

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation

Himanshu Neema
Xenofon Koutsoukos
himanshu.neema@vanderbilt.edu
xenofon.koutsoukos@vanderbilt.edu
Institute for Software Integrated
Systems
Vanderbilt University
Nashville, TN 37235

Bradley Potteiger
brad.potteiger@jhuapl.edu
Johns Hopkins Applied Physics
Laboratory
Laurel, MD 20723

CheeYee Tang
Keith Stouffer
cheeyee.tang@nist.gov
keith.stouffer@nist.gov
National Institute of Standards and
Technology
Gaithersburg, MD 20899

ABSTRACT

The last decade has seen an influx of digital connectivity, operation automation, and remote sensing and control mechanisms in the railway domain. The management of the railway operations through the use of distributed sensors and controllers and with programmable and remotely controllable railway signals and switches has led to gains in system efficiency as well as operational flexibility. However, the network connectivity has opened up the railway cyber communication networks to cyber-attacks. These are a class of cyber-physical systems (CPS) with interconnected physical, computational, and communication components. The cyber-attacks on these systems could potentially cascade through these interconnection and result into significant damage. These systems are safety-critical owing to their large-scale monetary and, more importantly, human life safety concerns. Therefore, it is better to incorporate security and resilience requirements right from the design time. In this paper, we describe a domain-specific framework for simulations in the railway domain. The framework allows analyzing the resilience of railway operations in the presence of cyber-attacks. In particular, our simulation framework allows modeling the railway network as well as the railway transportation. It provides an online graphical modeling environment that allows multiple users to collaborate, through a web-based interface, over the same model for the railway infrastructure as well as network attacks. The framework also allows the user to configure and run experiments through the web-interface and also to visualize the key operational metrics from the railway domain as the experiment is running. The framework also supports executing large simulations in the cloud. In addition, it supports hardware-in-the-loop (HIL) simulation for incorporating physical effects and network attacks that can only be realized realistically in the hardware. A detailed case study is provided to demonstrate the framework's capabilities.

CCS CONCEPTS

• **Computer systems organization** → **Embedded and cyber-physical systems**; *Redundancy*; • **Computing methodologies**

ACM acknowledges that this contribution was authored or co-authored by an employee, contractor, or affiliate of the United States government. As such, the United States government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for government purposes only.

HotSoS '20, April 7–8, 2020, Lawrence, KS, USA

© 2020 Association for Computing Machinery.

ACM ISBN 978-1-4503-7561-0/20/04...\$15.00

<https://doi.org/10.1145/3384217.3385623>

→ **Modeling and simulation**; • **General and reference** → *Cross-computing tools and techniques*; • **Networks** → Network reliability.

KEYWORDS

Railway infrastructure, Modeling and Simulation, Hardware-in-the-loop, Cybersecurity, Resilience

ACM Reference Format:

Himanshu Neema, Xenofon Koutsoukos, Bradley Potteiger, CheeYee Tang, and Keith Stouffer. 2020. Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation. In *Hot Topics in the Science of Security Symposium (HotSoS '20)*, April 7–8, 2020, Lawrence, KS, USA. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3384217.3385623>

1 INTRODUCTION

Railway infrastructure is going through a transformation through incorporation of network enabled sensors and actuators that make it possible to control its operations and remotely and in an automated manner. The growth in network connectivity and with programmable and remotely controllable railway signals and switches has made railway operations and management more efficient as well as operationally flexible. At the same time, the open connectivity has made them vulnerable to cyber-attacks. These systems are a class of CPS [14] with interconnected physical, computational, and communication components. These are also safety-critical systems because a large number of transportation and even human life depends on their continual safe operations. As such the railway infrastructure is one of the nationwide critical infrastructure. However, the tight coupling among the communication, computational, and physical components enable cascading failures once one of the component gets compromised and attacked. Thus, even though the integration of vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) enables fine-grained control over the transportation operations, it makes them susceptible for cyber-attacks that can cause significant damage to the systems and can even cause loss of human life. Therefore, analyzing the security and resilience of railway systems is critical for studying the effect of cyber-attacks.

Railway is unique due to the tight integration between legacy standalone devices and modern communication interfaces. As such, many systems which were designed several decades ago, do not take into account the vulnerability space presented by remote communication. This fact combined with the rush to market by Internet-of-Things (IoT) manufacturers makes railway susceptible to an increased and diversified attack surface, especially the communication-related vulnerabilities such as memory corruption.

As such, the threshold to a successful compromise is significantly lower compared to traditional information technology applications such as servers, websites, and databases. Since in modern railway there is a tight integration between software processes and physical dynamics, vulnerable applications can be exploited for causing physical damage, that could potentially include terrorist attacks by sophisticated adversaries.

One key differentiator between CPS and traditional software applications is the unpredictability in analyzing the impact of cyber-attacks on a live system, particularly the physical actuation of safety-critical components. Additionally, the increased interconnectedness between components increases the potential and impact of attack propagation. As such, it is no longer sufficient to rely on locking down the most critical components, but zero trust architectures must be utilized to take a weakest-link approach to prevent adversaries from gaining entry into critical networks. Finally, the necessity of requiring the stability of physical actuation, makes it important to not only analyze the cyber-attack behavior on the underlying software components, but also the physical operations of systems. As such, in railway applications, a high priority focus should be on system safety, high availability, system and data integrity and predictable operation.

The main problem that this paper addresses is how to leverage simulation and emulation capabilities to create secure and resilient CPS. In addition, we focus on how to provide a systematic methodology for creating cyber-attack experiments to assess their impact, with or without defense mechanisms, on the software and physical dynamics of the system. We also demonstrate integrated evaluation of key metrics and their visualization to provide real-time feedback to security researchers.

In this paper, we describe a domain-specific framework for simulations in the railway domain. The framework allows analyzing the resilience of railway operations in the presence of cyber-attacks. In particular, our simulation framework allows modeling and integrated simulation of the railway cyber communication network and the railway transportation. The framework is developed as an online graphical modeling tool that allows multiple users to collaborate, through a web-based interface, over the same model for the railway infrastructure as well as network attacks. In the framework, we have developed methods to define and calculate key operational metrics to study the impact of cyber-attacks on railway operations. Using this approach, one can design and evaluate different mechanisms for network defense and determine system's key network vulnerabilities. In the following sections we attempt to focus on the following objectives:

- Develop a software platform for rapidly designing and evaluating cyber-attacks for connected railway architectures.
- Design a component-based modeling approach that leverages our modular libraries for deploying cyber-attacks and collecting metrics from domain-specific experiment results in real-time.
- Integrate HIL testbed in order to evaluate the impact of cyber-attacks and physical effects in a hardware environment similar to that in the real-world.

- Create a case study using the Washington, DC Metro railway network model for demonstrating the capabilities of our experiment design platform.

The remainder of the paper is organized as follows. Section 2 provides the rationale for evaluating cybersecurity in the railway domain. Section 3 describes the architecture of our cybersecurity evaluation platform. Section 4 demonstrates the capabilities of our platform utilizing the case study of the Washington, DC Metro system. Section 5 discusses the work related to this research and Section 6 concludes.

2 RATIONALE

With the push to smart city implementations, railway transportation has experienced a significant disruption. New fuel sources, communication protocols, and control systems have rapidly increased the efficiency and safety of these systems, while reducing the operational cost. Trains now comprise several embedded electronic equipment dedicated for both internal operations and remote access purposes such as communicating with local infrastructure and central monitoring stations. With increased communication capabilities, manual mechanisms are no longer necessary for track configuration. Similar to the automobile industry, track control systems such as rail signals and switches are built with autonomous logic to systematically route trains. This advanced control requires vehicle to infrastructure (V2I) communication protocols which are largely being expanded due to the implementation of 5G.

Embedded microcontrollers and V2I communication have definitely disrupted the railway industry in a positive manner. However, this change has also negatively impacted cybersecurity of the system. Railway systems, like in the automotive industry, rely on a significant amount of legacy code, most of which has not been adapted in decades due to the safety and regulation costs. Consequently, the railway systems have a larger number of vulnerabilities compared to the traditional information technology infrastructure, which allows for nation states, terrorist organizations, and hackers to compromise these highly critical transportation networks. The presence of legacy code and remote communication capabilities effectively means that physical access is no longer necessary to disrupt train operations. Instead, an adversary can easily compromise train systems even when being several miles away. Furthermore, because safety-critical train networks are not isolated, once an attacker obtains access, they can pivot to safety-critical devices, causing them to behave dangerously that could lead to devastating crashes. Some of the high profile examples of attacks on railway systems include ransomware attacks against San Francisco and Sacramento, and system-wide disruption in train scheduling operations in London [12]. Fortunately, there haven't been any high profile examples of cyber-attacks leading to dangerous crashes. However, translating these results to the Amtrak crash in Philadelphia [25] paints a eye-opening picture of potential consequences of disruption of safety-critical control.

To successfully protect railway networks and systems, it is critical to utilize an objective and scientific methodology to evaluate the most effective cybersecurity defense mechanisms, as well as prioritizing relevant attack surfaces to address. As such, simulation has proved to be an effective technique in the CPS domain

to quantitatively evaluate the software effects on the physical dynamics. This ensures that safety and security can be designed into system architectures in a cost-effective manner. Furthermore, for a smooth transition to deployment settings, software emulation in a hardware-in-the-loop environment can increase trust in reliable system performance.

2.1 HIL Testbed

In order to measure the impact of security mechanisms on the performance of the Industrial Control Systems (ICS), the US National Institute of Standards and Technology (NIST) has developed an HIL testbed. NIST has also published a guide for implementation of security in ICS [22]. The testbed utilizes Commercial-Off-The-Shelf (COTS) control hardware as well as several simulation tools for emulating realistic scenarios. For this particular application, the HIL testbed is used for measuring the performance impact of cybersecurity mechanisms on railway operations. The testbed uses realistic ICS hardware as well as an integrated framework called the Cyber Physical Systems Wind Tunnel (CPSWT) [8] [9] [11] [18] that enables integrating large-scale heterogeneous simulations. The HIL setup in the NIST testbed emulates a railroad crossing scenario. It has a COTS Programmable Logic Controller (PLC), a commercial industrial network switch, and two embedded sensors. The simulation is hosted in a virtual machine that has an Ethernet connection to the PLC. The PLC has a Controller Area Network (CAN) interface to communicate with the embedded sensors. The CAN protocol is used widely for ICS in the railroad and automotive industries. Transmission Control Protocol (TCP) and Internet Protocol (IP) are the standard protocols used in the worldwide internet. The HIL testbed simulator communicates with the PLC through a TCP/IP socket for sending commands to the PLC and receiving sensor information. The PLC uses the sensor information to determine the train location and speed at a crossing, then uses its output to control the barrier and warning signal at the crossing. The barrier control and warning signal in the testbed are represented by simple analog outputs from the PLC. When an experiment is performed in the simulator, the hardware is functioning in real-time instead of simulation time, allowing for a more accurate representation of the railway behavior in deployment environments. This setup allows the researcher to evaluate any impact induced by the experiment to the crossing.

In the past, we have focused our work on utilizing the CPSWT simulation integration framework to evaluate the cybersecurity of railway scenarios [9]. CPSWT takes advantage of the IEEE High Level Architecture (HLA) standard [1] to integrate various domain-specific simulators synchronously and analyze integrated simulations with different system configurations and parameters in the context of many different CPS experiments. This work takes a step further by developing a cloud-based experiment manager to rapidly develop and evaluate railway specific attack scenarios. Furthermore, we have made our testbed setup more user friendly by utilizing an open source simulator [21], allowing easier creation of transportation scenarios from scratch. The next sections present the architecture of our testbed and demonstrate its capabilities with the use of a railway case study.

3 SYSTEM ARCHITECTURE

Railway transportation system is one of the nation's critical infrastructure as a large number of people travel by trains as well as a large amount of packages and goods are transported by the system. A failure or attack in one of the components of the system can lead to cascading failures in other parts of the system, which can quickly result in substantial financial and human loss. This is the reason why these are safety-critical systems. Therefore, evaluating these systems for safety, reliability, and security in the presence of cyber attacks is necessary.

However, these systems are highly complex with many different types of components that work together. For example, the trains, its engine, train tracks, track signals and switches are physical components that are key part of these systems. There are also computational components such as sensors and controllers that make the train operations possible. In addition, there are many communication networks and devices that form the cyber communication network topology of railway systems. Moreover, humans are integral part of all of its operations and workflows. Therefore, a holistic evaluation of these systems requires one to integrate simulators of each of these parts of the system so that overall system-of-systems (SoS) level studies can be conducted. Fig. 1 shows the setup of our testbed. As shown, the front-end provides a modeling environment where users can design simulation studies and execute them using web-based plugins that execute the simulations in the backend. Additionally, the hardware devices connected to the testbed can be used for attacks and effects more practically and realistically realizable in the real hardware.

There are three main components in our simulation framework: *Experiment Controller*, *Simulation Backend*, and *Simulation Analyzer*. The key aspects for analyzing railway systems in our simulation platform include: the development of simulation experiments, scientific design for resilience, ensuring security and resilience amidst sophisticated real-world attacks, and the use of operational quantitative metrics for analysis. Thus, various approaches for securing the railway infrastructure can be objectively compared. Fig. 2 shows the three components of our framework and the sub-sections below describe them in detail.

3.1 Experiment Controller

The *Experiment Controller* (EC) serves as the main orchestrator of experiments. It allows for designing experiment scenarios including modeling and deployment of cyber-attacks. For modeling purposes, the EC uses a web-based graphical modeling environment (or WebGME) [26]. WebGME provides a metamodeling framework that allows users to customize the experiment modeling language. In addition, WebGME provides a multi-user modeling environment with change tracking and allows multiple designers to work on the same model using a web-browser from different locations. Moreover, WebGME allows incorporating domain-specific plugins that enable model interpretation, generation of executable artifacts such as code, scripts, and configurations, and also execution of simulations on the compute platforms (include cloud backends). Furthermore, for analyzing the scenarios, the EC monitors the executed simulations, collects the experiment results, and brings it on the front-end for analysis and display tools.

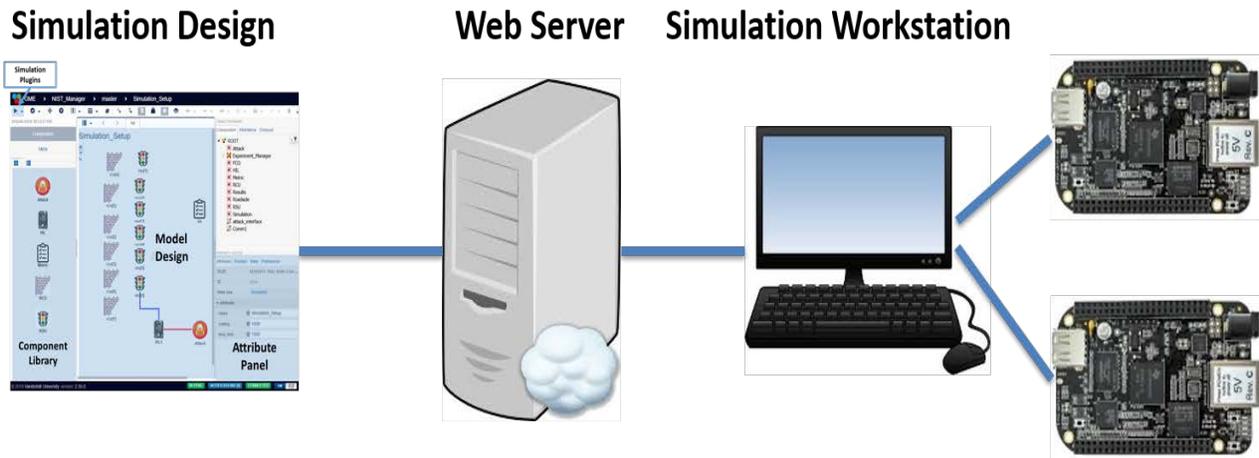


Figure 1: Railway Cybersecurity Evaluation Testbed Setup

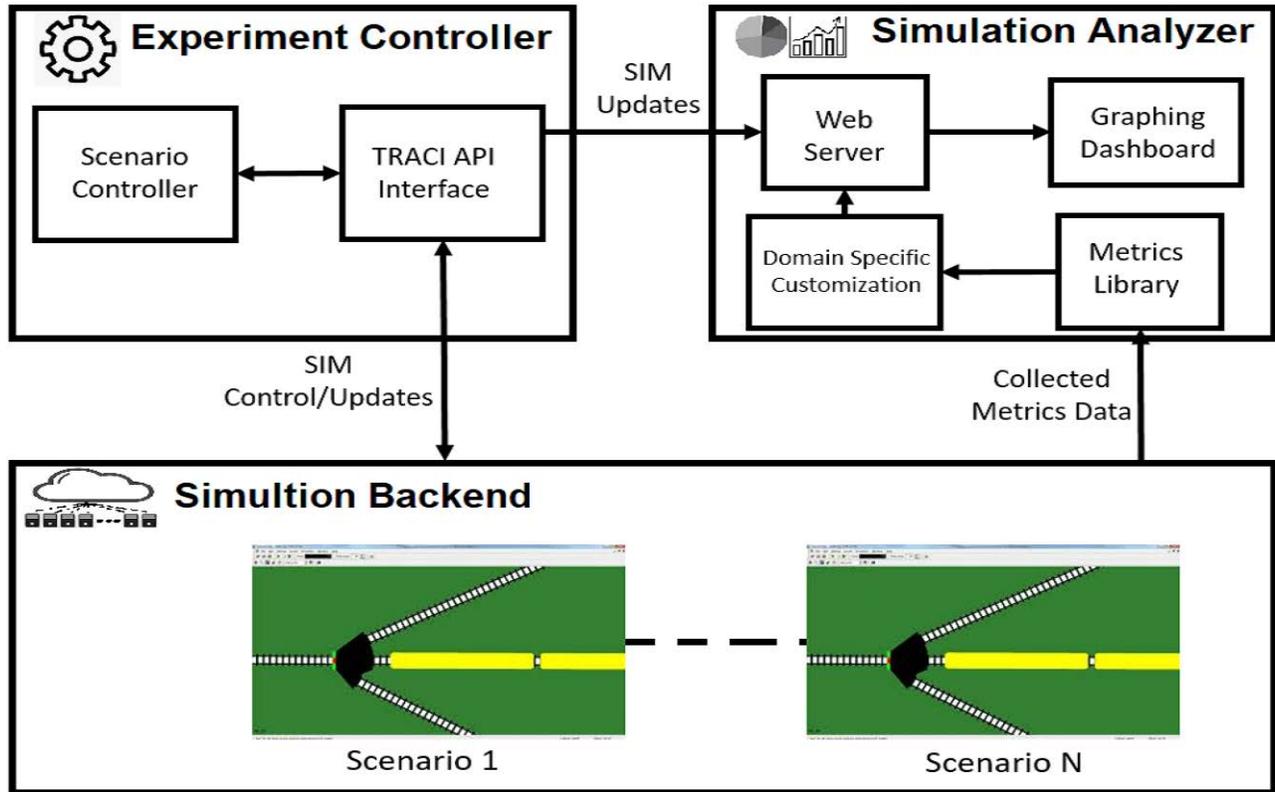


Figure 2: Testbed Architecture

3.2 Simulation Backend

The *Simulation Backend* (SB) is responsible for providing the compute platform and the associated tools and methods for running large-scale experiments. In the SB, we use an open-source simulator, called Veins [21], for modeling and simulating the railway networks and railway transportation as well as the railway infrastructure’s cyber communication network. Internally, the Veins simulator is

composed of two separate simulators, viz. SUMO [16] for road transportation simulation and OMNeT++ [23] for cyber communication network simulation. With support for simulation experiments to run in the cloud, multiple experiments could be executed at the same time.

3.2.1 Attack Library. An important feature of our framework is that it comes with a reusable set of cyber-attacks that can be configured and utilized in different experiment scenarios. These cyber-attacks are packaged in the form of an attack library. For implementation of the cyber-attacks in the library, we extended the Veins V2X communication module for attack specific source-code and for parameterization of the attacks according to requirements of different experiment scenarios. Currently, we support incorporating denial of service (DOS), integrity, corruption, and delay attacks on railway nodes in simulation, while distributed-DOS (DDOS) attacks can be implemented on the integrated hardware nodes.

3.2.2 HIL Testbed. In order to test for attacks that be deployed only in the hardware, such as DDOS, large amount of network traffic, or attacks exploiting vulnerabilities in the hardware, we integrated our HIL testbed with the simulation framework to provide a rich experimentation environment. The attack library described above already contains such attacks. This environment enables analysts to develop scenarios where the components can either be simulated in the software or emulated in the physical hardware. For example, in the context of railway simulations, one can design the railway network and transportation in the simulator and emulate railroad signals and actuators in a realistic integrated hardware. Our testbed is comprised of a cluster of multiple Beaglebone Black embedded microcontroller boards running the Ubuntu 16.04 operating systems. Additionally, we support realistic communication protocols by providing capabilities for 100 Mb/s Ethernet and 1 Mb/s CAN bus with the open source ZeroMQ and SocketCAN libraries.

3.3 Simulation Analyzer

The *Simulation Analyzer* (SA) component in our framework enables analysis of experiment results through integrated data capturing and visualization tools. When the users execute the experiment on the Simulation Backend, the experiment artifacts are generated both while the simulation is running and once it has completed. These artifacts are stored in a high-availability database using InfluxDB [3]. The SA has the ability to bring both types of artifacts to the web-based experimentation front-end. In addition, we developed several analysis tools and a presentation dashboard using Grafana [2]. The unique feature of SA is that the analyzed experiment results can be plotted and visualized to the users in real-time. This is accomplished by processing the artifacts as they get generated by the experiments and stored in the database and periodically running the analysis tools on them. Additionally, after experiment conclusion, final results are also plotted in a WebGME visualizer integrated with the user development environment. Moreover, the visualization tools also support comparing different domain-specific experimentation scenarios. For example, one can use these features to perform cyber-gaming experiments in the context of a particular railway scenario by playing various combinations of cyber-attacks against various security mechanisms.

3.3.1 Metrics Library. Domain-specific operational metrics [10] are require computation logic that is specific to the domain as well as the metric. However, many domain-specific aspects can be modularized in a form that becomes reusable for calculating different operational metrics. Our metrics library provides a set of

customizable and extensible methods to enable incorporation of newer operational metrics. We implemented this library by integrating a graphical modeling interface with a custom data acquisition module that collects various generic component parameter values from the simulation, and calculates system-level metrics utilizing predefined formulas. As of this writing, we support railway domain specific metrics including the average speed at which trains move in the railway network, the average amount of fuel consumed by the trains, amount of time trains spend waiting for signals to go green, and total distance traveled by the trains. These metrics are important to the railroad operators and serve as high-level system metrics for the experiment. Key operational metrics are used to help determine the health and efficiency of the railroad operation. By evaluating these metrics, researchers can assess the impact to the railroad system caused by each experiment or the cyber-attack simulation.

3.3.2 Domain Specific Customization. In addition to collecting individual simulation experiment metrics defined in the metrics library, it is often necessary to utilize a more sophisticated interpretation for gaining relevant insights. For example, a different unit of measurement may be necessary, or a more descriptive statistic may be developed through a combination of the smaller individual simulation metrics. Our domain specific customization module supports these efforts by providing the ability to define equations that relate the respective data collected by the metrics library.

4 CASE STUDY

For demonstration purposes, we utilize a scenario based on the Washington, D.C. Metro Railway System (see Fig. 3). This scenario builds a railway network mirroring to a part of the Washington, D.C. Metrol railway system coupled with signals (for stopping trains on the tracks or letting them proceed) and control switches (actuators for dynamically changing the tracks on which the trains will proceed). These railway switches are mirroring the functions of real-world railway junctions, where trains can be directed in different directions depending on their programmed destinations. The control of the actuator switches is determined by a control program that is executed based on the wireless signals that the approaching trains send to the control unit.

4.1 Attack Scenario

In this particular experiment, we focused on demonstrating the framework features of both the simulation testbed as well as the HIL testbed. For demonstrating cyber-attacks on the simulation, we utilize an integrity attack from the attack library. In particular, the integrity attack causes the railway switch to get incorrect messages from the approaching trains, thereby causing the trains to go on undesired tracks. Also, for demonstrating the cyber-attacks that are realizable realistically only in the physical hardware, we use the attack library's HIL-specific attacks. In particular, the DDOS attack is used to cause flood the network traffic destined to a specific railway signal controller. Consequently, the attacked railway signal controller is overwhelmed with the messages that it needs to process resulting in invalid or unchanged signal states. The result of this is that the approaching trains get delayed until the railway

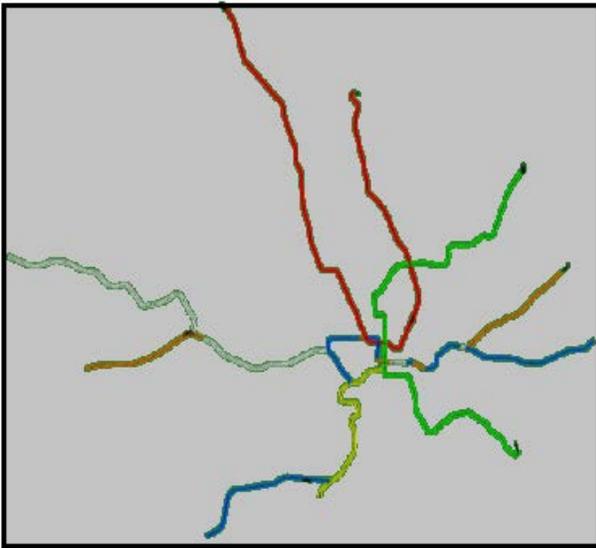


Figure 3: Washington, D.C. Metro Railway Network

signal updates to a green light. The experiment results from this scenario are described in the next subsection.

4.2 Results

To illustrate the results of our experimental scenario, we focus on analyzing the path of an individual train traveling through the Washington, DC metro network from Reston, VA to Greenbelt, MD. Utilizing the metrics library within our experiment design interface, we collect the following information: the average speed at which trains move in the railway network, the average amount of fuel consumed by the trains, amount of time trains spend waiting for signals to go green, and total distance traveled by the trains. Interestingly, the optimal path of the respective train is traveling east on the silver line, transferring to the blue line and traveling north of the inner city, and transferring to the green line to travel north east to Greenbelt. The attack process disrupts the train route through the following: the rail switch integrity attack results in the train being routed to the blue line south direction versus the optimal north route. As such, the train will have to travel around the southern perimeter of the city. Furthermore, while transferring to the green line, the DDOS attack on the corresponding rail signal causes a significant delay before the transfer is completed. Figures 4, 5, 6, and 7 illustrate the respective speed, fuel consumption, waiting time, and distance traveled for the train that experiences the worst impact due to attacks. In the figures, the red colored lines illustrate the train's metrics with the attack scenario enabled, while the blue colored line illustrates the train baseline scenario when traveling on the optimal path. The rail signal delay can be observed from approximately 9300 to 11000 seconds with the simulation. The figures show that there is a significant drop in speed at this time, the fuel consumption rate decreases as the train remains idle, and the accumulated waiting time increases sharply. Furthermore, the distance traveled metrics clearly show that the attack was successful as the train gets late in reaching its destination at Greenbelt by 1500 seconds.

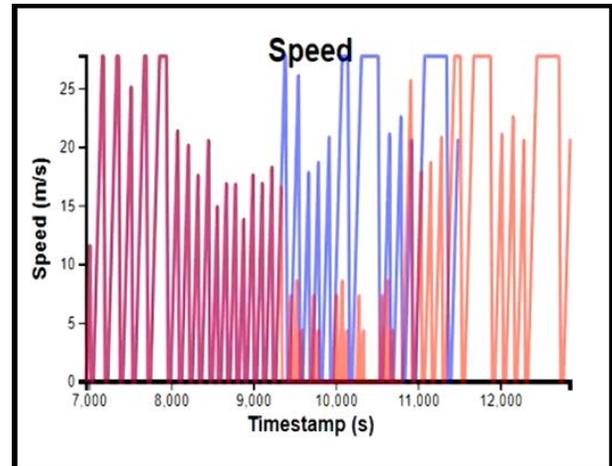


Figure 4: Speed

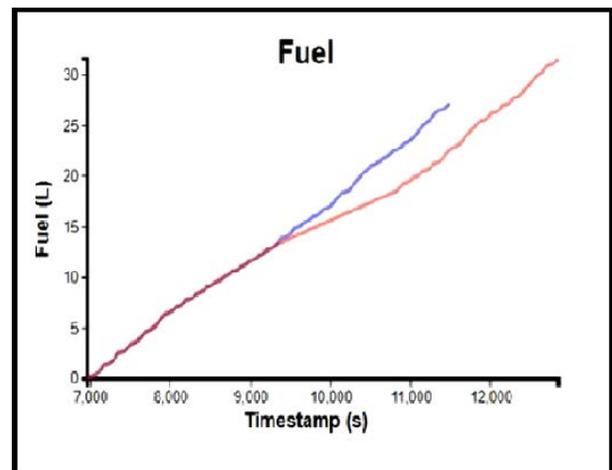


Figure 5: Fuel

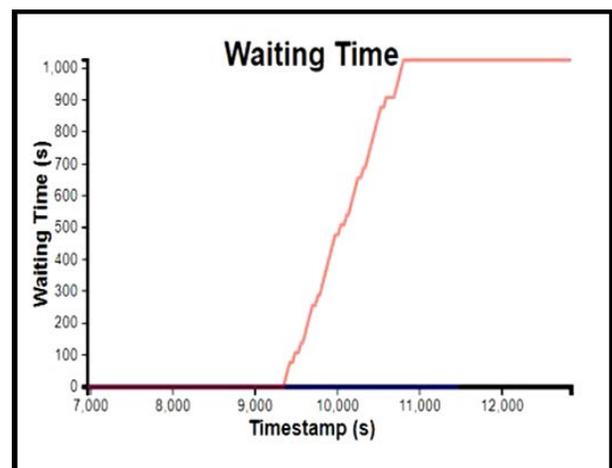


Figure 6: Waiting Time

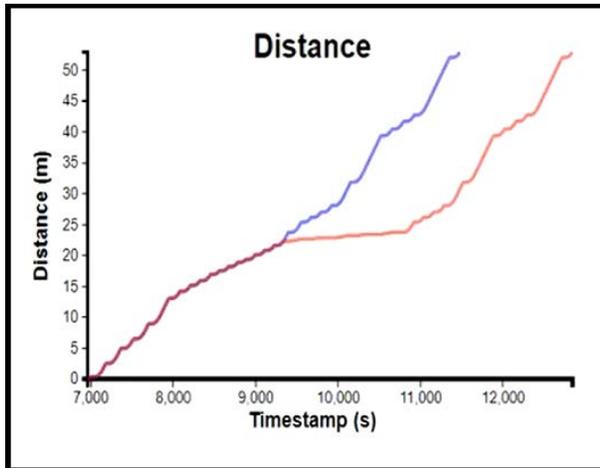


Figure 7: Distance

5 RELATED WORK

With the significant increase in the utilization of digital technologies in the railway domain, including the European Railway Traffic Management System (ERTMS), is becoming more susceptible than ever to cyber-attacks [17]. The physical consequences of railway failures have been very publicly demonstrated in explosion-based attacks [24], as well as infrastructure failures [27]. Additionally, there has been much concern about the possibility of utilizing railway software for terrorist activities, serving as a prime vector to inflicting maximum damage to patrons who are not prepared for cyber-attacks [19]. As such, it is crucial to incorporate security and resilience requirements right from the design time, thereby maximizing trust in the safety of operations on their deployment into the field [14].

There has been increasing research in the railway industry focusing on the CPS perspective [20] including communication security, actuation safety [7], and train operator authentication [6]. Additionally, there has been a large amount of interest in the academic community in creating simulation testbeds for analyzing safety-critical CPS for security, safety, and resilience in the presence of cyber-attacks. The goal is to maintain predictable and safe operation during all scenarios, including when the system is under attack [5]. These frameworks have ranged from risk assessment tools [4], integrated simulation environments [8] [11], as well as transportation-specific attacker-defender modeling interfaces [15]. Additionally, the WebGME meta-modeling toolsuite has been a popular graphical user environment for easily and rapidly controlling CPS simulations [13].

6 CONCLUSION

In present day society, transportation is becoming more interconnected with the use of embedded devices for computation and control and wireless networking for communication. Railway is no exception, essentially becoming a computer on tracks. Even though there are significant benefits, including cost savings and an increase in travel efficiency, the introduction of electronic components and remote interfaces creates a significant avenue for attacker exploitation. With the safety-critical actuation of trains, locking down data

from exfiltration is no longer enough as the railway operations also need to be maintained safely on a continual basis. A failure in this effort can lead to devastating consequences including high-speed train crashes, hazardous leaks of laboratory compounds or gasoline, and even loss of human life.

In this research work, we have illustrated a railway infrastructure experimentation platform, that can leverage cloud backend for large-scale computations, and that allows users to rapidly develop cyber-attack scenarios against train software to evaluate the resulting physical behavior. The goal of this approach is to allow railway designers to test the safety of algorithms and infrastructure well before deployment, providing trust in defense protections once in the field.

We developed three key components in our simulation framework, viz. the Experiment Controller, the Simulation Backend, and the Simulation Analyzer. The Simulation Backend provides the ability to evaluate railway infrastructure components in a simulation environment using the Veins simulator. Additionally, an integrated HIL testbed allows the users to emulate software on embedded microcontrollers similar to deployment environments. This allows for creating a realistic environment for getting a sense of the full spectrum of possible cyber-attack reactions, allowing for designers to have a more accurate sense of prioritizing the most critical vulnerabilities and attack vectors to protect against. Our Experiment Controller provides a graphical modeling environment for designing experiment scenarios including modeling and deployment of cyber-attacks. Further, we evaluated our platform with a case study of the Washington, DC metro network, where we captured domain-specific operational metrics as they were being generated, thereby validating our experimental design approach. We demonstrate the Simulation Analyzer that enables analysis of experiment results through integrated data capturing and visualization tools.

Further ahead, we plan to continue to extend our testbed for applying it to other transportation applications, including self-driving vehicles, and for enriching the re-configurable model libraries with more cyber-attacks and security solutions.

7 ACKNOWLEDGEMENTS

This work at Vanderbilt is supported by the National Security Agency (NSA) through award number H98230-18-D-0010, the National Institute of Standards and Technology (NIST) through award number 70NANB17H266, and the National Science Foundation (NSF) through award number CNS-1739328. No approval or endorsement of any commercial product by NSA, NIST, or NSF is intended or implied. Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NSA, NIST, or NSF, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose. This publication was co-authored by United States Government employees as part of their official duties and is, therefore, a work of the U.S. Government and not subject to copyright. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSA, NIST, or NSF.

REFERENCES

- [1] 2010. IEEE Std 1516–2010, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)- Framework and Rules. , 3 pages.
- [2] 2020. Grafana - The open observability platform for metrics and analytics. <https://grafana.com/>
- [3] Andreas Bader, Oliver Kopp, and Michael Falkenthal. 2017. Survey and comparison of open source time series databases. *Datenbanksysteme für Business, Technologie und Web (BTW 2017)-Workshopband (2017)*.
- [4] Bradley Potteiger, Goncalo Martins, and Koutsoukos, Xenofon. 2016. Software and attack centric integrated threat modeling for quantitative risk assessment. In *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM, 99–108.
- [5] Bradley Potteiger, Zhenkai Zhang, and Xenofon Koutsoukos. 2018. Integrated instruction set randomization and control reconfiguration for securing cyber-physical systems. In *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*. ACM, 5.
- [6] Andrey V Chemov, Maria A Butakova, Ekaterina V Karpenko, and Oleg O Kartashov. 2016. Improving security incidents detection for networked multilevel intelligent control systems in railway transport. *Telfor Journal* 8, 1 (2016), 14–19.
- [7] Jahanzeb Farooq and José Soler. 2017. Radio communication for communications-based train control (CBTC): A tutorial and survey. *IEEE Communications Surveys & Tutorials* 19, 3 (2017), 1377–1402.
- [8] Himanshu Neema. 2018. Large-Scale Integration of Heterogeneous Simulations. *Ph.D. Dissertation, Vanderbilt University* (Jan. 2018).
- [9] Himanshu Neema, Bradley Potteiger, Xenofon Koutsoukos, CheeYee Tang, and Keith Stouffer. 2018. Metrics-Driven Evaluation of Cybersecurity for Critical Railway Infrastructure. In *2018 Resilience Week (RWS)*. IEEE, 155–161.
- [10] Himanshu Neema, Bradley Potteiger, Xenofon Koutsoukos, CheeYee Tang, and Keith Stouffer. 2018. Metrics-Driven Evaluation of Cybersecurity for Critical Railway Infrastructure. In *2018 Resilience Week (RWS)*. IEEE, 155–161.
- [11] Himanshu Neema, Bradley Potteiger, Xenofon Koutsoukos, Gabor Karsai, Peter Volgyesi, and Janos Sztipanovits. 2018. Integrated Simulation Testbed for Security and Resilience of CPS. *The 33rd ACM/SIGAPP Symposium On Applied Computing* (Apr. 2018).
- [12] Sidra Ijaz, Munam Ali Shah, Abid Khan, and Mansoor Ahmed. 2016. Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications* 7, 2 (2016), 612–625.
- [13] Gabor Karsai, Holger Krahn, Claas Pinkernell, Bernhard Rumpe, Martin Schindler, and Steven Völkel. 2014. Design guidelines for domain specific languages. *arXiv preprint arXiv:1409.2378* (2014).
- [14] Sangjun Kim, Yuchang Won, In-Hee Park, Yongsoo Eun, and Kyung-Joon Park. 2019. Cyber-physical vulnerability analysis of communication-based train control. *IEEE Internet of Things Journal* 6, 4 (2019), 6353–6362.
- [15] Xenofon Koutsoukos, Gabor Karsai, Aron Laszka, Himanshu Neema, Bradley Potteiger, Peter Volgyesi, Yevgeniy Vorobeychik, and Janos Sztipanovits. 2017. SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber-physical systems. *Proc. IEEE* 106, 1 (2017), 93–112.
- [16] Daniel Krajzewicz, Jakob Erdmann, Michael Behrisch, and Laura Bieker. 2012. Recent Development and Applications of SUMO - Simulation of Urban MObility. *International Journal On Advances in Systems and Measurements* 5, 3&4 (December 2012), 128–138. <http://elib.dlr.de/80483/>
- [17] Igor Lopez and Marina Aguado. 2015. Cyber security analysis of the European train control system. *IEEE Communications Magazine* 53, 10 (2015), 110–116.
- [18] Neema, H., H. Nine, G. Hemingway, J. Sztipanovits, and G. Karsai. 2009. Rapid Synthesis of Multi-Model Simulations for Computational Experiments in C2. *Armed Forces Communications and Electronics Association - GMU Symposium, Critical Issues in C4I* (May 2009).
- [19] M-Elisabeth Paté-Cornell, Marshall Kuypers, Matthew Smith, and Philip Keller. 2018. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis* 38, 2 (2018), 226–241.
- [20] Mouna Rekik, Christophe Gransart, and Marion Berbineau. 2018. Cyber-physical security risk assessment for train control and monitoring systems. In *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.
- [21] Christoph Sommer, David Eckhoff, Alexander Brummer, Dominik S Buse, Florian Hagenauer, Stefan Joerer, and Michele Segata. 2019. Veins: The open source vehicular network simulation framework. In *Recent Advances in Network Simulation*. Springer, 215–252.
- [22] Keith Stouffer, S Lightman, V Pillitteri, Marshall Abrams, and Adam Hahn. 2015. Guide to Industrial Control Systems (ICS) Security–NIST Special Publication (SP) 800-82 revision 2. *NIST, Tech. Rep* (2015).
- [23] Andras Varga. 2019. A practical introduction to the OMNeT++ simulation framework. In *Recent Advances in Network Simulation*. Springer, 3–51.
- [24] Wikipedia. 2020. 2004 Madrid train bombings — Wikipedia, The Free Encyclopedia. <http://en.wikipedia.org/w/index.php?title=2004%20Madrid%20train%20bombings&oldid=934598985>. [Online; accessed 21-January-2020].
- [25] Wikipedia. 2020. 2015 Philadelphia train derailment — Wikipedia, The Free Encyclopedia. <http://en.wikipedia.org/w/index.php?title=2015%20Philadelphia%20train%20derailment&oldid=936015816>. [Online; accessed 20-January-2020].
- [26] Peng Zhang, Zsolt Lattmann, James Klingler, Sandeep Neema, and Ted Bapty. 2015. Visualization techniques in collaborative domain-specific modeling environment. In *SoutheastCon 2015*. IEEE, 1–6.
- [27] Zhipeng Zhang, Xiang Liu, and Keith Holt. 2018. Positive Train Control (PTC) for railway safety in the United States: Policy developments and critical issues. *Utilities Policy* 51 (2018), 33–40.