome;

**Simulating** attack with cyber-physical interactions;
**Summarize** the affordability of attacks

**Risk Profile Development:**
Summary of risk level and threat prognostics;
**Contingency plans:**
- ***Cyber-based:*** Review Step 2.1 technical details: seek upgrade options for cyber components
- ***Physical-based:*** Review Step 2.2 consequences: optimize policies and rules

**Fig. 2.** Execution flow of rail-CPS cyber security risk management methodology.

of cyber defense and exclude less relevant scopes. This aims to prevent the waste of resources before the process goes into the slow-turnover cycle of technical research, evaluation, and development.

Two executable steps follow threat identification: technical decomposition (Step 2.1) and consequence analysis (Step 2.2). In Step 2.1, cyber-physical interactions are investigated between the identified critical physical components and their associated cyber foundations, with the extensive technical anatomy performed to generate prognostic attack flows. This step has often been performed in previous case-based studies on various subjects. According to Table 1, common attack flow modeling tools include sequence diagram modeling and attack tree modeling.

Consequence analysis (Step 2.2) carries forward the procedures to determine the "affordability" of the identified threats. This step can be performed either following the technical decomposition or directly after threat identification. In the case of following Step 2.1, the generated attack flow will facilitate the refined depiction of consequences. However, if identified threats can be abstracted and indexed with certain metrics, Step 2.2 can be skipped, and the consequence evaluation can take advantage of the threat abstraction: for example, monetization of consequences. Common practices in consequence analysis include qualitative and quantitative methods. When there is a lack of historic cyber-attack events in the relevant domain, consequence analysis based on forensics is unavailable. Simulation is often used in conjunction with the quantified values to indicate the severity and affordability of consequences.

Finally, the procedures converge into mitigation strategies and recovery solutions (Step 3). It consists of the development of risk profiles and contingency plans. If technical decomposition reveals the attack flow in detail, pertinent mitigation strategies can be put forth with direct correspondence; meanwhile, if the threat has been indexed into abstractions, solutions can focus on the macroscopical aspects to minimize the idiographic aftermath abstraction values.

Upon the completion of Step 3, a new cascading risk management process shall be started to close a loop, which aims at expanding the comprehensiveness of risk management for rail-CPSs. It forms a closed-loop that provides both perceptive and iterative perspectives on the risk management subject and should be practiced across all stages of the rail-CPS lifecycle. The special part of the procedure of this methodology is its origination point, where it divides rail-CPS cyber risks by their physical components. With the looping design, the methodology expands both the breadth and depth of the rail-CPS cyber security risk study and becomes sustainable for the cyber robustness of rail-CPSs.

## 4. Risk management case study – on the security paths toward the ATCS system

### 4.1. Threat identification: scope and concept of operations (ConOps)

Following Fig. 1 and searching "downstream" from the "Critical"[1] category, we intend to apply the methodology to an example rail-CPS that plays both the "**Vital**"[2] and "**Non-vital**" roles in railway operations. One intuitive "Subject of Interest" is the railway signaling system. A modern railway signaling system is a rail-CPS with high cyber dependence and extremely high criticality. The signaling system directly controls the safety of train operations, whose failure can easily turn into a tragic loss, at worst leading to train collision and secondary disasters. Among all the components of global railway signaling systems, the centralized traffic control (CTC) system is an essential one. CTC employs various networking and cyber technologies to achieve two-way communications between the field and the central dispatching office. In the U.S., the Advanced Train Control System (ATCS) is one major implementation of the CTC cyber network, carried by an unencrypted radio protocol on the 900 MHz railway-licensed band (Craven and Craven, 2008). Serving as the CTC backbone in the U.S., ATCS has been standardized in the common practices of U.S. rail operators (Association of American Railroads, 2005). The importance of the CTC system and the lack of encryption design in ATCS should jointly arouse our cyber security vigilance.

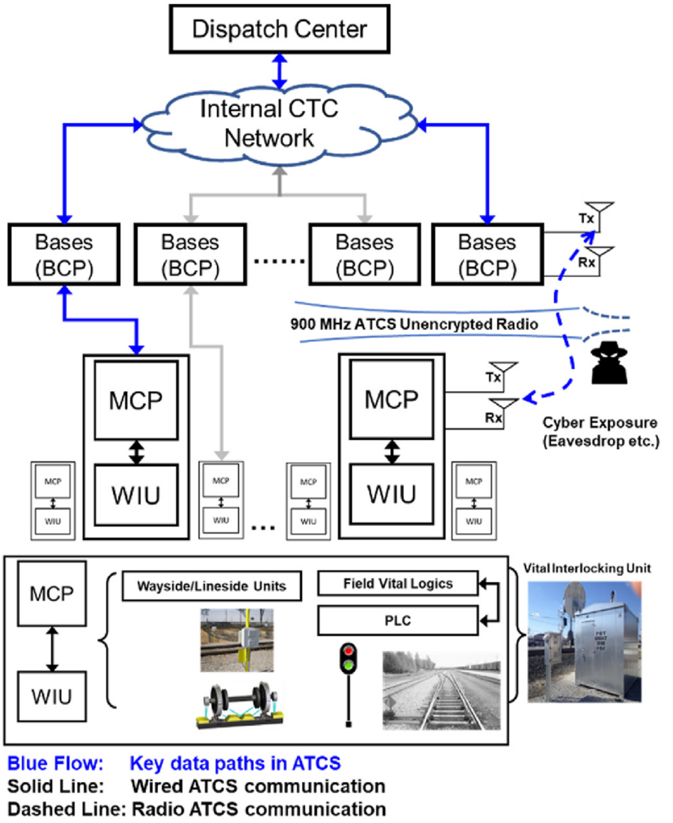


**Fig. 3.** ConOps architecture of the CTC-ATCS network with location of cyber exposure.

In fact, eavesdropping activities through ATCS have been undergoing within a large hobbyist community for over 15 years, involving thousands of active eavesdroppers. The eavesdropping implicates more than 30 U.S. railway companies, 35,000 railway route miles, and 5000 signal interlocking locations (Liu et al., 2020). Distributed local eavesdropping decoders capture, unpack, and exchange the unencrypted CTC data by personal software-defined radio (SDR). The data is then collectively aggregated via the Internet to monitor rail operations. Among the various rail-CPS cyber implementations, this scale of eavesdropping is almost unheard of, pointing to a concern about rail-CPS cyber exposure.

Although most CTC-ATCS functions in the U.S. are non-vital in normal operations, there are a few vital functions that CTC system can take part in under special circumstances (Wang et al., 2019). Since the joint CTC-ATCS system directly serves train signaling, instinct security concerns are raised for vital risks, by which it might invalidate the enforcement of train movement authority, leading to an increased likelihood of derailments or collisions. Meanwhile, when fail-safe designs are actuated to confront potential abuses, it results in system degradation and functional loss. This introduces non-vital risks that also need to be seriously treated. Following from the actual eavesdropping activities, we focus on the communication-based attackability and cyber-physical radio

[1] **Critical**: We specifically define critical functions as important components in rail-CPS that may or may not dictate train safety. To be compared against "Vital" functions.

[2] **Vital**: Vital functions in rail-CPS are those that are directly involved in the enforcement of train movements. According to IEEE standard (IEEE, 2000), vital components are required to be implemented in a fail-safe manner, including those sub-components upon which they depend.

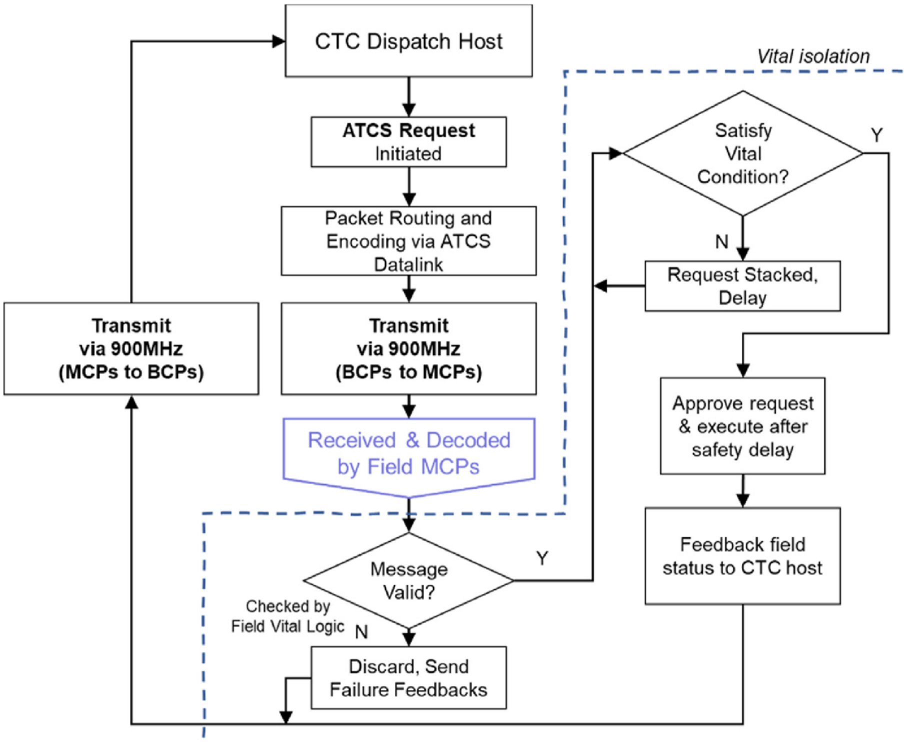

CTC Dispatch Host
ATCS Request Initiated
Packet Routing and Encoding via ATCS Datalink
Transmit via 900MHz (BCPs to MCPs)
Received & Decoded by Field MCPs
Message Valid?
Checked by Field Vital Logic
Y
N
Discard, Send Failure Feedbacks
Transmit via 900MHz (MCPs to BCPs)
Vital isolation
Satisfy Vital Condition?
Y
N
Request Stacked, Delay
Approve request & execute after safety delay
Feedback field status to CTC host

**Fig. 4.** Deduction of message flow in ATCS between CTC host and field vital logics.

interactions inside the CTC-ATCS system. Fig. 3 summarizes a simplified architecture of the ATCS network. The major system users, regular cyber-physical interactions, and location of cyber exposure have been identified accordingly. Specifically, the major system users of the ATCS network include:

- Base communication packages (BCP):

BCPs interface between the ATCS internal network and the mobile communication packages (MCPs), serving as radio base stations. BCPs enable the ATCS radio messages to pass between the CTC dispatch center, and the MCPs that are located at the field signaling locations. The communication link over the 900 MHz radio is the identified location of cyber exposure in this case study.

- Mobile communication packages (MCP) and Wayside interface units (WIU):

MCP and WIU connect the ATCS network with the wayside equipment. They relay and process CTC messages between upstream BCPs and the wayside/lineside units.

- Field vital logics and wayside/lineside units:

These field-side devices communicate with the CTC system through the MCP and WIU. The field vital logics autonomously govern the signaling system to enforce the train movement authorities. It is commonly implemented through programmable logic controllers (PLCs) and the associated signaling apparatus. Wayside/lineside units can serve various rail-CPS systems with non-vital functions such as hot box detectors, or side load detectors. Some of the data is incorporated into the ATCS network for dispatching purposes.

In U.S. CTC systems, dispatchers send CTC command requests through the ATCS radio. The self-governed field vital logics in the interlocking equipment receive and process these requests, either accepting or rejecting them. This mechanism implements a layer of safety isolation between the vital interlocking units and the ATCS system. This isolation achieves the fail-safe mechanism and helps to prevent conflicting train movement authorities from being executed in the field. Shown in Fig. 4, the relevant CTC-ATCS radio messages employ two major paths: *request message path* and *feedback message path*. The request path provides the logic channel that delivers the CTC commands to the field vital logics. Conversely, field vital logics will initiate ATCS feedback messages to the CTC office. Feedback messages may contain the acknowledgment of the request, confirmation of CTC actions, or updates regarding field status with no actions.

The deduction of message flows for ATCS in Fig. 4 facilitated the technical delimitation in risk management. In Fig. 5, we generalize the vital and non-vital threats from ATCS radio links according to their respective attack flows. With the formulated system architecture and deduction of message flows, we make the following statements to justify ATCS as our research subject selection:

- No matter how the CTC internal network and the field vital logics are secured, the ATCS radio link still exposes private messages directly to the public.
- Breaching the PLC-based field vital logics for unsafe train movements often requires physical intrusion. Therefore, we consider such threats to be outside of the scope of the case study.

### 4.2. Technical decomposition: a vital threat

Concerns over spoofing attacks are raised due to the ongoing eavesdropping activities. Spoofing attacks may cause the CTC-ATCS system to inhale unauthorized messages. Although the vital isolation and the autonomy of field vital logics are capable of rejecting messages that conflict with vital safety, there is one special scenario when the vital isolation can be bypassed through ATCS operation, formulated as the red flow in Fig. 5. Based on the working flows and spoofing attack potential, a feature of ATCS implementations called “Blue Block” is identified as one exception, where ATCS spoofing messages may bypass the fail-safe design and pose vital risks.

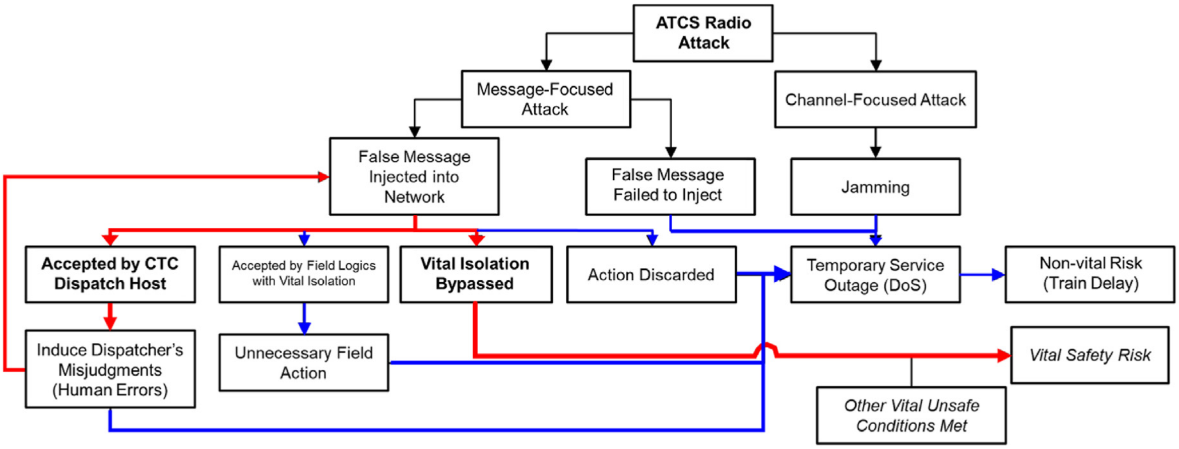

ATCS Radio Attack
Message-Focused Attack
Channel-Focused Attack
False Message Injected into Network
False Message Failed to Inject
Jamming
Accepted by CTC Dispatch Host
Accepted by Field Logics with Vital Isolation
Vital Isolation Bypassed
Action Discarded
Temporary Service Outage (DoS)
Non-vital Risk (Train Delay)
Induce Dispatcher's Misjudgments (Human Errors)
Unnecessary Field Action
Vital Safety Risk
Other Vital Unsafe Conditions Met

**Fig. 5.** Generalized attack flow targeting ATCS radio link.

In a CTC-ATCS system, dispatchers can remotely set the blue protection[3] for a certain track segment for maintenance. This feature is often referred to as the Blue Block.[4] In the field, a Blue Block Switch is in place and remains "connected" in normal CTC operations. When Blue Block is activated, the switch must disconnect and disable the testing signal from being cleared into the protected track. Ideally, it provides an extra layer of protection to further reduce the risk of an unexpected signal clearing (incorrect train movement authorization).

ATCS radio messages in some implementations can directly manipulate the Blue Block Switch (Wang et al., 2019). Jamming and interceptions through the ATCS radio link may impede the requests to establish the Blue Block, counter to the CTC dispatcher's intention. If this happens, the CTC-ATCS system by itself is not able to validate the status of Blue Block. In the worst-case scenario, if any signal testing actions were underway by assuming the Blue Block protection had been in place, the signal might be accidently cleared, and the vital isolation could be bypassed. Fig. 6 shows the conceptual risk scenario of Blue Block signal testing when an unsafe train movement occurs due to an ATCS radio attack. Considering common practices, the standard procedure of ATCS-based Blue Block establishment in many U.S. rail companies incorporates at least voice communications and a checklist for verification. In an operational context, we used the UML sequence diagram (Fig. 7) to fully model the ATCS cyber-physical interactions during the lifecycle of the Blue Block operation. The risky components and activities are identified accordingly and are highlighted for pertinent prevention.

### 4.3. Consequence analysis: abstraction for a non-vital threat

A compromised ATCS system has wide-ranging impacts on rail operations. If the CTC-ATCS radio channel is jammed or spoofing attacks bring down the system, the ATCS stops functioning. This would hamper rail traffic and service at different levels (Fig. 5, blue flow). The radio channel jamming attacks can directly bring down the system; some spoofing attacks may invoke the fail-safe mode, resulting in system degradation. Although these attacks would neither violate vital safety principles nor lead to catastrophic railway accidents like derailments or collisions, they would still create serious service disruptions. In our case study, we regard these attacks as a non-vital threat.

To seek effective remedies, practitioners should first attempt to presume the level of service disruption resulting from these hypothetical DoS attacks and then combat them accordingly. However, the intertwined relationships inside a rail-CPS like ATCS make it complicated to analytically predict the degree of the service outage. It is also inefficient and impractical to analyze the risk through technical decomposition over the large-scale network in the top-down approaches. Additionally, there has been no record of DoS attacks on ATCS serving as empirical references.

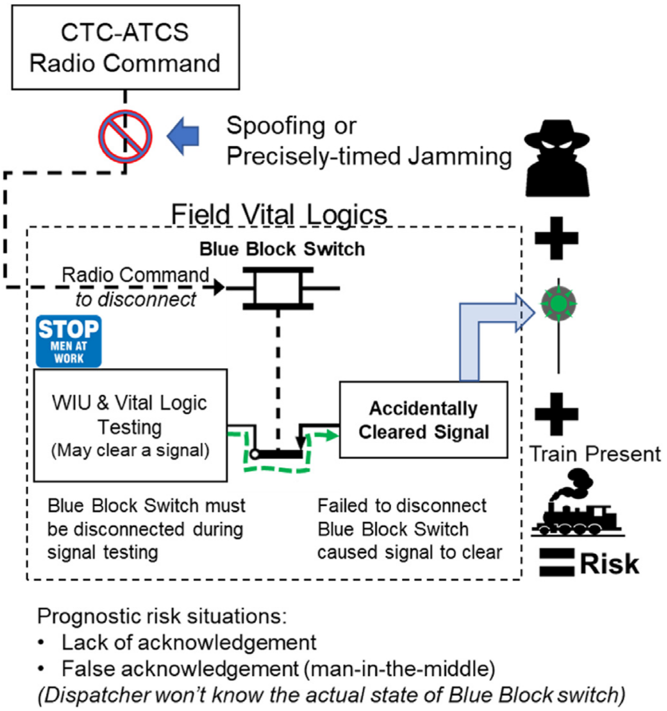

CTC-ATCS Radio Command
Spoofing or Precisely-timed Jamming
Field Vital Logics
Blue Block Switch
Radio Command to disconnect
STOP MEN AT WORK
WIU & Vital Logic Testing (May clear a signal)
Accidentally Cleared Signal
Train Present
Blue Block Switch must be disconnected during signal testing
Failed to disconnect Blue Block Switch caused signal to clear
Risk
Prognostic risk situations:
Lack of acknowledgement
False acknowledgement (man-in-the-middle)
(Dispatcher won't know the actual state of Blue Block switch)

**Fig. 6.** Illustration of the Blue Block vulnerability over ATCS radio attacks: a fictive case during signal testing.

Meanwhile, the normality of rail operations is closely associated with train delay. Likewise, DoS attacks targeting ATCS are fundamentally similar to a period of dispatching and signaling outage with specific durations and locations. Therefore, we select the level of train delay as the quantified metric for threat abstraction in the consequence analysis for the DoS attack. Indicated by train delay, we simplify the consequence (cost of damage) from an ATCS DoS attack as expressed in Eq. (1). Amongst other parameters, we focus only on the train delay for the scope of the current research.

The DoS-induced delay should always depend on the railway's

[3] Blue protection in U.S. rail operations provides safety to maintenance workers by preventing inadvertent train movements.

[4] Blue Block is designed to isolate the track entry signal from field vital logics to prevent an unexpected clear signal that accidently allows trains to enter. It is often used when debugging and configuring field vital logics.

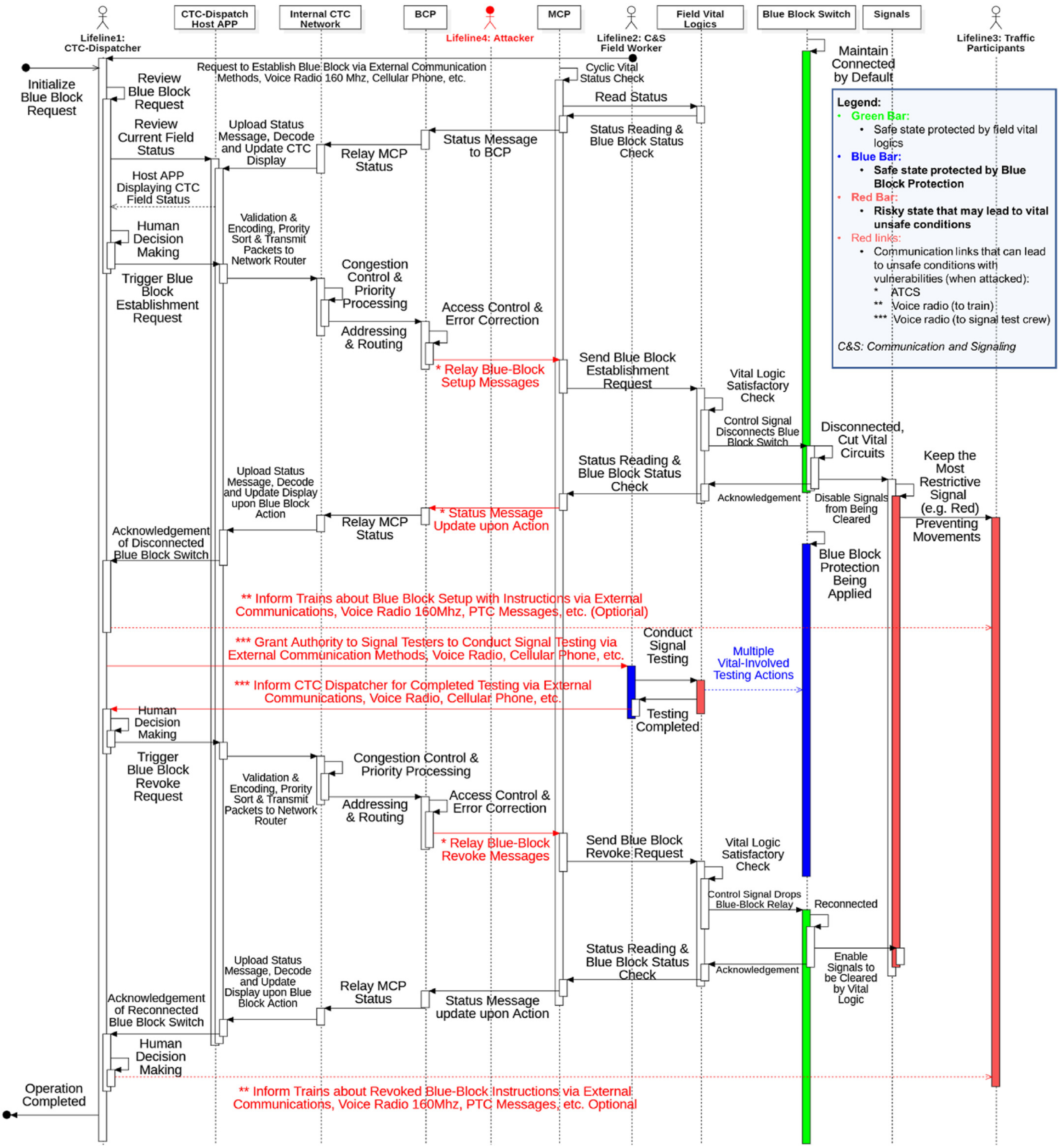

CTC-Dispatch Host APP
Internal CTC Network
BCP
MCP
Field Vital Logics
Blue Block Switch
Signals
Lifeline1: CTC-Dispatcher
Lifeline4: Attacker
Lifeline2: C&S Field Worker
Lifeline3: Traffic Participants
Initialize Blue Block Request
Request to Establish Blue Block via External Communication Methods, Voice Radio 160 Mhz, Cellular Phone, etc.
Cyclic Vital Status Check
Maintain Connected by Default
Review Blue Block Request
Read Status
Review Current Field Status
Upload Status Message, Decode and Update CTC Display
Relay MCP Status
Status Message to BCP
Status Reading & Blue Block Status Check
Host APP Displaying CTC Field Status
Legend:
Green Bar:
Safe state protected by field vital logics
Blue Bar:
Safe state protected by Blue Block Protection
Red Bar:
Risky state that may lead to vital unsafe conditions
Red links:
Communication links that can lead to unsafe conditions with vulnerabilities (when attacked):
* ATCS
** Voice radio (to train)
*** Voice radio (to signal test crew)
C&S: Communication and Signaling
Human Decision Making
Validation & Encoding, Prority Sort & Transmit Packets to Network Router
Trigger Blue Block Establishment Request
Congestion Control & Priority Processing
Access Control & Error Correction
Addressing & Routing
* Relay Blue-Block Setup Messages
Send Blue Block Establishment Request
Vital Logic Satisfactory Check
Control Signal Disconnects Blue Block Switch
Disconnected, Cut Vital Circuits
Keep the Most Restrictive Signal (e.g. Red) Preventing Movements
Status Reading & Blue Block Status Check
Acknowledgement
Disable Signals from Being Cleared
Upload Status Message, Decode and Update Display upon Blue Block Action
Relay MCP Status
* Status Message Update upon Action
Acknowledgement of Disconnected Blue Block Switch
Blue Block Protection Being Applied
** Inform Trains about Blue Block Setup with Instructions via External Communications, Voice Radio 160Mhz, PTC Messages, etc. (Optional)
*** Grant Authority to Signal Testers to Conduct Signal Testing via External Communication Methods, Voice Radio, Cellular Phone, etc.
Conduct Signal Testing
Multiple Vital-Involved Testing Actions
*** Inform CTC Dispatcher for Completed Testing via External Communications, Voice Radio, Cellular Phone, etc.
Testing Completed
Human Decision Making
Trigger Blue Block Revoke Request
Validation & Encoding, Prority Sort & Transmit Packets to Network Router
Congestion Control & Priority Processing
Access Control & Error Correction
Addressing & Routing
* Relay Blue-Block Revoke Messages
Send Blue Block Revoke Request
Vital Logic Satisfactory Check
Control Signal Drops Blue-Block Relay
Reconnected
Enable Signals to be Cleared by Vital Logic
Status Reading & Blue Block Status Check
Acknowledgement
Upload Status Message, Decode and Update Display upon Blue Block Action
Relay MCP Status
Status Message update upon Action
Acknowledgement of Reconnected Blue Block Switch
Human Decision Making
Operation Completed
** Inform Trains about Revoked Blue-Block Instructions via External Communications, Voice Radio 160Mhz, PTC Messages, etc. Optional

**Fig. 7.** Complete sequence diagram modeling for Blue Block establishment and prognostic risks over ATCS radio link.

network topology and realistic traffic patterns. Common practices in the rail industry use software-based rail traffic simulation to evaluate delay levels. In the case study, we developed a customized DoS attack simulation software based on Python 3 and the NetworkX package (Hagberg et al., 2008). In our simulation, delay $T_{i\text{arrival}}^{\text{impacted}} - T_{i\text{arrival}}^{\text{scheduled}}$ are calculated as Eqs. (2) and (3) below:

$$C_{\text{TOTAL}} = \sum_{i}^{N} C_i \times \left(T_{i\text{arrival}}^{\text{impacted}} - T_{i\text{arrival}}^{\text{scheduled}}\right) + \sum_{j}^{M} K_j + C_{\text{Misc.}} \tag{1}$$

$$T_{i\text{arrival}}^{\text{scheduled}} = f\left(G_{\text{Network}}, \{t_{\text{current}}\}, O\right) \tag{2}$$

$$T_{i\text{arrival}}^{\text{impacted}} = f\left(G_{\text{Network}}, \{t_{\text{current}}\}, O, T_{\text{DoS}}, L_{\text{DoS}}\right) \tag{3}$$

where $C_{\text{TOTAL}}$ is the total monetary impact resulting from the DoS attack,

$C_i$ is the monetary impact per hour to the delayed train $i$, $K_j$ is the total monetary impact for the cancelled train $j$, $C_{\mathrm{Misc.}}$ is the total monetary impact of miscellaneous recovery tasks (e.g., maintenance and repair), $T_{i\,\mathrm{arrival}}^{\mathrm{impacted}}$ is the impacted arrival time for train $i$ after DoS attacking the ATCS system, $T_{i\,\mathrm{arrival}}^{\mathrm{scheduled}}$ is the scheduled arrival time for train $i$, $O$ is the operational logics of the corridor (e.g., signaling, dispatching, and train priorities), $T_{\mathrm{DoS}}$ is the duration of the DoS attack, $L_{\mathrm{DoS}}$ is the location of the DoS attack, $G_{\mathrm{Network}}$ is the topology and infrastructure profile of the rail corridor, and $\{t_{\mathrm{current}}\}$ is the set of currently scheduled trains.

Our simulation model (Fig. 8, left) assumes that a successful DoS attack on the CTC-ATCS system would trigger the stop signal for affected locations, and the affected trains would react accordingly by obeying signals, introducing traffic congestion. When the DoS attack stops, the CTC-ATCS system resumes its full function with rational dispatching actions. For normal train schedules, the simulator seeds a randomized set of parameters for generality before the schedule calculation. The same set of parameters is then persisted to calculate train delay under DoS attacks, with consistent simulator configurations.

The simulation parameters and results are summarized in Table 2. The current configurations define a hypothetical single-track, fixed block, four-aspect signaling rail corridor with unidirectional train traffic. Although the settings in our case study do not represent any realistic lines, they profile many U.S. freight lines with reasonable simplifications. Therefore, it can also be adapted by practitioners with specific interests to generate practical results. The system model (left) and visualization of the simulated train delay (right) are shown in Fig. 8.

According to the simulation results from our setup, on the one-directional single-track corridor with redundant capacity, a 1-h DoS attack can result in almost 9 h of cascading train delays. In this case, the traffic could eventually recover. However, in other extreme cases with saturated traffic, recovery may not even be an option unless trains are cancelled. Therefore, to accurately simulate the consequence of the DoS attack on the CTC-ATCS system, we advocate for the definition and careful modeling of the following simulation parameters for each case:

- DoS time, duration, and location.
- Network topology and CTC-ATCS coverage of the railway.
- Traffic patterns and operational logics.
- Models, logics, and train cancellation plans for the recovery from DoS attack.

### 4.4. *Mitigation strategies and recovery solutions*

By far, the U.S. rail industry maintains the use of legacy ATCS protocol for cost saving purposes. The identified risks of CTC-ATCS are still valid. For the identified threats in this case study, the risk profiles are outlined accordingly:

- For the vital threat of spoofing the Blue Block, the detailed sequence diagram (Fig. 7) has effectively summarized our prognosis for the potential attacks.
- For the non-vital threat of DoS attacks, the risk profile has been abstracted to the level of consequence, represented by train delay. The specific consequence would vary by specific cases, which can be quantified by simulation analyses with realistic inputs.

It is noteworthy that the presented case study only consists of a single-round risk management procedure. The cyber risk management loop should continue for other components within the chosen rail-CPS and other rail-CPS systems to expand the coverage of preventive security enhancement efforts. According to the case study results, the following recommendations are made to properly handle the identified risks for ATCS itself and for similar rail-CPS subjects in other domains and realms.

#### 4.4.1. *Comments and notes on vital risks: of and beyond the Blue Block threat*

Generally, due to multiple layers of required human verifications in railway operational rules, any risks like spoofing a Blue Block of U.S. ATCS system to breach vital system are still mostly under the control of authorities and stakeholders. For the Blue Block threat, the identified vital risk consists of both attacking the ATCS radio messages, and compromising the voice communication channels to create “advantageous conditions” of human error. Therefore, it is always necessary to reinforce rule compliance for employees to conduct vital activities such as ATCS Blue Block.

As commonly practiced by worldwide rail operators, multi-verification of messages is always required in vital activities. Therefore, such administration-level risk mitigation strategies can greatly increase the onerousness for attackers to achieve their goal of vital safety breach. In the meantime, technical upgrades are still required to solve cyber risks at the root.

#### 4.4.2. *Radio carrier and other cyber security upgrades*

U.S. ATCS’s 900 MHz unencrypted radio link paved the way for security risks. Therefore, communication-based critical rail-CPS systems should always embrace newer security upgrades and deprecate legacy technologies. Conversely, traditional industries like the railway tend to have attachments to legacy technologies. For example, continuous service availability requirements and minimal downtime tolerance prevent the deployment of the newest technologies with security enhancement. We therefore provide the following justifiable strategies not only to mitigate the identified risks for ATCS, but also to infer the cyber robustness improvement for similar systems.

*4.4.2.1. Move to cutting-edge wireless solutions.* Both jamming and spoofing attacks on a narrow-band radio like ATCS could be made much more difficult with current wireless technologies. Earlier on, the U.S. rail industry has evaluated the 802.11 protocol (spread spectrum on unlicensed frequencies) and the CDMA (cell phone spread spectrum on licensed frequencies) protocol as possible alternatives to ATCS narrow-band radio (Craven and Craven, 2008). Current developments such as 5G and Wi-Fi mesh present much better privacy and robustness against interference. In a perfect world, these legacy radios would be replaced altogether. However, given the earlier advocation of replacing ATCS narrow-band with CDMA staying on paper, the reluctance of the industry to adopt upgrades is assumed.

*4.4.2.2. Fall back solutions: alternative carriers.* Another effective alternative, which would be less costly than a complete migration, is to use an entirely different carrier as a backup for radio communications. For example, sticking with the ATCS protocol, some eastern U.S. rail operators have instead deployed fiber-optics to substitute for the narrow-band link in their CTC systems. If similar protocols are deployed within a small area, a local area network (LAN) is also an effective and secure method as compared to the unencrypted radio link.

To improve system redundancy and reliability, some U.S. rail operators have already elected to back up their narrow-band ATCS radio link service over commercial cellular carriers. Although these operators still prioritize their licensed 900 MHz band to save costs, such backups can be switched over when the ATCS narrow-band is down, and effectively combat jamming/DoS attacks.

The U.S. positive train control (PTC) communication protocol on the dedicated 220 MHz band was rolled out much later than ATCS. The PTC radio came with a native design of security and encryption. Likewise, piggybacking the ATCS packets over PTC is feasible to eliminate ATCS vulnerabilities. Similar activities exist in European railways, where voice radio communications have been switched from analog to digitized GSM-R, a more secure radio link owned by railways.

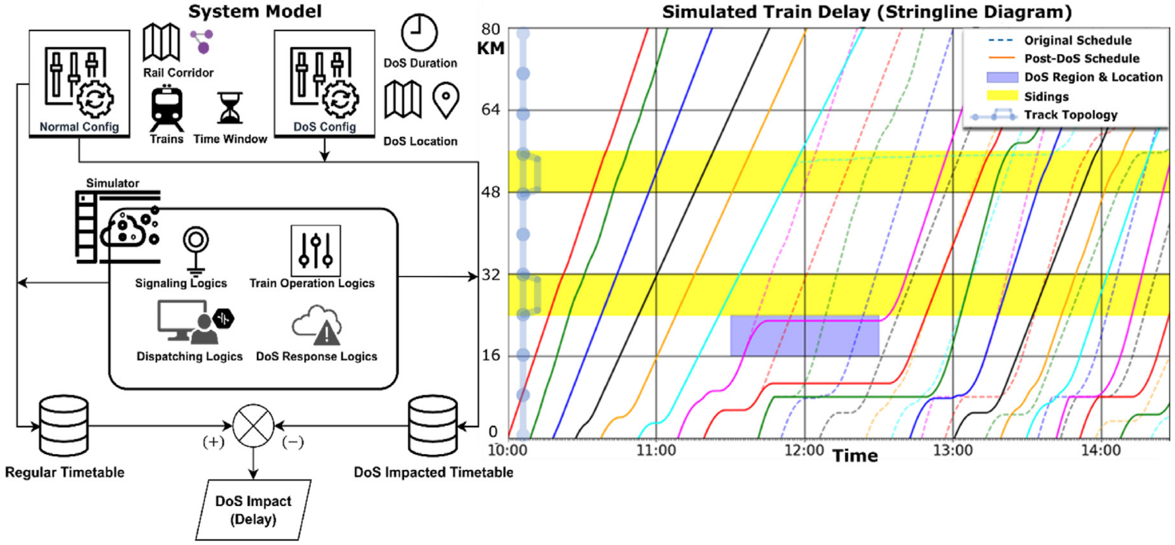


**Fig. 8.** Left: the simulation-based system model for DoS consequence analysis. Right: train delay stringline diagram of the simulated DoS attack (snapshot, showing the first 4.5 h).

**Table 2**
ATCS-DoS train delay simulation setups and simulation results.

| Simulation Parameter | Value | Simulation Results | Value |
|---|---|---|---|
| Total Number of Trains | 10 | Number of Delayed Trains | 47 |
| Length of Block | 8 km (5 miles) | Number of Cancelled Trains | 0 |
| Total Number of Blocks | 10 | Cumulative Delay | 24.9 train-hours |
| Mean Train Speed | 86 kph (54 mph) | Average Train Delay | 0.53 h |
| Mean Train Acceleration | 9.6 kph/min (6 mph/min) | Maximum Train Delay | 1.9 h |
| Mean Train Deceleration | 96 kph/min (60 mph/min) | Recovery Time | 8.6 h |
| DoS Duration | From 11:30 to 12:30 (1 h) | – | – |
| DoS Location | The 3rd block (not siding) | – | – |
| Mean Headway | 1000 s | – | – |

## 5. Conclusions

This study presents a new methodology for cyber security risk management for rail-CPSs, covering the procedures of threat identification, technical decomposition, consequence analysis, and recovery solutions. Especially, we underline two important procedures for the best results to practice the methodology:

- Cyber-physical decomposition.
- Approach from physical components to cyber components.

To visualize the emphasized procedures, we practiced the cyber risk management methodology on a case study from the U.S. CTC-ATCS system. Both a vital and a non-vital threat for the subject have been handled:

- Vital: we conducted technical decomposition for the Blue Block testing threat with sequence diagram modeling.
- Non-vital: we conducted consequence analysis for the DoS threat via simulation, modeling the consequence by delay.

The cyber risk management of the case study calls for industry awareness before the risks being exploited by imposters. It can help the current U.S. railway operators to evaluate the security profile and urgency for upgrades of their ATCS systems.

Equally contributive in this paper is the joint reference by the case study and the methodology. In the methodology, we proposed the top-down (technical decomposition) and the bottom-up (consequence analysis) approaches, both of which have been validated in the case study. This remarked the efficacy and flexibility of the methodology for application to general rail-CPSs: cyber risk profiles can be effectively outlined by at least one approach from this methodology. Further refinements and adaptations of the methodology can be made possible with further applications to different rail-CPS cases.

## Replication and data sharing

The codes for reproducing the simulation results reported in the case study of the paper are available at https://github.com/hegxiten/PyRailSim. The data of the simulation can be re-generated from the execution of the simulation, and the input parameters are available in the configuration files of the repository.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements and disclaimer

This study was supported by a research grant from the Federal Railroad Administration (FRA) of the U.S. Department of Transportation (USDOT) (Grant No. DTFR5317C00018). The authors thank Mr. Brian Sykes, Dr. Duminda Wijesekera, and Dr. Mark Hartong for providing their profound industry knowledge, advice, and kind support. The views

and opinions expressed herein are those of the authors and do not necessarily state or reflect those of the USDOT or the FRA, and shall not be used for advertising or product endorsement purposes.

## References

Adin, I., Mendizabal, J., Portillo, J. del, 2012. Impact of electromagnetic environment on reliability assessment for railway signalling systems. In: Railway Safety, Reliability, and Security: Technologies and Systems Engineering. IGI Global.

Ali, S., Al Balushi, T., Nadir, Z., Hussain, O.K., 2018. Cyber Security for Cyber Physical Systems, vol. 768. Springer International Publishing.

Andre'B, A., 2014. Combining Operational and Spectrum Characteristics to Form a Risk Model for Positive Train Control Communications. Ph.D. Dissertation. George Mason University.

Association of American Railroads, 2005. Manual of Standards and Recommended Practices Section K-II: Railway Electronics.

Bandara, K.R.D.S., Kolli, S., Wijesekara, D., 2017. *Secure Intelligent Radio For Trains (SIRT)*. 2017 Joint Rail Conference.

Bantin, C.C., Siu, J., 2011. Designing a secure data communications system for automatic train control. Proc. Inst. Mech. Eng. - Part F J. Rail Rapid Transit 225 (4), 395–402.

Bastow, M.D., 2014. Cyber security of the railway signalling amp; control system. In: 9th IET International Conference on System Safety and Cyber Security (2014), pp. 1–5.

Bergman, R., 2021. Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains (The New York Times).

Bezzateev, S., Voloshina, N., Sankin, P., 2013. Joint Safety and Security Analysis for Complex Systems. *2013 13th Conference of Open Innovations Association (FRUCT)*, vols. 3–13.

Bloomfield, R., Bloomfield, R., Gashi, I., Stroud, R., 2012. How secure is ERTMS? In: Ortmeier, F., Daniel, P. (Eds.), In *Computer Safety, Reliability, and Security*. Springer, pp. 247–258.

Bondavalli, A., Ceccarelli, A., Grønbæk, J., Iovino, D., Kárná, L., Klapka, Š., Madsen, T.K., Magyar, M., Majzik, I., Salzo, A., 2009. Design and evaluation of a safe driver machine interface. Int. J. Perform. Eng. 5 (2), 153.

Burmester, M., Magkos, E., Chrissikopoulos, V., 2012. Modeling security in cyber–physical systems. Int. J. Crit. Infrastruct. Protect. 5 (3), 118–126.

Chang, S.-Y., Cai, S., Seo, H., Hu, Y.-C., 2017. Key update at train stations: two-layer dynamic key update scheme for secure train communications. In: Security and Privacy in Communication Networks, pp. 125–143.

Chang, S.-Y., Tran, B.A.N., Hu, Y.-C., Jones, D.L., 2015. Jamming with power boost: leaky waveguide vulnerability in train systems. In: 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS), pp. 37–43.

Chen, B., Schmittner, C., Ma, Z., Temple, W.G., Dong, X., Jones, D.L., Sanders, W.H., 2015. Security analysis of urban railway systems: the need for a cyber-physical perspective. In: Koornneef, F., van Gulijk, C. (Eds.), Computer Safety, Reliability, and Security. Springer International Publishing, pp. 277–290.

Chen, L., Shan, Z., Tang, T., Liu, H., 2011. Performance analysis and verification of safety communication protocol in train control system. Comput. Stand. Interfac. 33 (5), 505–518.

Chernov, A.V., Butakova, M.A., Karpenko, E.V., 2015. Security incident detection technique for multilevel intelligent control systems on railway transport in Russia. In: 2015 23rd Telecommunications Forum Telfor (TELFOR), pp. 1–4.

Chothia, T., Ordean, M., de Ruiter, J., Thomas, R.J., 2017. An attack against message authentication in the ERTMS train to trackside communication protocols. In: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp. 743–756.

Craven, P.V., 2004. A brief look at railroad communication vulnerabilities. In: Proceedings. The 7th International IEEE Conference on Intelligent Transportation Systems. IEEE Cat. No.04TH8749), pp. 245–249.

Craven, P.V., Craven, S., 2008. Security of ATCS Wireless Railway Communications, pp. 227–238.

de Ruiter, J., Thomas, R.J., Chothia, T., 2016. A formal security analysis of ERTMS train to trackside protocols. In: Lecomte, T., Pinger, R., Romanovsky, A. (Eds.), Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. Springer International Publishing, pp. 53–68.

DiMase, D., Collier, Z.A., Heffner, K., Linkov, I., 2015. Systems engineering framework for cyber physical security and resilience. Environ. Syst. Decisions 35 (2), 291–300.

Emmelmann, M., Bochow, B., Kellum, C., 2010. Vehicular Networking: Automotive Applications and beyond. John Wiley & Sons.

Gallagher, R., 2022. Belarus Hackers Allegedly Disrupted Trains to Thwart Russia. BloombergQuint.

Grønbæk, J., Madsen, T.K., Schwefel, H.P., 2008. Safe Wireless Communication Solution for Driver Machine Interface for Train Control Systems. Third International Conference on Systems (Icons 2008), pp. 208–213.

Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain. Cities Soc. 50, 101660.

Hagberg, A.A., Schult, D.A., Swart, P.J., 2008. Exploring network structure, dynamics, and function using NetworkX. In: Proceedings of the 7th Python in Science Conference (SciPy 2008),, pp. 11–15.

Harshan, J., Chang, S.-Y., Kang, S., Hu, Y.-C., 2017. Securing balise-based train control systems using cryptographic random fountains. In: 2017 IEEE Conference on Communications and Network Security (CNS), pp. 405–410.

Hartong, M., Goel, R., Wijesekera, D., 2008. Securing positive train control systems. In: Goetz, E., Shenoi, S. (Eds.), Critical Infrastructure Protection. Springer US, pp. 57–72.

Hartong, M., Goel, R., Wijesekera, D., 2012. Mapping Misuse Cases to Functional Fault Trees in Order to Secure Positive Train Control Systems, pp. 394–399.

Heddebaut, M., Gransart, S.M., Ch, Rioult, J., 2015. SECRET SECurity of Railways against Electromagnetic aTtacks.

IEEE, 2000. IEEE standard for verification of vital functions in processor-based systems used in rail Transit control. IEEE Std 1483–2000, 1–36.

Lakshminarayana, S., Teng, T.Z., Tan, R., Yau, D.K.Y., 2018. Modeling and detecting false data injection attacks against railway traction power systems. ACM Trans. Cyber-Phys. Syst. 2 (4), 1–29.

Lakshminarayana, S., Teo, Z.-T., Tan, R., Yau, D.K.Y., Arboleya, P., 2016. On false data injection attacks against railway traction power systems. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. DSN), pp. 383–394.

Leyden, J., 2008. Polish Teen Derails Tram after Hacking Train Network.

Lim, H.W., Temple, W.G., Tran, B.A.N., Chen, B., Kalbarczyk, Z., Zhou, J., 2019. Data Integrity Threats and Countermeasure Railway Spot Trans. Syst. ACM Trans. Cyber-Phys. Syst. 4, 1–26.

Liu, X., Wijesekera, D., Wang, Z., Jablonski, M., Wang, Y., Yavvari, C., Holt, K., Sykes, B., 2020. Cyber Security Risk Management for Connected Railroads. United States. Department of Transportation. Federal Railroad Administration.

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. Comput. Electr. Eng. 47, 275–285.

Masson, É., Gransart, C., 2017. Cyber security for railways – a huge challenge – shift2Rail perspective. In: Pirovano, A., Berbineau, M., Vinel, A., Guerber, C., Roque, D., Mendizabal, J., Bonneville, H., Aniss, H., Ducourthial, B. (Eds.), Communication Technologies for Vehicles. Springer International Publishing, pp. 97–104.

McGoogan, C., Willgress, L., 2016. UK Rail Network Hit by Multiple Cyber Attacks Last Year.

Melaragno, A., Bandara, K.R.D.S., Fewell, A., Wijesekera, D., 2016. Rail radio intrusion detection system (RRIDS) for communication based train control (CBTC). In: 2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT), pp. 39–48.

Mili, S., Deniau, V., Sodoyer, D., Heddebaut, M., Ambellouis, S., 2015. Jamming detection methods to protect railway radio communication. Methods 4 (7).

Mo, Y., Kim, T.H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., Sinopoli, B., 2012. Cyber–physical security of a smart grid infrastructure. In: Proceedings of the IEEE, vol. 100, pp. 195–209, 1.

Neuman, D.C., 2009. Challenges in Security for Cyber-Physical Systems.

Nguyen, H.H., Tan, R., Yau, D.K.Y., 2015. Impact of signal delay attack on voltage control for electrified railways. In: TENCON 2015-2015 IEEE Region 10 Conference, pp. 1–3.

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. In: Mendizabal, J., Berbineau, M., Vinel, A., Pfletschinger, S., Bonneville, H., Pirovano, A., Plass, S., Scopigno, R., Aniss, H. (Eds.), Communication Technologies for Vehicles. Springer International Publishing, pp. 98–100.

Reuters, 2022. Italy's State Railway May Have Been Target of Cyber Attack. Reuters.

Rodríguez-Piñeiro, J., Fraga-Lamas, P., García-Naya, J., Castedo, L., 2012. Long Term Evolution Security Analysis for Railway Communications.

Ross, R., McEvilley, M., Carrier Oren, J., 2016. Systems Security Engineering: Considerations For a Multidisciplinary Approach In the Engineering Of Trustworthy Secure Systems. National Institute of Standards and Technology (NIST SP 800-160; p. NIST SP 800-160).

Schlehuber, C., Heinrich, M., Vateva-Gurova, T., Katzenbeisser, S., Suri, N., 2017. A security architecture for railway signalling. In: Tonetta, S., Schoitsch, E., Bitsch, F. (Eds.), Computer Safety, Reliability, and Security. Springer International Publishing, pp. 320–328.

Sternstein, A., 2012. Hackers Manipulated Railway Computers, TSA Memo Says. Nextgov.Com.

Temple, W.G., Li, Y., Tran, B.A.N., Liu, Y., Chen, B., 2017a. Railway system failure scenario analysis. In: Havarneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S. (Eds.), Critical Information Infrastructures Security, vol. 10242. Springer International Publishing, pp. 213–225.

Temple, W.G., Tran, B.A.N., Chen, B., Kalbarczyk, Z., Sanders, W.H., 2017b. On train automatic stop control using balises: attacks and a software-only countermeasure. In: 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing. PRDC), pp. 274–283.

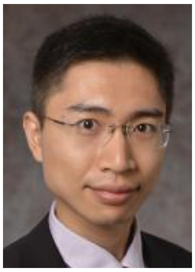
Teo, Z.-T., Tran, B.A.N., Lakshminarayana, S., Temple, W.G., Chen, B., Tan, R., Yau, D.K.Y., 2016. SecureRails: towards an open simulation platform for analyzing cyber-physical attacks in railways. In: 2016 IEEE Region 10 Conference (TENCON), pp. 95–98.

Wang, Z., Liu, X., Wang, Y., Yavvari, C., Jablonski, M., Wijesekera, D., Sykes, B., Holt, K., 2019. *Cyber Security Analysis For Advanced Train Control System (ATCS) in CTC Systems: Concepts And Methods*. 2019 Joint Rail Conference.

Xu, Z., Zhu, Q., 2017. A game-theoretic approach to secure control of communication-based train control systems under jamming attacks. Proc. 1st Int. Workshop on Safe Control of Connected and Autonomous Veh. 27–34.

Yampolskiy, M., Horváth, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J., 2015. A language for describing attacks on cyber-physical systems. Int. J. Crit. Infrastruct. Protect. 8, 40–52.

**Zezhou Wang** received his M.S. degree in civil engineering from the University of Illinois at Urbana Champaign in 2018. He is a current Ph.D. student at Rutgers University in civil engineering, and also dual-majored as a Master student in electrical and computer engineering. His research interests include railway cyber security, signaling and communications, railway ITS and train control.



**Xiang Liu** received his Ph.D. degree from the University of Illinois at Urbana Champaign and is an Associate Professor in the Department of Civil and Environmental Engineering at Rutgers University. Dr. Liu is the director of the Rutgers Rail and Transit Program (RTP), leading and managing a portfolio of rail-centric research, education, and workforce development initiatives, supported by a variety of U.S. public and private sectors. Dr. Liu's research focuses on developing and testing advanced technologies for improving rail operational safety & efficiency. Dr. Liu has published over 100 papers in peer-reviewed journals and at international conferences. Dr. Liu is the Associate Editor for *Journal of Rail Transport Planning & Management* and *Smart and Resilient Transportation*.