Security Analysis of Urban Railway Systems: The Need for a Cyber-Physical Perspective

Binbin Chen[1], Christoph Schmittner[2], Zhendong Ma[2], William G. Temple[1],
Xinshu Dong[1], Douglas L. Jones[31], and William H. Sanders[3]

[1] Advanced Digital Sciences Center, Singapore
binbin.chen@adsc.com.sg, william.t@adsc.com.sg, xinshu.dong@adsc.com.sg
[2] Austrian Institute of Technology, Austria
christoph.schmittner.fl@ait.ac.at, zhendong.ma@ait.ac.at
[3] University of Illinois at Urbana-Champaign, IL
dl-jones@illinois.edu, whs@illinois.edu

Abstract. Urban railway systems are increasingly relying on information and communications technologies (ICT). This evolution makes cybersecurity an important concern, in addition to the traditional focus on reliability, availability, maintainability and safety. In this paper, we examine two examples of cyber-intensive systems in urban railway environments—a communications-based train control system, and a mobile app that provides transit information to commuters—and use them to study the challenges for conducting security analysis in this domain. We show the need for a cyber-physical perspective in order to understand the cross-domain attack/defense and the complicated physical consequence of cyber breaches. We present security analysis results from two different methods that are used in the safety and ICT security engineering domains respectively, and use them as concrete references to discuss the way to move forward.

Keywords: security analysis, urban railway systems, cyber-physical systems, railway safety

1 Introduction

Information and communications technologies (ICT) play a vital role in helping railway operators improve their system safety and service reliability, provide higher transit capacity, and keep the costs of building, operating, and maintaining their infrastructure in check. For example, many urban transportation systems around the world have deployed some form of communications-based automatic train control (e.g., [1], [2]). In those systems, multiple cyber components, including wireless communication, software-defined control logic, and near-real-time data visualization at control centers, have been introduced to replace their conventional physical counterparts. As another example, with smart phones becoming ubiquitous, transit operators (e.g., [3], [4]) are introducing mobile apps to provide consumers with information about train schedules, as well as push-notifications about emergency events or other relevant information.

While the benefits of *digitizing* urban railway systems are obvious, the potential implications of this evolution could be multi-faceted and profound, especially when it comes to the issue of security. For older railway systems, where train protection is based on track circuits and mechanical relay signaling, the security concerns reside primarily in the physical domain. In comparison, the ICT components used in newer automatic train control systems expose additional cyber attack surfaces, which could allow sophisticated attackers to combine cyber attack vectors with physical attack means to achieve malicious goals. This makes it difficult to assess the security of digitized urban railway systems using traditional approaches (e.g., safety analysis methods) that are most familiar to transit operators and other stakeholders. At the same time, security analysis approaches used in other ICT systems (e.g., enterprise networks) are also not readily applicable to urban railway systems, since cyber components can have complicated interactions with the physical assets, or even passengers (e.g., with a false notification through a mobile app).

In this work, we take a close look at two concrete examples of cyber-intensive systems used in urban railway environments—a communications-based train control (CBTC) system and a mobile transit information app—and use them to analyze the cyber-physical security challenges introduced by the digitization of urban railway systems. At the high level, we identify two key challenges:

- **Cross-domain attack and defense:** For a digitized urban railway system, with its many components that span a large geographic area in the physical domain and interconnect with each other in the cyber domain, attack and defense can manifest in multiple stages, involving both cyber and physical actions.
- **Physical-domain consequences from cyber breaches:** Security breaches in the cyber domain, such as falsified information or malicious control logic, can have a complicated impact on the physical domain, which is also subject to an urban railway system's underlying design features, such as fail-safe mechanisms.

The evolution of urban railway systems requires the corresponding evolution of security analysis methodologies—in particular, the need for encompassing a systematic cyber-physical perspective. In the second part of this work, we make an initial attempt to apply existing security analysis approaches for the CBTC and mobile transit information app cases. We use these two examples to illustrate the implications of the two challenges mentioned above. In particular, we find that in the CBTC example, the Failure Modes, Vulnerabilities and Effects Analysis (FMVEA) approach [5], which originates from the safety engineering domain, provides a convenient starting point, since the primary concern in train signaling is avoiding "hazards" such as train collisions or derailments, regardless of whether they are caused by cyber or physical means. However, new extensions are needed to better model the complicated cross-domain multi-stage attacks. On the other hand, in the second example of a mobile transit information app where the delivery of accurate, relevant, and timely information is the key, we find attack tree analysis [6], which is used widely in ICT systems, can serve as a natural starting point, although further extension to better understand the physical consequences of cyber security breaches is necessary.

In summary, we analyze the cyber-physical security implications of the ongoing evolution of urban railway systems, present analysis results obtained from two different methods, and use them as concrete references to discuss the way to move forward. We begin by discussing features of urban railway systems and describing the two example cases in Section 2. In Section 3 we present our efforts to apply different methods to analyze the security risk in the two cases. In Section 4 we summarize our findings and provide additional recommendations for future work. We then conclude in Section 5.

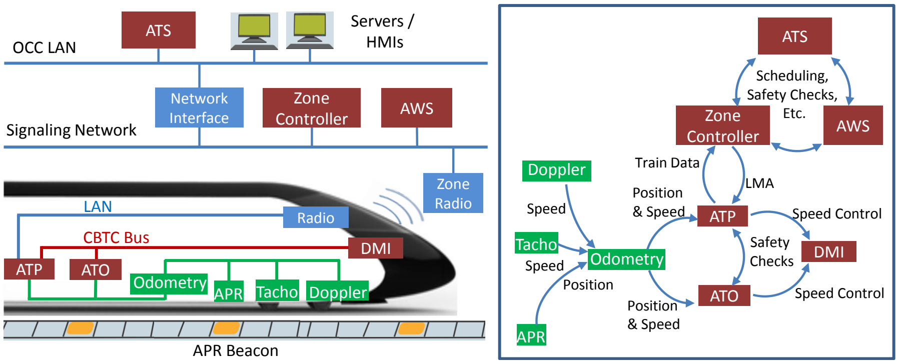

Fig. 1. An example CBTC system and its simplified data flow for LMA determination.

2 Railway Security Risks and Implications

To provide safe, dependable, and efficient transportation service, a rail transport operator needs to coordinate dozens of different systems, including, e.g., the railway signalling system, fire detection/suppression system, ventilation system, traction power system, passenger information system, and fare collection system. The increasing reliance of such systems on ICT introduces cybersecurity risks with complex cyber-physical implications, as exemplied by the two scenarios we describe next.

2.1 Scenario 1: Risks in CBTC Systems

The train control/railway signaling system is a safety-critical system that lies in the core of a railway infrastructure. It can be implemented in diverse forms: from a purely manual form as in the early days, to a fully automatic form as in the communications-based train control (CBTC) systems that serve many cities today. Traditionally, fixed block signaling is used, where the track is divided into physical sections, and no more than one train is allowed in each section. Today's urban railway systems increasingly use a moving block design, which gets rid of the fixed blocks so the block locations and lengths can be dynamically changed according to train location, weight and speed. One primary advantage of a moving block system is that the spacing between trains is reduced, allowing for higher capacity for transit operators.

Broadly speaking, a CBTC system [7] consists of trainborne systems, wayside systems, and a central management system, which are all connected continuously through high-speed data communication networks, as shown in the left subfigure of Fig. 1. They implement automatic train protection (ATP), automatic train operation (ATO), and automatic train supervision (ATS) functions. The right subfigure of Fig. 1 shows a simplified data flow diagram for some key CBTC operations. The train determines its position and speed based on data from onboard sensors (tachometer, Doppler) and data from the absolute position reference (APR) beacons located on the track. It submits train data (including position and speed) via the radio-based communication link to the wayside system, which is further connected with the central ATS system located at the operations control center (OCC). In a fully-automated CBTC system, zone controllers use the high-resolution train information to determine for trains their limit of movement authority (LMA), which describes the distance on the tracks until the next obstacle. A zone controller sends individual commands to each train under its control. The trainborne ATP and ATO systems then use the LMA information in conjunction with local train data to issue appropriate train control commands to the train, typically through some driver machine interface (DMI). Many CBTC systems also include auxiliary wayside systems (AWS), which implement auxiliary functionalities (e.g., interlocking) that can provide a "fall-back" signaling system if some other CBTC components become faulty.

Cyber-physical challenges for analyzing CBTC's security risk. By using radio-based digital transmission (instead of track circuits) to determine train location and perform train-trackside data communications, CBTC can increase the capacity, reduce the amount of wayside equipment needed, and improve the reliability. However, the new digital elements in CBTC — the passive APR beacons that provide accurate localization to trains, the trainborne and wayside systems that implement control logic in software, the radio-based communication system, and the central ATS at the OCC all present potential new attack surfaces. These components are interconnected, and engineered with various safety-enhancing mechanisms, e.g., physical access control, redundant data sources and networks, and fault-response procedures. This complexity makes it challenging to analyze the security level of such a system. In particular, an attacker can start from a physically less protected component (e.g., devices used by system maintenance staff), exploit a series of system vulnerabilities to compromise more critical ones, along the way leveraging or bypassing various safety-enhancing mechanisms, and finally use the compromised critical components to cause physical consequences.

2.2 Scenario 2: Risks in Mobile Transit Information Apps

The complicated coupling of different systems in an urban railway can lead to security implications with cascading effects. For example, while the public address (PA) or public information display (PID) systems do not directly impose safety issues, abusing those systems can potentially lead to overcrowding which could indirectly impact the passengers' safety. Also, for a rail transit operator, there are important non-safety-related security concerns: for example, whether an attack will cause interruption or degradation of service, leakage of information, loss of fare revenue, or damage to their reputation. This is the focus of our second risk scenario.

Traditionally in public transit systems, the operators at the operations control center and individual train stations broadcast traffic update information to commuters via the PID and PA systems. Beyond ordinary information such as train arrival times, those systems are also used to inform commuters of incidents, delays and even the crowdedness of certain routes, to advise them on alternative routes and means of transportation. Recently, urban rail systems have started to extend such information updates to mobile apps installed on commuters' mobile devices (e.g., [3] [4]). For simplicity, we call them *PID apps* in this paper. PID apps can also push messages to end users regarding specific incidents, enabling commuters to plan adjustments to their route ahead of time. However, such extended PID or PA channels could be misused.

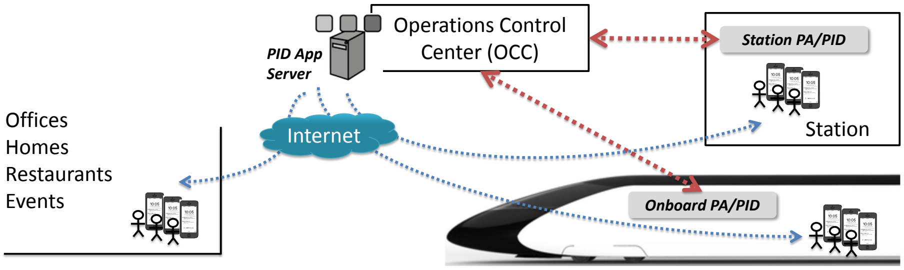

Fig. 2. Railway PA/PID systems, simplified from [8].

Cyber-physical challenges for analyzing PID apps security risk. As Fig. 2 illustrates, the emerging adoption of PID apps has complicated the landscape of passenger traffic updates with additional channels and terminals that are much harder to properly secure. Although traditional PID/PA systems are clearly not immune from cyber threats, attackers would have to gain non-trivial physical access to well-guarded control rooms or direct connections with in-station PID or PA systems before they could launch attacks. These physical proximity requirements limit the time, venue, as well as scale of the attacks, and can easily expose attackers to monitoring systems and security personnel. On the other hand, the traffic update messages pushed to PID apps are potentially more susceptible to cyber attackers. The primary cause is that the communication channel for them is outside the premise and control of typical public transport operators. The PID app server has to deliver the messages to the mobile apps via internet, which makes it a much more accessible target for cyber attackers than control servers well protected in the OCC. As we describe in Section 3.2, there are various vectors that cyber attackers can utilize to compromise the traffic update messages pushed to commuters' PID apps, with no or reduced reliance on physical access to the system.

In addition to examining cyber-physical intrusions, a systematic security analysis also needs to assess the physical consequence of possible cyber incidents in such systems. For example, announcing to all passengers that a certain train service has broken down, or that they can enjoy free rides on a certain route could cause abnormal and even unsafe crowding (e.g., stampeding) at stations or on trains.

3 Applying Existing Security Analysis Approaches

It is important to conduct a thorough and systematic analysis to understand the security postures of urban railway systems. There is a clear gap in this regard. In particular, in current railway safety standards like EN 5012X Series [9] for general railway systems and IEEE 1474 Series [7] for CBTC systems, security is still a lesser concern. Meanwhile, there is also a large body of research work and industrial experience to draw upon. On the one hand, there are well-established approaches for safety-critical system engineering (e.g., HAZOP [10] and FMEA [11]), and noticeable efforts (e.g., [12], [5]) have been devoted to extending some of those methodologies to also consider the security aspect. On the other hand, security assessment methodologies for ICT systems have been studied and applied for a few decades (e.g., [6], [13], [14]), with several recent efforts focusing on cybersecurity issues of critical infrastructures (e.g., [15], [16]).

Table 1. Excerpt of FMVEA results for a CBTC system

Element	Failure / Threat Mode	Direct Effect	System Effect	Cause	S	P	ID
Train Odometry	APR beacon fails to send data	Train receives no data from APR beacon	Missing data can be detected through comparison with tacho, Doppler data and track geometry; the affected train switches to fail-safe state	Failure of hardware / software in APR Beacons	I	-	1
				Attacker jams or disables APR beacons	I	4	2
	Attacker manipulates data from APR beacon	Train receives wrong data from APR beacon	Wrong data can be detected through comparison with tacho data and track geometry; the affected train switches to fail-safe state	Attacker manipulates APR beacons	I	3	3
				Attacker installs additional APR beacons	I	3	4
Signaling Network	Attacker sends wrong LMA to train	Train receives wrong LMA	Train ATO and ATP detect inconsistent LMA; the affected train switches to fail-safe state	Attacker installs additional wireless transmitter to send manipulated LMA to train	I	3	5
	Attacker sends spoofed train data to wayside system	ATS slows down trains to adjust for additional train	OCC raises an alarm to investigate the event	Attacker installs additional wireless transmitter to send spoofed train data to wayside system	I	3	6
	Attacker blocks the authenticated LMA	Train ATO and ATP stop to receive LMA	All trains switch to fail-safe mode	Attacker gains access to signaling network and jams transmission	III	2	7

3.1 Analysis of Scenario 1 with FMVEA Method

With the increasing awareness of the security implications for safety-critical systems, safety assessment methodologies and standards are being extended to explicitly take security into account. A recent example is the *Failure Modes, Vulnerabilities and Effects Analysis (FMVEA)* approach [5], which extends the well-established *Failure Mode and Effects Analysis (FMEA)* methodology [11] to include security related risks. Since safety remains the top concern for CBTC systems, we start our security analysis of Scenario 1 by using this safety engineering methodology extended with security features.

FMEA starts by dividing the studied system into elements. One then analyzes each of the elements one by one to identify potential failure modes. Afterwards, based on the functions of elements and their interactions, one rates the effects of each failure mode on the system's safety. For failure modes with intolerable system effects, one further identifies the causes. If enough information is available, one can further determine the risk based on the severity of the system effect and the probability of the causes. As its security generalization, FMVEA considers both failure modes and threat modes. While a failure mode describes the manner in which a component fails, a threat mode describes the manner in which a component can be misused by a potential attacker. Failure causes are also extended to include vulnerabilities and intentional malicious actions. The risk of a mode is determined not only by the system attributes, but also by the properties of potential attackers.

FMVEA based security analysis. We follow the FMVEA approach to conduct a systematic analysis of various failure and threat modes of a CBTC system. For each element in Fig. 1, potential failure and threat modes, their direct and system effects, and causes are identified. Due to space limitation, we report a selected subset of our FMVEA results in Table 1. Column S depicts the severity, and column P depicts the susceptibility against potential attacks, based on reachability and knowledge about the element.

As shown in the table, a potential threat mode for APR beacon is forged messages. This causes incorrect position data for the train, which would lead to an inconsistency between the position data from the APR beacon and the position data inferred from the tacho and track geometry. When such an inconsistency is detected, the train will send an alarm to the wayside system and switch to a fail-safe state. We also identify potential causes in order to assess the risks. For example, forged data from an APR beacon could be caused by manipulating an existing APR beacon or installing additional APR beaconing devices, both of which require cyber and physical actions.

Our FMVEA result shows that no single failure or threat mode *directly* leads to a safety hazard, due to the built-in safety-assured design features, specifically, redundancy checking and triggering of fail-safe mode under lost communication or inconsistent information. However, we do identify cases (e.g., case 6) where an attacker may be able to gradually influence measured position and speed to manipulate the system into a hazardous situation. Launching such an attack, however, requires access to the trainborne network and the manipulation of multiple measured values.

While our analysis does not identify major safety risks, there are multiple single events that can lead to degradation of functionality and system availability. For example, manipulations of the APR beacons in the tracks (see cases 1–4) can lead to missing or inconsistent data for the determination of the train position and cause a switch to a fail-safe mode. If an attacker is able to compromise the signaling network via direct access or via the installation of additional wireless antennas, she could cause the whole system to switch to a fail-safe mode (see case 7). The built-in safety-assured mechanisms makes such denial-of-service attacks easier to launch. This suggests some potential issue with the EN 50129 approach, which considers the overloading of the transmission system out-of-scope. While the EN 50129 approach is sound from a safety-centric perspective, its potential implications to the system's resilience and availability under malicious threat scenarios require systematic investigation.

Gaps in analyzing multi-stage cross-domain attacks. While the FMVEA approach helps an analyst to systematically consider failure and threat modes, their effects (i.e., physical consequences) and potential causes in an element-by-element manner, it does not provide support for the analysis of multi-stage cross-domain attacks. For example, consider a cyberattack on signaling network (case 7) that might cause critical incidents, the analysis does not include information about how such attacks could be launched. Also, in a multi-stage cross-domain attack an attacker may gain control of multiple elements. It does not readily provide the consequence analysis for such joined threat/failure modes.

3.2 Analysis of Scenario 2 with Attack Tree Method

Since the delivery of accurate, relevant, and timely information is the key for a mobile transit information app as described in our Scenario 2, we approach its analysis through the application of methods that have been more widely adopted in ICT systems security analysis context.

Assessment methodologies used in ICT security domain. ICT security analysis methods are often used to identify potential weaknesses (e.g., software vulnerabilities) in the systems under inspection, and evaluate the likelihood of these weaknesses being misused by an assumed attacker to penetrate the system. Such analysis can also include assessing the consequences of successful attacks in terms of confidentiality, integrity,

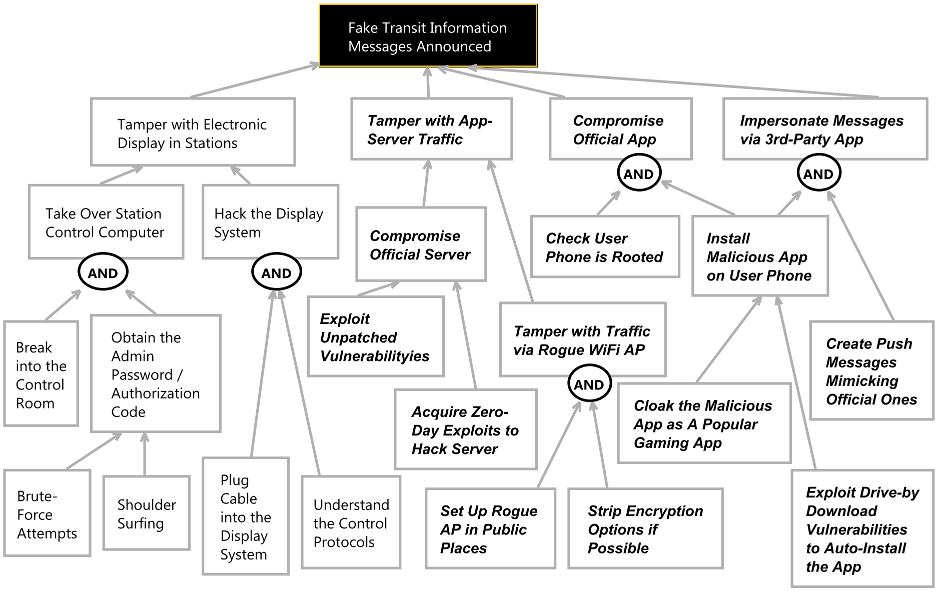
Fake Transit Information Messages Announced
Tamper with Electronic Display in Stations
Tamper with App-Server Traffic
Compromise Official App
Impersonate Messages via 3rd-Party App
Take Over Station Control Computer
Hack the Display System
AND
AND
Compromise Official Server
Check User Phone is Rooted
AND
Install Malicious App on User Phone
AND
Break into the Control Room
Obtain the Admin Password / Authorization Code
Exploit Unpatched Vulnerabilityies
Tamper with Traffic via Rogue WiFi AP
AND
Create Push Messages Mimicking Official Ones
Acquire Zero-Day Exploits to Hack Server
Cloak the Malicious App as A Popular Gaming App
Brute-Force Attempts
Shoulder Surfing
Plug Cable into the Display System
Understand the Control Protocols
Set Up Rogue AP in Public Places
Strip Encryption Options if Possible
Exploit Drive-by Download Vulnerabilities to Auto-Install the App

Fig. 3. An attack tree on announcing fake messages. *Branches are OR gates by default, unless marked as AND gates.* ***Bold italics denote attacks from PID apps.***

and availability. Here we take *attack tree* analysis [6] as an example: this is a widely-used technique to model attacker behaviour and deduce attack paths to a specific malicious goal, which is usually associated with a certain asset. In the railway security domain, the American Public Transportation Association [17] has recently proposed to use attack trees to analyze "narrow and deep" security questions in railway systems.

Attack tree based analysis. Fig. 3 shows an attack tree that illustrates a selected subset of possible attack vectors that can lead to the delivery of fake transit information to passengers. We focus on the information integrity here, since such fake messages can be used by attackers to mislead passengers into overcrowded stations, which could cause safety hazards, e.g., stampedes.

The root node on top of the tree denotes the end goal of the threats, while the subsequent nodes along the branches represent the sub-attacks that attackers can launch to achieve the goal of the sub-attacks in the parent nodes. For instance, one of the ways attackers can push fake transit information to passengers is to compromise the official PID app, which in turn can be achieved by installing a malicious app on users' phones that are rooted. Furthermore, there can be various ways to install such a malicious app, e.g., by uploading it to app stores, or by exploiting a drive-by download vulnerability on victim users' phones.

The attack tree here includes both traditional threats to the electronic display boards in stations via physical attacks, as well as new threats brought in by PID apps (bold italics). As we can see, PID apps can potentially open up a larger attack surface for attackers to send fake transit information messages. With traditional display systems, in order to achieve this, the attackers would have to physically go to the station or control center, and manipulate either display board or server inside the control room. With modern CCTV monitoring systems, the chances of an attacker being caught and stopped is high. However, with PID apps in use, the attackers immediately gain access to such transit messages with much greater "convenience". For instance, they could sit at home and launch remote attacks against the official rail transit operator's PID server, or set up a rogue WiFi access point (AP) in a backpack when taking the train. Making matters worse, attackers have many other means to penetrate commuters' mobile devices directly and at a larger scale, e.g., by uploading a malicious app on Android or iOS app store, which may appear as an interesting game app, but surreptitiously push transit messages mimicking those from official PID apps.

Attack trees provide a convenient and intuitive way for security analysts to construct an overview on how attackers can take steps to achieve their goals. It is also a generic methodology that can model the blend of cyber and physical attacks in a unified way. For example, Fig. 3 models both traditional physical threats as well as emerging cyber threats, and how they may be exploited together by an attacker. With attack trees, one can also associate each individual attack step (regardless of whether it is cyber or physical) with some success probability (or more qualitative judgement about its likelihood). While it is much harder to obtain such quantitative data for security analysis as compared to fault analysis with fault trees, rough estimation based on empirical attacker models can help identifying more plausible attack paths. In particular, the overall attack success probability for the whole tree can be computed according to the logical (combinatorial) relationship among the different attack steps.

Note that the attack tree is only one example of the ICT security analysis methodologies available today. If necessary, more advanced security assessment tools are available, including, e.g., attack graph [13, 14], ADVISE [15], CyberSAGE [18], attack-defense tree [19], etc. These tools support features such as automatic generation of likely attack scenarios based on vulnerability and system information, and more detailed modeling of attacker behavior and attacker/defender interactions.

Gaps in analyzing physical consequences of cyber breaches. While attack tree analysis provides support for modeling multi-stage cross-domain attacks, it provides little aid and guidance in analyzing physical consequences of attacks, especially in terms of quantifying the severity of the consequences along with the likelihood of attack steps. We find that existing ICT security assessment methods generally lack in this aspect. They do not have mechanisms to analyze physical consequences of cyber breaches, nor do they provide support to incorporate such analysis results from other analysis methods. To meet the domain requirement of urban railway systems, it is important to extend ICT security analysis methodologies, such as attack trees, with the necessary mechanisms to have better capabilities of modeling physical consequences of cyber attacks.

4 Moving Forward

As illustrated in Section 3, the cyber-physical nature of modern railway systems presents new challenges for the analysis of their security posture. In particular:

- **Threat Prioritization.** Modern urban railway systems present large attack surfaces. In risk-driven analysis, security analysts need to understand what attacks are more likely to happen, considering factors like attacker motivation, skills, access, and traceability of the attacks.
- **Physical Consequences.** Attacks on railway systems often ultimately aim at the physical world. Security and safety analysts need to understand how cyber breaches can lead to various physical consequences.

Addressing the above challenges demands an integrative cyber-physical perspective. For example, if an attacker wishes to manipulate LMA commands in a covert way, she might consider different combinations of cyber and physical attack steps to find a better attack sequence. In fact, in a recently published railway security analysis exercise [17], the experts analyze different attack sequences for compromising a trackside programmable logic controller (PLC) and argue that a multi-stage cross-domain attack is among the most likely to happen since it reduces the traceability of malicious insiders. Supposing a cyber breach has been made, security analysts need a cyber-physical perspective to understand how relevant factors (e.g., safety-enhancing mechanisms and human behaviors) affect the outcomes of potential attacks, and how the consequences vary with time, location, and other physical context. One also need to consider non-safety-critical risks (e.g., degradation of service) together with safety-critical risks.

Existing approaches for security and safety analysis only partially fulfil such needs. In particular, while the FMVEA analysis in Section 3.1 provides a systematic way to examine individual components and reason about both the consequence (effect) and the likely cause, we see a clear need to further improve its support for analyzing more complicated causes (e.g., those spanning both cyber and physical domains and involving multiple stages) and consequences (e.g., those could be resulted from manipulation of multiple components in a coordinated manner). In comparison, while the attack tree analysis in Section 3.2 allows one to conveniently construct different possible combinations of attack sequences, it provides little aid and guidance in systematically analyzing the consequence of the attacks or exploring all potential attacks. Some safety standards for electronic systems (e.g., the automotive standards ISO26262 [20]) are already defined in a more extensible way that allows the inclusion of physical (such as mechanical) aspects. However, most existing ones (e.g., those from EN 5012X Series) often treat the physical aspect as “out of scope”.

Hence, we need a cyber-physical integrative approach to address the two challenges in threat prioritization and physical consequences of cyber breaches. In particular, analyzing the security of urban railway systems requires the consideration of many different cyber and physical factors. Multiple approaches and techniques are often needed to fulfil the purpose, which calls for a framework to tie different parts in a consistent and meaningful way. Fig. 4 illustrates a new framework that we are working on to integrate various security assessment results. The proposed framework is inspired by existing methods on risk analysis, such as [21]. As shown in the center of Fig. 4, the analysis will be anchored around a possible failure / threat mode induced by cyber breach (e.g., the manipulation of the LMA), or a set of such modes. The left hand side of Fig. 4 shows various attack sequences that lead to the cyber breach, which are enriched with more details about relevant information. Specifically, different attack steps are mapped

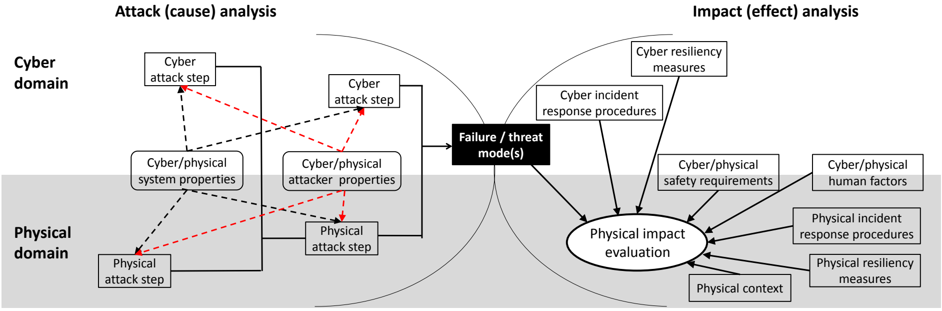
Attack (cause) analysis
Impact (effect) analysis
Cyber domain
Physical domain
Cyber attack step
Cyber attack step
Cyber/physical system properties
Cyber/physical attacker properties
Physical attack step
Physical attack step
Failure / threat mode(s)
Cyber resiliency measures
Cyber incident response procedures
Cyber/physical safety requirements
Cyber/physical human factors
Physical incident response procedures
Physical resiliency measures
Physical context
Physical impact evaluation

Fig. 4. Analyzing railway systems security with an integrative cyber-physical approach.

to either cyber or physical domain. As shown by the dashed edges, each attack step further associates with various system and attacker properties, which can be integrated to estimate the overall attack likelihood. On the right hand side of Fig. 4, the physical consequences of the cyber breach are evaluated based on an impact model (e.g., through high-fidelity simulation) that considers physical context, as well as various cyber / physical procedures, measures, safety requirements, and human factors. A unified view of the cyber and physical domains, as provided in Fig. 4, can contribute to a more thorough security analysis of railway systems. It can also potentially enable the use of quantitative metrics to better understand the scenarios.

We envision such a framework can address the two challenges we highlight earlier by providing the capabilities for "cross-over" analysis for cyber-physical threats and multi-factor analysis for physical consequences.

Analysis of "cross-over" attacks in the cyber and physical domain. Threats from physical attacks will continue to be of primary concern in urban transportation systems, especially in regions where control on weapons and explosives are relatively weak. Nevertheless, threats from the cyber space are increasingly yielding alternative and often complementary means to physical attacks.

Our new framework aims to provide an integrative way to analyze attacks, by explicitly associating attack steps to properties like requirement on attackers' proximity (physical or via a network), the knowledge or tools necessary to cause harm, and the level of attribution that may be possible to discourage an attack. For example, if a would-be attacker needs to be physically on a train at the time of the incident to disrupt a CBTC/signaling system, this scenario may be less risky than another scenario where an attacker remotely hacks into passengers' laptops or mobile phones and causes a train disruption. While our approach focuses on the threat modes, it also can be extended to model the typical operational processes and information flows in the system and analyze their implications on the system's security level (e.g., similar to [16]).

Multi-factor analysis of physical consequences. Unlike cyber attacks on ICT systems that target information, attacks on urban railway systems often target passengers and physical assets, with an aim to cause safety hazards or widespread panics. Hence, our proposed framework incorporates detailed analysis of the physical impact of cyber breaches. High-fidelity modeling and simulation are needed to understand how the consequences change as a function of the time, location, and various cyber-physical resilience measures and response procedures. More empirical data is needed to back up any assumption or model used. The long term effects of such attacks on the railway system as a whole are also largely unexplored. We plan to incorporate realistic traffic models for human passengers in urban transit systems into our framework. This will strengthen security analysts' capabilities of understanding the consequences of such attacks [22]. In addition, we will develop methodologies and tools to incorporate empirical data, as well as advanced modeling and simulation techniques to estimate the potential physical consequences and correlated or cascading effects under different attack scenarios.

5 Conclusion

While the importance of cybersecurity in urban railway systems has become increasingly recognized, the exact roadmap to ensuring it is still largely an open problem. To shed some light into this topic, we examine two concrete examples of cyber-intensive systems in urban railway environments. One is a communications-based train control system, which is a modernized form of a classic safety-critical system. The other is a mobile app that provides transit information to commuters, which is a good example of how new information and communications technologies change the way critical information is propagated between systems and users. We use these two urban railway scenarios to illustrate the strengths of two widely adopted methods (FMVEA and attack trees), and potential gaps present in leveraging them to analyzing cybersecurity of urban railway systems. Our study highlights the need for a cyber-physical perspective in order to understand the cross-domain attack and defense, as well as complicated consequences of cyber breaches in physical domains.

To address the complex security engineering challenges in these safety-critical cyber-physical systems, we believe new security assessment methods and tools are needed. We outline a new framework for analyzing failure and threat modes that can link together attack and impact analysis, and embed the analysis in both cyber and physical domain contexts. We plan to further refine and apply this framework as part of our future work on urban railway security.

Acknowledgments

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate, and supported in part by Singapore's Agency for Science, Technology, and Research (A*STAR) under the Human Sixth Sense Programme (HSSP). The work of Schmittner and Ma was partially funded by the European Commission through the project Creating an Agenda for Research ON Transportation sEcurity (CARONTE).

References

1. Ansaldo STS, "CBTC Communication Based Train Control," http://www.ansaldo-sts.com/sites/ansaldosts.message-asp.com/files/imce/cbtc.pdf.
2. Siemens AG, "Trainguard sirius CBTC," http://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/rail-solutions/rail-automation/train-control-systems/trainguard-sirius-cbtc-en.pdf, 2013.
3. "MyTransport.SG App," http://www.mytransport.sg/mobile/mytransport_mobile.html.
4. "Massachusetts Bay Transportation Authority Apps," http://www.mbta.com/rider_tools/.
5. C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Proc. of the International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 2014.
6. B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobb's Journal*, 1999.
7. IEEE Vehicular Technology Society, "IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements (1474.1-2004)," 2004.
8. Thales, INOV, "Secur-ed cyber-security roadmap for ptos," http://www.secur-ed.eu/wp-content/uploads/2014/11/SECUR-ED_Cyber_security_roadmap_v3.pdf.
9. EN 50129, "Railway applications—Communication, signalling and processing systems—Safety related electronic systems for signalling," 2010.
10. M. Chudleigh and J. Catmur, "Safety assessment of computer systems using hazop and audit techniques," in *Proc. of the Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 1992.
11. IEC 60812, "Analysis techniques for system reliability - procedure for failure mode and effects analysis (FMEA)," 2006.
12. R. Winther, O.-A. Johnsen, and B. A. Gran, "Security assessments of safety critical systems using hazops," in *Proc. of the 20th International Conference on Computer Safety, Reliability and Security (SAFECOMP)*, 2001.
13. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. Wing, "Automated generation and analysis of attack graphs," in *Proc. of the IEEE Symposium on Security and Privacy*, 2002.
14. X. Ou, W. Boyer, and M. McQueen, "A scalable approach to attack graph generation," in *Proc. of the ACM Conference on Computer and Communications Security (CCS)*, 2006.
15. E. LeMay, M. Ford, K. Keefe, W. H. Sanders, and C. Muehrke, "Model-based security metrics using ADversary VIew Security Evaluation (ADVISE)," in *Proc. of the Conference on Quantitative Evaluation of SysTems (QEST)*, 2011.
16. B. Chen, Z. Kalbarczyk, D. M. Nicol, W. H. Sanders, R. Tan, W. G. Temple, N. O. Tippenhauer, A. H. Vu, and D. K. Yau, "Go with the flow: Toward workflow-oriented security assessment," in *Proc. of the New Security Paradigms Workshop (NSPW)*, 2013.
17. APTA Standards Development Program, "Securing Control and Communications Systems in Rail Transit Environments: Part IIIa," 2014. [Online]. Available: www.apta.com/resources/standards/public-comment/Documents/APTASS_CC_WPSecuringCandCSystemsinRailTransitEnvironmentsPartIIIaPC4Q2014.doc
18. A. H. Vu, N. O. Tippenhauer, B. Chen, D. M. Nicol, and Z. Kalbarczyk, "CyberSAGE: A Tool for Automatic Security Assessment of Cyber-Physical Systems," in *Proc. of the Conference on Quantitative Evaluation of SysTems (QEST)*, 2014.
19. B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Foundations of attack-defense trees," in *Proc. of the conference on Formal Aspects of Security and Trust (FAST)*, 2011.
20. ISO 26262, "Road vehicles – Functional safety," 2011.
21. "Bowtie Method," www.caa.co.uk/bowtie.
22. E. F. Legara, C. Monterola, K. K. Lee, and G. G. Hung, "Critical capacity, travel time delays and travel time distribution of rapid mass transit systems," *Physica A: Statistical Mechanics and its Applications*, vol. 406, no. 0, pp. 100 – 106, 2014.