Metrics-Driven Evaluation of Cybersecurity for Critical Railway Infrastructure

Himanshu Neema, Bradley Potteiger, Xenofon Koutsoukos
Institute for Software Integrated Systems
Vanderbilt University
Nashville, TN 37235

CheeYee Tang, Keith Stouffer
National Institute of Standards and Technology
Gaithersburg, MD 20899

ABSTRACT

In the past couple of years, railway infrastructure has been growing more connected, resembling more of a traditional Cyber-Physical System [1] model. Due to the tightly coupled nature between the cyber and physical domains, new attack vectors are emerging that create an avenue for remote hijacking of system components not designed to withstand such attacks. As such, best practice cybersecurity techniques need to be put in place to ensure the safety and resiliency of future railway designs, as well as infrastructure already in the field. However, traditional large-scale experimental evaluation that involves evaluating a large set of variables by running a design of experiments (DOE) may not always be practical and might not provide conclusive results [2]. In addition, to achieve scalable experimentation, the modeling abstractions, simulation configurations, and experiment scenarios must be designed according to the analysis goals of the evaluations. Thus, it is useful to target a set of key operational metrics for evaluation and configure and extend the traditional DOE methods using these metrics. In this work, we present a metrics-driven evaluation approach for evaluating the security and resilience of railway critical infrastructure using a distributed simulation framework. A case study with experiment results is provided that demonstrates the capabilities of our testbed.

Keywords

Metrics-driven evaluation, Model Based Simulation Integration, Cyber-Physical System, Railway Critical Infrastructure, Cybersecurity, Resilience

I. Introduction

Railway is a prime example of a Cyber-Physical System (CPS) [1], consisting of co-engineered interacting networks of computational and physical components. Infrastructure such as switches and signals are now controlled by complex autonomous algorithms, or operators located in remote monitoring centers. Due to this increased connectivity, new avenues are emerging that allow adversaries to inflict physical damage remotely through cyber vulnerabilities. Additionally, it is not just enough to utilize traditional cybersecurity techniques to harden systems, but resiliency needs to be built-in to ensure the proper and safe operation of safety-critical systems under all scenarios, including when experiencing a cyber-attack.

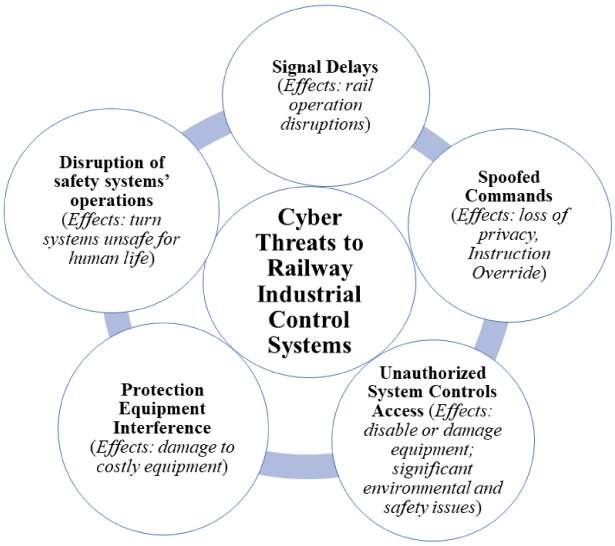

Fig. 1: Cyber Threats in Railway Networks

In traditional information technology applications, it can be difficult to determine how a cyber-attack will affect the running system, especially given that the same attack will most likely have different effects depending on which subset of the system is being attacked. Given how networks and communication channels interconnect the components of a system, determining attack propagation behavior can compound the difficulty of such analysis and prediction of attack severity. These problems are exacerbated when such networked systems are connected to sensors and actuators, coupling the system to the surrounding physical environment. In this case, the attack's effects propagate not only through the cyber and communications portions of the system, but also through the embedded controllers, and into the physical world [4] [19] [20].

This work at Vanderbilt is supported by NIST 70NANB17H266.

Modern railway systems use various equipment that comprise standard commercial components. In addition, with the increase in automation and remote system controls, new vulnerabilities have opened in the networking infrastructure for cyber threats such as delays in operation signals, spoofing of commands, unauthorized access to system controls, interference in the protection equipment, and disruptions in the operations of the safety systems. These cyber threats and their potential harmful effects are shown in Figure 1. These cyber threats were originally defined in the National Institute of Standards and Technology's (NIST) [22] special publication 800-82, revision 21 [18].

Design of Experiments (DOE) is a powerful technique for evaluating a large number of CPS scenarios. In order to evaluate different parameter value combinations, DOE methods systematically vary multiple input variables according to a sampling scheme such as *Full Factorial*, *Random Uniform*, or *Latin Hypercube*. The basic idea is to identify, explore, and evaluate important component interactions that otherwise might get missed by varying one variable at a time. Scalability becomes a key issue here, particularly when all parameter variation combinations are to be evaluated. Thus, for scalable cybersecurity evaluations of a large-scale CPS, such as railway infrastructure, goal-driven abstractions and composition of models are needed for focusing on specific system-level resilience properties and attack models and configurations.

Real-world experimental scenarios usually involve a large number of complex models, making evaluation highly challenging. The task of simulation-based CPS security evaluation requires one to build and evaluate both the cyber and physical models. However, both the cyber and physical models can be designed at many different levels of abstractions. For example, a road traffic simulation can be simulated at higher aggregate level by modeling overall city traffic patterns (i.e., *macroscopic*), or by using stochastic queuing models (i.e., *mesoscopic*), or modeling individual vehicles and their flows (i.e., *microscopic*). The level of abstraction chosen has substantial affect on the performance of the simulation. In addition, the design of experiments (DOE) and experiment scenarios also are highly dependent on the modeling abstractions used. In order to achieve scalable simulation performance, while still meeting the analysis requirements, the modeling abstractions, simulation configurations, and experiment scenarios all must be designed accordingly. Therefore, it is useful to target a set of key operational metrics for the evaluations needed [2], and configure and extend the traditional DOE methods using them.

To address the difficulties of performing impact analysis of cyber-attacks on the critical railway infrastructure, we have developed a set of key operational metrics to measure how effectively trains operate and complete schedules. We also developed a distributed simulation environment with an integrated metrics based data analytic module for the purpose of streamlining and simplifying the process of evaluating CPS designs. We further integrated a hardware-in-the-loop (HIL) testbed for conducting a more thorough evaluation of CPS software in hardware consistent with the deployment environment. This setup allows for maximizing system design safety by utilizing the computing power of the simulation testbed for scaling designs, while reserving the HIL testbed for evaluating the most critical components of the system.

The rest of the paper is organized as follows. First, in Section II we present a motivating example from the railway critical infrastructure domain. Section III describes the operational metrics we developed for railroad operations. Section IV provides a detailed overview of our testbed. Section V presents a detailed case study and experiment results. Section VI discusses the related work. Finally, Section VII concludes the paper and discusses our future work.

II. Motivating Example: Train Level Crossing Architecture Evaluation through HIL Simulation

NIST [22] has developed a testbed for railroad transportation systems. The purpose of the testbed is to study the effects of cybersecurity measures on the railroad system and to measure its performance impact. In our testbed, the railroad track system and the movement of trains were previously simulated in the software. However, it is more effective to simulate the railroad system operation in the laboratory environment. To better simulate the real-world environment, we have extended the testbed to support an HIL architecture. It uses real embedded hardware that is used in real-world deployment to sense and actuate the physical system.

A. Railway Level Crossing Network Architecture

We have identified the railroad level-crossing system to use in our HIL implementation. As shown in Figure 2, level-crossing is an interaction where a railroad track crosses a road at the same level. There are over 130,000 railroad level-crossings in North America. Higher traffic level-crossing usually has a signal system to help manage the traffic, and the system typically consists of several components (Figure 3):

- Siemens S7-1500 series Programmable Logic Controller (PLC) system with an Ethernet interface, an analog input output (AIO) card, and a digital input output (DIO) card.
- Motor controller and two motors to drive the gate barriers.
- Motion sensors to detect the position and speed of a train approaching and departing the crossing.
- Light-Emitting Diode (LED) array to provide the functionality of a road signal and warning sign.

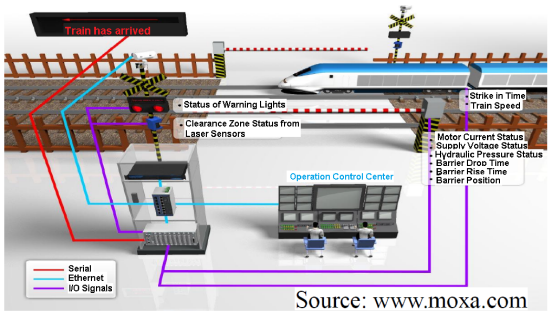

Fig. 2: Train Level Crossing

B. Theory of Operation

The PLC acts as the controller of the overall signal system for the crossing. The motion sensors are connected to the AIO of the PLC to provide the location and speed of the approaching or departing train. The motor controller is connected to the DIO of the PLC to control the gate movement, and the LED array is connected to the DIO.

The PLC will sample the analog input periodically to determine if any train is in the level-crossing proximity. When an approaching train's position and speed are determined, the PLC will calculate the time for the train to reach the level-crossing and will command the motor controller to lower the gates and to flash the road and warning signals. Figure 3 shows the input and output signals from the level crossing system. The requirement is to have the gate in lowered position and warning signals in active mode at least 10 seconds before the train arrives, but no more than 30 seconds before the train arrives, regardless of the train speed. For example, if the train is 1km away from the crossing and traveling at 10km/h, the controller has about 6 minutes to lower the gate and to flash the warning signals. If the same train is traveling at 30km/h, the controller only has 2 minutes to respond.

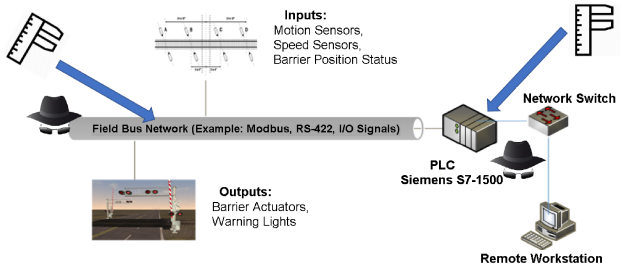

Fig. 3: Rail Crossing Input and Output Signals

Figure 4 shows how Command and Control Wind Tunnel (C2WT) [8] (described in section IV.A) is used for this HIL simulation. As shown, the PLC is connected to C2WT via the Ethernet port, and the simulation components *Train Operation* and *Dispatch Center* are executed directly in C2WT.

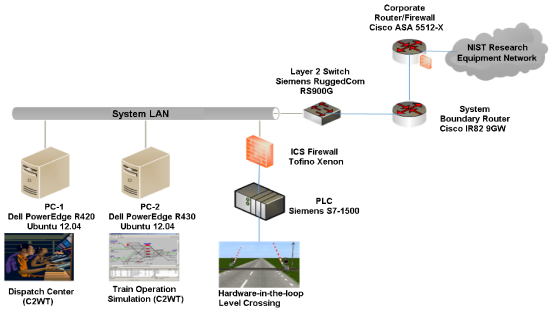

Fig. 4: Level Crossing Network Architecture

III. Operational Metrics

As part of experimental evaluations conducted using our testbed, we have identified several key metrics that have operational significance to the railroad operation. As shown in Table I, these operational metrics include: route length, travel time, average duration, train speed, average train speed, individual waiting time, average waiting time, accumulated waiting time, train length, and fuel cost.

Distance (Route Length) (*Units: meters*)	Total distance that the train travels according to the actual path taken. This path is dependent on the railroad switch control algorithm for achieving better throughput of trains.
Duration (Travel Time) (*Units: seconds*)	Travel time of a train from origin to destination.
Average Duration (*Units: seconds*)	Average duration of all trains in the network.
Train Speed (*Units: meters/second*)	Average speed of a train from origin to destination.
Average Train Speed (*Units: meters/second*)	Average train speed of all trains in the network.
Individual Waiting Time (*Units: seconds*)	Amount of time since last time step in which a train has been idle, stopped, or moving slower than 1 meters/second.
Accumulated Waiting Time (*Units: seconds*)	Total amount of time for which a train is idle, stopped, or moving at slower than 1 meters/second during a trip.
Average Waiting Time (*Units: seconds*)	Average accumulated waiting time of all trains in the network.
Train Length (*Units: meters*)	Length of a train. This can also be transformed into other metrics such as number of rail cars.
Fuel Cost (*Units: milliliters*)	Total fuel a train consumes between its origin and destination.
Average Fuel Cost (*Units: milliliters*)	Average fuel cost of all trains in the network.

TABLE I: Operational Metrics

Along with metrics of the communication network, control network, and computing resources, these metrics will form the basis to assess the performance impact of the railroad system when cybersecurity measures are implemented. We use some of these key operational metrics in our experimental case study (provided later in the paper) in order to study the resilience properties of the railway critical infrastructure in the presence of a full or partial cyber-attack.

IV. Testbed Architecture

Railway infrastructure is an integral part of modern businesses, from shipment of goods to transportation of passengers. Therefore, maintaining the safety of rail operations is critical. Further, owing to an immense growth of cyber-attack capabilities, cybersecurity of the entire railway systems must be evaluated to ensure resilient rail operations even in the presence of cyber threats. Railway operations are complex and involve many cooperating components including physical devices, computation and control nodes, communication networks, and human operators and operational workflows. Thus, to evaluate the cybersecurity of railway networks and the effect of cyber-attacks on the rail operations, we need to integrate a number of simulators and execute them in an

integrated manner. Our testbed for evaluating cybersecurity of rail operations leverages our past research work and is built using C2WT [8].

In this section, we describe the core technological components of our testbed. The majority of these components have been previously published. Therefore, below we only provide a brief summary of each of them and point the reader to appropriate references.

A. Command and Control Wind Tunnel

The C2WT [8] is a novel, distributed, heterogeneous simulation integration framework. It has a composable and modular architecture. The framework provides an intuitive and extensible platform for rapidly integrating many heterogeneous simulations. Each of the integrated simulations can be executed using a variety of special-purpose simulation tools that span many application domains.

1) Overview: The C2WT framework provides a model-based integration approach. In this approach, models are used not only for the system modeling, but also for their configuration, parameterization, integration, and execution. Each of the integrated simulators are represented as abstract modeling elements and their interactions are also captured using model relationships. The framework relies on the IEEE standard for distributed simulations called the High-Level Architecture (HLA) [12]. To support HLA-based distributed simulation, we use an open source HLA implementation (a.k.a. *Run-Time Infrastructure (RTI)*) called *Portico* [21]. The framework automatically synthesizes the *integration code* according to the models. This integration code for each integrated simulation adapts the original simulation model to become HLA compliant, which can be executed directly as a supported simulation over the RTI.

2) Reusable Communication Network Simulation: Railway operations are really an example of a complex cyber-physical system (CPS) [1]. The cyber aspects of CPS (i.e., communication, control, and computation) are central to their proper functioning. Additionally, as in CPS the physical and cyber components are tightly inter-connected, a small change in cyber component can cascade to large problems in the physical components. Thus cybersecurity evaluations are central to all CPS, such as railroad operations. However, integrating a communication network simulator is a challenging task as it requires one to properly work with the variety of devices, network layers, communication protocols, application models, etc. For this purpose, we designed a generic communication network simulation component that can be directly used in any CPS cybersecurity evaluation scenario. The only customization it needs is the network topology and its routing configuration. [7]

3) Cyber-Attack Library: Cyber-attacks are needed for evaluating how the system will behave when a particular cyber-attack is enacted on the system's communication network. For example, in railroad operations, a Distributed Denial of Service (DDoS) attack on a key control server can easily disrupt the entire operations and can potentially lead to highly damaging consequences. In order to make it reusable, we developed a customizable, modular cyber-attack library [7] that can be used in any cybersecurity evaluation scenarios by simply configuring the cyber-attacks. The configuration of different attacks in the library require different parameter values in the configuration. For example, a *Network Filter Attack* requires one to specify the source and destination network subnets and the full path of the network node on which the attack is enacted. The result is that all network traffic, that has the origin and destination address matching to that specified in the configuration of the attack, gets filtered out, while the rest of the network traffic continues to flow as normal. A large library of such cyber-attacks has been developed and can be easily used for cybersecurity evaluations.

4) COAs for Scenario-Based Experimentation: The integrated simulation, even with configured cyber-attacks for a particular experimental scenario, still represents a static evaluation. In order to evaluate the systems under a variety of dynamic test scenarios (such as many different *what-if* situations), we developed a language that can be used to program such scenarios. We call it the Courses-of-Action (COA) modeling language [7]. Each COA model, based on this language, represents a sequence of *observations* and *actions* that interact with the running distributed simulation. For example, based on messages sent between certain simulators, the COA executor can inject new information into the simulation that can drive the simulation into a different evaluation trajectory. Such COA models are highly useful for evaluating potential cyber threats on CPS. For example, one can use the injection of different cyber-attacks (from the cyber-attack library) in different COA models and test them against different security mechanisms. This is sometimes also referred to as *cyber-gaming* in the literature. The COA execution engine in our testbed can perform full factorial of all COA combinations that the user models and packages into different COA-Groups.

B. Train Simulators

In our testbed, we had previously integrated a train simulator called TrainDirector [23] and published our work on railroad operations [3]. In our current work, we use *Simulation of Urban MObility (SUMO)* [26] for simulating trains. We have developed an integration adapter for SUMO previously in order to make it HLA-compliant [6]. We use SUMO's Traffic Control Interface (TraCI) for interacting with the SUMO process running in parallel and controlling its scheduler for synchronizing the simulation with the rest of the simulators.

C. HIL Testbed

From our past experience, we realized that many attacks and physical phenomena are not easily suited to simulations. For example, an attack that changes system behavior after a certain sequence of characters are pressed on the keyboard is better deployed directly on the hardware. Similarly, when a large number of zombie network nodes are to be used in a network simulation in order to achieve the effect of a *DDoS* attack, it can be computationally highly expensive. In fact, it can be so

slow that it may become unusable. On the other hand, the same attack implemented in the hardware using a set of embedded boards can easily generate and send a large number of network packets and can effectively and quickly perform the DDoS attack. For this purpose, we have created a novel HIL testbed that is configurable for different use-cases. In our testbed [6], we have a set of embedded boards, a programmable network switch for emulating the communication network, a physics simulator, and a computer for developing and controlling the HIL-simulation.

V. Case Study: Impact Assessment of Cyber-Physical Attacks on Railroad Networks

This reference case study is based on a railway transportation system. In this example, there are many railway signals and switches that route trains throughout the rail network. Railway signals have a green or red state and determine whether a train can travel to the next rail segment. In circumstances where a junction exists that connects multiple rail segments, rail switches are used to route trains to the appropriate adjacent rail segment. Each rail switch or signal is controlled by command messages sent through a communications network by a train operator located at a central facility. The communication network is comprised of network switches, routers, and basestations that transport communications from a central operating station to the respective rail segments.

Figure 5 shows the railway network used for this case study. Here, the trains start at node *A* and are pre-routed through the railway network to arrive at a randomly chosen destination out of three locations, viz. *B*, *C*, or *D*. Each destination location has three possible routes leading to it from the starting point. By default, trains are assigned the route that has the minimum travel time to reach the destination location. To simulate unexpected delays that occur in the real world, each train is assigned a respective speed constraint for every rail segment in the rail network based on a random distribution between 7 and 15 meters per second. As such, the current optimal route the train can take to reach its destination at the current time, may not be the best in the future due to the changing of rail segment speeds, as well as congestion caused by other trains in the network. This behavior leads to trains being distributed through the complete subset of the possible routes to optimize the flows throughout the rail network.

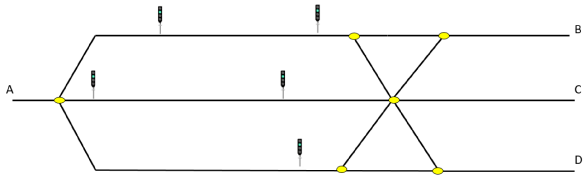

Fig. 5: Railway Network

For the CPS cyber-attack experiment, a critical rail segment is selected for attack which serves as a central hub to the rest of the network. Additionally, we look at the impact of physical manipulations such as construction on the efficiency of the trains. To analyze these cascading effects, we simulated three scenarios as described in the sub-sections below.

Metric	**Baseline**	**Partial Attack**	**Rail Block**
Fuel	3907 mL	4785 mL	5631 mL
Waiting Time	10.52 s	131 s	241 s
Train Length	66m	66 m	66 m
Train Travel Distance	8314 m	8356 m	8420 m
Train Travel Direction	993 s	1230 s	1448 s
Average Train Speed	8.36 m/s	6.97 m/s	6.22 m/s

TABLE II: Operational Metrics from Railway Simulation

A. Scenario 1: Baseline Operation

This scenario focuses on normal operation of a rail network with no blockages. This case provides a baseline for measuring the respective effects of the attack on the train scenario. In experiment results, it is shown in blue color.

B. Scenario 2: Partial Cyber-Attack

This scenario focuses on the effects of cyber-attacks on the physical behavior of the trains. In this scenario, a DDOS attack campaign will be executed on the communication leading to the first railway switch element, preventing communication from the central operating system, and leading to an inoperable state for the rail switch. However, at approximately halfway through the simulation, we assume that the security personnel have successfully resolved the situation by rerouting communication through a parallel communication network to reach the rail switch element. This enables the rail switch to become operable and allows for trains to access all of the respective routes. In experiment results, it is shown in red color.

C. Scenario 3: Full Railroad Blockage (Physical Attack)

This scenario focuses on the effects of physical manipulations on the train routes, and arrival times. The bottom two routes will be closed due to physical damage, presumably caused by a physical attack on the railway infrastructure. As such, the trains will be rerouted to the top route, forming increasing congestion due to waiting times at respective rail signals on the route. With the backups on the routes, trains will be delayed, possibly arriving late for deliveries. In experiment results, it is shown in yellow color.

D. Experiment Results

To illustrate the results, we performed all three scenarios in parallel, while developing a real time interactive plotting mechanism for comparing the various results. This plot obtains the real time results for the average speed of all vehicles in a simulation, as well as the average waiting time of all vehicles at the current time step. By comparing this real time plot results to the graphical illustrations in SUMO, the attack's physical effects can be analyzed in context. Table II shows the key operational metrics calculated from the railway simulation for each of the scenarios.

A post-simulation plotting mechanism was also implemented for comparing simulation based metrics such as average speed, average waiting time, average trip consumption, and average trip duration where the results of all vehicle trips are averaged together. Figure 6 illustrates the live measurement results during the simulation, and Figure 7 illustrates the post-simulation simulation results. Finally, Figure 8 illustrates the observable congestion within the physical simulator (SUMO) resulting from the cyber-attack during the simulation.

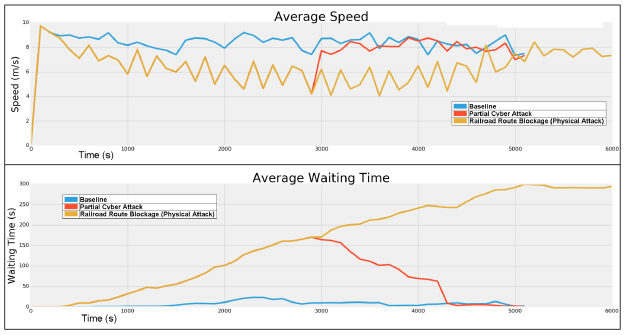

Fig. 6: Results During Simulation

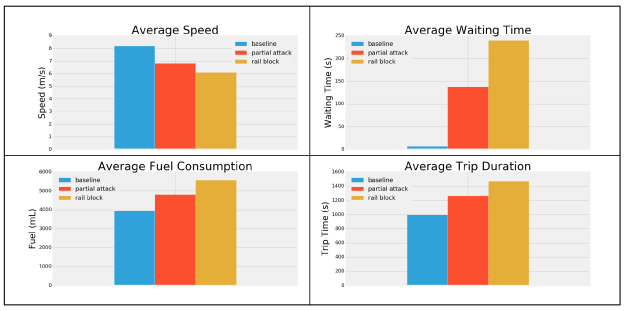

Fig. 7: Post Simulation Results

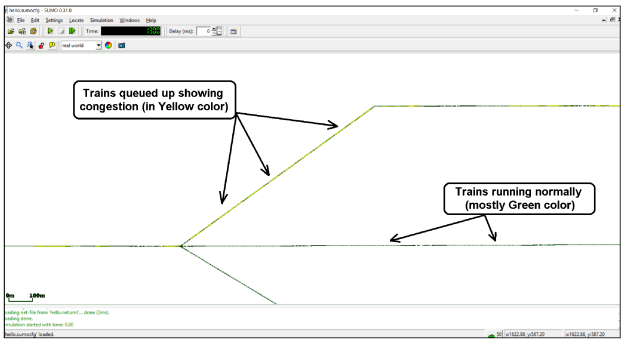

Fig. 8: Sumo Railway Simulation

From analyzing the results, various scenarios can be compared by metrics-driven evaluation, combined with visual observation within the physical simulator. The two attack scenarios were successful in increasing the congestion within the railway network, negatively affecting the efficiency of the railway trips. Additionally, it is observed that once the partial attack is resolved at approximately 3,000 seconds into the simulation, the efficiency of the train trips increases to the baseline level as a result of the other two routes opening up. It is due to this fact that the full attack scenario has the worst results, with the partial attack scenario second, and the baseline scenario with the best results. For example, when comparing the train travel duration, the baseline scenario had an average of 993 seconds per train trip, while the partial attack and full rail block scenario had an average of 1230 seconds and 1448 seconds, respectively. This corresponding difference is further represented as a 23% increase in trip duration for the partial attack scenario, and 45% increase for the full rail block scenario compared to the baseline scenario.

VI. Related Work

In recent years, there have been a number of successful attacks against CPS, illustrating the ability to inflict physical damage through cyber vulnerabilities. These attacks have provided motivation for the rise of security and resilience research within the CPS field. Security looks at implementing prevention mechanisms to deter attacks, while resilience focuses on maintaining safe operation of a compromised system. The key challenge is to integrate both security and resilience models to provide optimal protections, while ensuring safe and reliable operation during all scenarios [5]. To accomplish this task, modeling and simulation have been widely utilized to analyze the vulnerability of systems. The HLA is an IEEE standard that has been widely popular for utilization within distributed simulation environments relating to safety-critical applications [12]. Additionally, there has been extensive work related to domain-specific modeling toolsuites, most notably the WebGME meta-modeling toolsuite [9].

Cyber-attacks on railway infrastructure have been limited thus far. Most attacks have been of the physical nature using Improvised Explosive Devices (IEDs) or other explosive devices [16]. However, there have been some high profile crashes caused by failures in railway infrastructure such as positive train control [17]. These examples pose the closest resemblance of the potential consequences of a successful cyber-attack. Additionally, there have been concerns in the past about adversarial actors leveraging these types of systems, to inflict maximum damage with a limited amount of resources [13].

In order to protect these critical infrastructure systems, there has been increasing research from the CPS perspective [1], including securing the communication between sensors and actuators in the network [14], as well as implementing detection algorithms for more rapidly identifying suspicious activity to the train operators [15]. Hubaux, et al. provide a good overview of security and privacy of smart vehicles [24]. Hoh, et al. describe techniques of enhancing security and privacy in a traffic-monitoring system [25]. In addition, there are existing testbeds that aim to assess security of complex Industrial Control Systems (ICS) [10] [11].

VII. Conclusion and Future Work

Railway represents a critical infrastructure that we rely on for our transportation needs. It is crucial that the railroad operations continue safely and in a resilient manner in the presence of cyber-attacks. However, railway operations are highly complex as they involve not only a tight interaction of physical and computational components, but also human operators and controllers. Ensuring cybersecurity of these operations thus becomes highly challenging. A large number of experimental analyses are needed for evaluating the designed security mechanisms and operational workflows. As this is a rather complex problem with potentially millions of variables, the evaluations need to be goal-driven. The key resilience metrics against the operational goals can be evaluated under a variety of cybersecurity scenarios. In this paper, we developed a set of core metrics for railroad operations and presented our distributed simulation testbed that can be used for cybersecurity evaluations of the railroad operations and measure its operational performance by calculating these metrics for each scenario. We also demonstrated the testbed capabilities through an extensive case-study.

In our experiments, we used a standard coordination protocol for railway scheduling and switching control. In the future, we plan to deploy novel security mechanisms in our testbed and investigate algorithms that makes the railroad operations resilient against cyber threats. Additionally, for the train level-crossing system, the PLC is currently using its AIO and DIO cards to interface with the sensors and actuators (motor controller and LED array). In the future, we plan to use the Controller Area Network (CAN) protocol for the PLC to communicate with the sensors and actuators because a CAN network can support a more scalable and complex crossing system with more sensors and actuators.

References

[1] B. Chen, C. Schmittner, Z. Ma, W. G. Temple, X. Dong, D. L. Jones, and W. H. Sanders, "Security analysis of urban railway systems: the need for a cyber-physical perspective," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2014, pp. 277–290.

[2] Subhav Pradhan, Abhishek Dubey, Tihamer Levendovszky, Pranav Srinivas Kumar, William A. Emfinger, Daniel Balasubramanian, William Otte, and Gabor Karsai, "Achieving resilience in distributed software systems via self-reconfiguration," *Journal of Systems and Software*, vol. 122, pp. 344–363, Dec. 2016.

[3] Bradley Potteiger, William Emfinger, and Xenofon Koutsoukos, "Evaluating the Effects of Cyber-Attacks on CPS using a HIL Simulation Testbed," *Resilience Week*, Aug. 2016.

[4] Neema, H., J. Sztipanovits, M. Burns, and E. Griffor, "C2WT-TE: A Model-Based Open Platform for Integrated Simulations of Transactive Smart Grids," *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Apr. 2016.

[5] B. Potteiger, Z. Zhang, and X. Koutsoukos, "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, 2018, p. 5.

[6] Himanshu Neema, Bradley Potteiger, Xenofon Koutsoukos, Gabor Karsai, Peter Volgyesi, and Janos Sztipanovits, "Integrated Simulation Testbed for Security and Resilience of CPS," *The 33rd ACM/SIGAPP Symposium On Applied Computing*, Apr. 2018.

[7] Himanshu Neema, "Large-Scale Integration of Heterogeneous Simulations," *Ph.D. Dissertation, Vanderbilt University*, Jan. 2018.

[8] Neema, H., H. Nine, G. Hemingway, J. Sztipanovits, and G. Karsai, "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.

[9] J. Sztipanovits and G. Karsai, "Model-integrated computing," *Computer*, vol. 30, no. 4, pp. 110–111, 1997.

[10] C. Davis, J. Tate, H. Okhravi, C. Grier, T. Overbye, and D. Nicol, "SCADA cyber security testbed development," *In 38th North American Power Symposium (NAPS)*, pp. 483–488, 2006.

[11] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," *In 2011 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–7, 2011.

[12] "IEEE Std 15162010, IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)- Framework and Rules," pp. 1–38, 2010.

[13] B. Gellman, "US fears Al Qaeda cyber attacks," *Washington Post*, vol. 26, p. 1, 2002.

[14] J. Moreno, J. M. Riera, L. De Haro, and C. Rodriguez, "A survey on future railway radio communications services: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 62–68, 2015.

[15] A. V. Chernov, M. A. Butakova, and E. V. Karpenko, "Security incident detection technique for multilevel intelligent control systems on railway transport in russia," in *Telecommunications Forum (TELFOR), 2015 23rd*. IEEE, 2015, pp. 1–4.

[16] W. Rose, R. Murphy, and M. Abrahms, "Does terrorism ever work? The 2004 Madrid train bombings," *International Security*, vol. 32, no. 1, pp. 185–192, 2007.

[17] J. Peters, "Positive train control (PTC): overview and policy issues," 2012.

[18] "NIST Special Publication 800-82, revision 21 - Guide to Industrial Control Systems Security, URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf," Apr. 2018.

[19] Mitropoulos, D., Karakoidas, V., Louridas, P., Gousios, G., and Spinellis, D., "Dismal code: Studying the evolution of security bugs," *In Proceedings of the LASER Workshop*, pp. 37–48, 2013.

[20] Hahn, A., Ashok, A., Sridhar, S., and Govindarasu, M., "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," Smart Grid, IEEE Transactions on 4, *2*, pp. 847–855, 2013.

[21] "Portico - RTI, URL: https://github.com/openlvc/portico," Apr. 2018.

[22] "National Institute of Standards and Technology, URL: https://www.nist.gov/," Apr. 2018.

[23] "TrainDirector RailRoad Simulator, URL: http://www.backerstreet.com/traindir/en/trdireng.php," Apr. 2018.

[24] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy, vol. 2, no. 3*, pp. 49–55, 2004.

[25] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems," *IEEE Pervasive Computing, vol. 5, no. 4*, pp. 38–46, 2006.

[26] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO – Simulation of Urban MObility: An overview," in *Proceedings of the 3rd International Conference on Advances in System Simulation (SIMUL)*, 2011, pp. 63–68.