Railway System Failure Scenario Analysis

William G. Temple[1], Yuan Li[1], Bao Anh N. Tran[1], Yan Liu[1], Binbin Chen[1]

Advanced Digital Sciences Center, Illinois at Singapore
1 Fusionopolis Way, Singapore 138632
{william.t, yuan.li, baoanh.t, yan.liu, binbin.chen}@adsc.com.sg

Abstract. Cyber security has emerged as an important issue for urban railway systems (URS) due to the increasing usage of information and communication technologies (ICT). As a safety-critical public infrastructure with complex, interconnected, and often legacy systems, URS pose challenges for stakeholders seeking to understand cyber threats and their impact, and prioritize investments and hardening efforts. However, other critical infrastructure industries such as the energy sector offer best practices, risk assessment methodologies, and tools that may be both useful and transferable to the railway domain. In this work we consider one successful security initiative from the energy sector in North America, the development of common failure scenarios and impact analysis (NESCOR failure scenarios), and assess their applicability and utility in URS. We use a publicly-available software tool that supports failure scenario analysis to assess example failures on railway supervisory control systems and identify directions for further improving railway failure scenario analysis.

1 Introduction

Urban transportation systems are increasingly reliant on information and communication technology (ICT) for more efficient operation with lower cost. However, such systems come with an elevated risk of malware and targeted cyber attacks by malicious agents. Multiple cyber incidents affecting the rail industry have been reported publicly [4]. For example, in 2003 the "So Big" virus caused a morning shutdown of CSX's signalling and dispatch systems in 23 states in the U.S. In another case from 2008, a Polish teenager used a wireless remote controller to change track points, derailng multiple trains and injuring 12 people. More recently, in 2016, a UK-based cybersecurity firm disclosed the discovery of four cyber attacks against UK rail infrastructure within a period of twelve months [13]. As the threat landscape changes, coping with the increasing risks of cyber attacks has become a major concern for transit agencies. For those organizations, systematic risk assessment is essential for exploring system vulnerabilities and supporting the design and deployment of more secure systems.

One approach that has proven useful in other critical infrastructure domains is the practice of failure scenario analysis. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of cyber assets creates a negative operational impact. The most

prominent example of this practice is the failure scenario and impact analysis compiled by the U.S. NESCOR (National Electric Sector Cybersecurity Organization Resource) Technical Working Group 1(TWG 1) in the electric power industry. The NESCOR failure scenarios [21] describe specific types of undesirable cyber incidents and their impacts, as well as the vulnerabilities and potential mitigations associated with the failures. Their work, progressively updated and released from 2012 through 2015, pushes toward more comprehensive and rigorous security assessment in the industry.

However, as far as we know there is no similar systematic failure scenario analysis effort in transit control systems, and the extent to which scenarios from the power domain may be translated to railway is unclear. In this work, we seek to bridge this gap by (1) assessing the structural differences between power and railway infrastructure, (2) identifying the applicability of NESCOR failure scenarios to railway systems, and (3) proposing sample failure scenarios that are then analyzed for a railway supervisory control system. To carry out the railway case study we leverage a publicly-available software tool called CyberSAGE, which has been recently used for electric power grid failure scenario analysis [20].

The paper is organized as follows. In Section 2 we introduce the concept of failure scenarios and analyze the translatability of power grid scenarios to the railway domain. In Section 3 we provide examples of railway failure scenarios for the supervisory control system. In Section 4 we provide a case study by using the CyberSAGE software tool to analyze scenarios on a specific system model. We discuss related work in Section 5 and conclude in Section 6.

2 Failure Scenario Analysis: From Power Grid to Railway

The cybersecurity of critical infrastructure systems has received significant attention over the last decade. One infrastructure in particular that has emerged at the forefront of this awareness and system hardening effort is the electric power grid. High-profile research projects and academic/industry partnerships have brought new tools and best practices into the power industry and increased system resilience [8, 9]. This proved to be much needed: according to ICS-CERT in the U.S., over 40% of cyberattacks targeting industrial control systems in 2014 were focused on the energy sector [19]. Transportation, however, was also significant at 5% and in other parts of the world (e.g., Europe, Asia) public transport plays an even more critical role in citizens' lives than in the U.S.

In the U.S. electric power sector there was an important government/industry initiative to establish a set of electric sector failure scenarios and impact analyses. That reference document allowed utility companies to share a common understanding of typical cyber threats facing the industry, and provided a resource for educating staff, communicating requirements to vendors, and conducting risk assessment. It is our belief that other industries—particularly the rail transportation industry—can benefit from adopting a similar failure scenario framework that is shared throughout the industry. In this section we describe the key fea-

tures of NESCOR failure scenarios and provide an example. We then discuss our process and the challenges for translating this concept into the railway domain.

2.1 NESCOR Failure Scenarios for the Energy Sector

Detailed documentation from the NESCOR team may be found online [16]. In this section we summarize salient features and objectives of the effort to provide readers with context for our own work on railway system failure scenarios.

According to NESCOR Technical Working Group 1 [21]: *A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power.* These failure scenarios have been developed for various power grid subsystems, including generation (GEN), advanced metering infrastructure (AMI), and distributed energy resources (DER) among others.

Irrespective of the power grid subsystem, the failure scenarios follow a common format: (1) a text description of the failure; (2) a list of relevant vulnerabilities enabling the failure; (3) a list of impacts; and (4) a list of potential mitigations. Below we provide an excerpt from scenario DER14 [21], which is relevant to renewable generation or energy storage systems, as a reference:
Example Scenario: DER Systems Shut Down by Spoofed SCADA Control Commands

- **Description:** A threat agent spoofs DER SCADA control commands to perform emergency shutdowns of a large number of DER systems simultaneously.
- **Sample Vulnerability:** *Users lack visibility of threat activity*, specifically messages sent to DER systems but not originated by the SCADA system
- **Sample Impact:** Power system instability, including outages and power quality problems
- **Sample Mitigation:** *Authenticate data source* for the DER SCADA protocols

Certainly the impacts in a NESCOR failure scenario are specific to the power grid, but other aspects are more general. While the original NESCOR document contained ad hoc vulnerabilities and mitigations for each scenario, the newer versions have systemized these to establish 82 common vulnerabilities and 22 common mitigations across all subsystems. In the scenario description above these are indicated by italicized text, while non-italicized text contextualizes the vulnerability or mitigation more specifically to the scenario at hand. Table 1 provides additional examples of common vulnerabilities and mitigations.

2.2 Toward Railway Transportation Failure Scenarios

Our process for adapting cyber failure scenario analayis for railway applications is to (1) identify critical sub-systems that form the basis for scenario categories;

Common Vulnerabilities	Common Mitigations
system takes action before confirming changes with user	authenticate users
users lack visibility that unauthorized changes were made	check message integrity
network is connected to untrusted networks	limit remote modification
default password is not changed	test after maintenance

Table 1: Examples of NESCOR common vulnerabilities and mitigations.

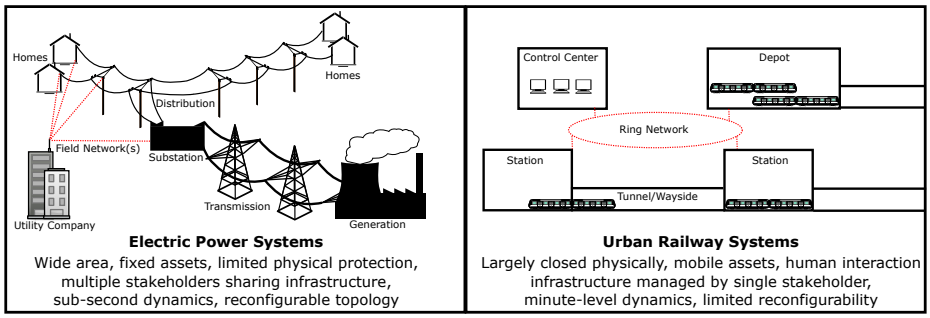


Fig. 1: Contrasting power grid and urban railway systems.

(2) assess which features and information can be leveraged from the electric power grid effort; and (3) develop the failure scenario details. We address steps 1 and 2 in this section, and provide example scenarios in the next section. This preliminary work has been undertaken as part of an ongoing research project [7]. However, to realize a similar level of impact as the power grid NESCOR scenarios, a broader consortium or working group effort is necessary.

To address the first step, it is necessary to differentiate between main line (long distance, typically above ground) and urban (shorter distance, often underground) railway systems. Each present certain unique cyber security challenges. For example, urban railway systems (i.e., metro systems) typically rely more heavily on automation than main line systems due to their more controlled environment. Main line systems place more emphasis on interoperability, leading to standardization efforts like the European Train Control System. As a starting point we focus on urban railway systems in this paper. Through survey and discussions with railway stakeholders, our team assessed the system architecture of automated passenger railway (metro) infrastructure and identified operationally-critical subsystems which may be appropriate for failure scenario analysis. These include the *traction power system*, *signalling system*, *tunnel ventilation system*, *communication systems*, and *trainborne systems*. Particularly in newer rail systems, the various operational subsystems will be integrated and managed through a common supervisory control and data acquisition (SCADA) system (see Section 3). This represents a key point of differentiation with respect to the power grid, which often has siloed communication and control systems (e.g., the advanced metering network, the substation control network). Following on this point, the second phase in developing railway failure scenarios is leveraging information from the NESCOR power grid effort.

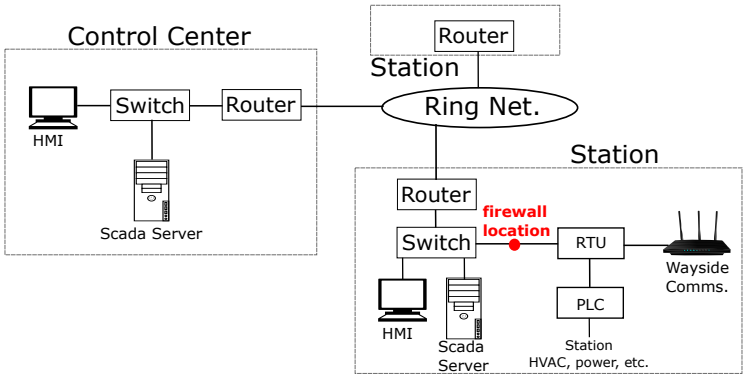


Fig. 2: Sample railway control system architecture emphasizing station devices.

Translating scenarios across domains Due to the fundamental differences between power and railway systems (see Figure 1) it is not straightforward to directly translate failure scenarios between domains. We examined each of the 123 NESCOR failure scenarios (excluding the 'generic' category, which is applicable by definition) to identify those which could translate to the railway domain. Of the original power grid scenarios, 64 (52%) were found to be translatable, either due to the nature of the cyber threat/failure, or the types of systems/devices that were affected. For example, one could imagine a scenario similar to AMI.8–*False Meter Alarms Overwhelm AMI and Mask Real Alarms* unfolding with false alarms in railway supervisory control systems. Similarly, DER.9–*Loss of DER Control Occurs due to Invalid or Missing Messages* could be reinterpreted as *Loss of train control occurs due to invalid or missing messages.*

To identify common failure modes, we categorized those 64 scenarios according to the following list:

- **Message** [34%] spoofing, false data injection, or improper commands
- **Malware** [19%] introduction of compromised or malicious software
- **Configuration** [17%] incorrect or compromised device/system settings
- **Access control** [14%] inadequate physical or logical access control
- **Denial of service** [9%] degradation or disruption of a system service
- **Process** [4%] absent or inadequate business processes

While the relative frequency of those failure classes are most meaningful within their application setting (i.e., power grid), the classification process provides insights into the types of failures that may be of concern in railway systems. The railway supervisory control system in particular, identified as a critical subsystem earlier, may be particularly susceptible to message, malware, or denial of service failure scenarios. In the next section we use the NESCOR common vulnerabilities/mitigations to develop two failure scenarios focusing on these issues.

3 Sample Railway System Failure Scenarios

In the previous section, messages, malware, and denial of service were identified as high-risk failure modes for railway systems. In this section we examine a sample railway control system loosly based on the reference architecture in NIST Special Publication 800-82 [24], which is shown in Figure 2, and describe two railway failure scenarios that could impact that system. In Section 4 we introduce and apply a tool to analyze these scenarios. As we discuss in the case study (Section 4.2), these scenarios illustrate trade-offs and conflicting objectives for system operators seeking to secure their infrastructure.

3.1 Compromised HMI sends malicious commands to devices

A human-machine interface is infected with malware, either through a USB flash drive, or through the network. This malware can send unauthorized commands to devices in the station or at the trackside to disrupt railway operations.

Vulnerabilities

- *system permits installation of malware* in the HMI
- *system permits potentially harmful command sequences* enabling the compromised device to affect operations

Impact

- Settings are changed, degrading system performance
- Devices are remotely shut down, affecting train service

Mitigation

- *authenticate users* for all software changes
- *test after maintenance* for malware
- *create audit logs* of all changes to software
- *protect audit logs* from deletion
- *validate inputs* with the user for all control actions
- *authenticate messages* communicated in the SCADA network

3.2 SCADA firewall fails and critical traffic cannot reach devices

SCADA firewalls are installed to only allow authorized computers to send commands to control devices. In some cases, these firewalls are susceptible to Denial-of-Service attacks (DoS) that are exploitable by low-skill attackers[12]. Once under DoS, no packet can go through the firewall, which disrupts critical real-time communication with devices.

Vulnerabilities

- *commands or other messages may be inserted on the network by unauthorized individuals*
- *unnecessary access is permitted to system functions*

Impact

- Operators from the control center lose sight of the status of devices
- Operators from the control center are unable to send commands to devices

Mitigation

- *restrict network access* to firewall administrative functions
- *require intrusion detection and prevention* as part of the SCADA network

4 Analyzing Scenarios for a Railway System

While there are ancillary benefits to developing a common set of railway system failure scenarios, the main objective is enhancing cyber risk assessment. To this end, tool support is important to help operators quickly and easily assess their risk exposure and make decisions about how best to harden their systems. In this section we adapt the CyberSAGE tool [2], which is freely available for academic users, to conduct a case study using the railway supervisory control failure scenarios from Section 3.

4.1 Failure Scenario Analysis Tool

The CyberSAGE tool was originally developed for analyzing security properties in cyber-physical systems [25]. It was subsequently extended to support analysis of NESCOR failure scenarios over a user-defined system model in the power and energy sector [20]. We use that version of the tool as a starting point for our work analyzing railway system failure scenarios.

At a high level, the process for analyzing a failure scenario is as follows:

1. Represent the scenario description as a mal-activity diagram [23]
2. Draw the system architecture and specify properties
3. Specify adversary profiles describing skills, resources, access, and intention
4. Modify graph generation rules, if necessary
5. Generate the assessment results

Note that steps 1-3 need not be followed in any particular order. Since identifying assets and interfaces is typically the first step in cyber risk assessment [22], we created the system architecture model first. As an output, CyberSAGE calculates the probability of a failure scenario occurring based on user-defined properties. An analyst may then multiply this probability with an impact value (e.g., financial loss) for the failure scenario to compute a risk score.

Certain modifications were necessary to adapt CyberSAGE for railway systems. The software has a GUI for drawing a system using devices and edges. There are a number of default devices, and each device has a list of properties. For the most part, the existing devices were sufficient to model railway SCADA systems, but some new devices (e.g., programmable logic controller) had to be created during step 2 of the process. This involves naming the device and specifying an image to use as the icon. Each device has a set of properties associated with it. Rather than creating new properties, we re-used the property set from other devices. During the assessment, the user can deactivate or otherwise modify a specific device's properties, so having a large default set was not restrictive.

Finally, during step 4 it was necessary to create new rules for combining the various inputs. These are specified in a drools format [3]. To model scenario 3.2 we created a *reboot system template* to capture the vulnerabilities and mitigations associated with the firewall.

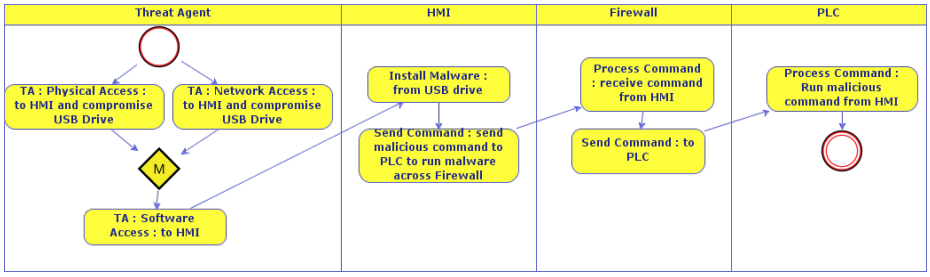


Fig. 3: Mal-Activity input for Scenario 3.1 with SCADA firewall.

Attacker	IT Skill	Domain Knowledge	Physical Access	Logical Access
Insider	Medium	High	True	True
Contractor	Low	Low	True	False
Nation State	High	High	False	True

Table 2: Adversary profiles

4.2 Case Study: Deploying SCADA Firewalls

We observe from the failure scenarios in Section 3 that adding SCADA firewall devices to station control networks can help to mitigate certain failures (e.g., malicious commands), while potentially introducing new failure scenarios. In this case study we assume the role of a railway operator seeking to holistically evaluate the benefits of adding SCADA firewalls to the system shown in Figure 2. This example is intended to illustrate the role that systematic failure scenario analysis can play in the rail industry.

Model Inputs We model failure scenario 3.1 for the system with and without the firewall between the station switch and RTU. Figure 3 shows the first input: a mal-activity diagram depicting how the scenario unfolds when the firwall is present. The "Firewall" swimlane and the activity steps within it are removed when there is no SCADA firewall in place. Figure 4 shows the mal-activity diagram for the second failure scenario.

The next step in the assessment process is modelling the system and devices. Figure 5 shows the system architecture after it has been modelled in the tool. By clicking on each device the user can specifiy which cyber securtiy controls (i.e., mitigations in failure scenario terminology) are present, and the degree to which they are effective (taking values within 0-1). The default value is 0.5.

An essential step in any cybersecurity risk assessment is understanding the potential threat actors. For critical infrastructure systems, *insiders* and *nation states* or advanced persistent threat actors are likely to be the top threats. A third threat actor that may be overlooked is 3rd party contractors or technicians who access certain systems (e.g., HVAC) for maintance. Table 2 summarizes the adversary properties.

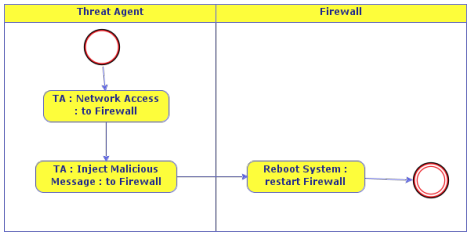


Fig. 4: Mal-Activity input for Scenario 3.2.

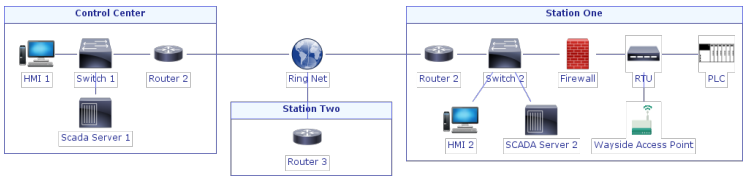


Fig. 5: Railway SCADA topology created in the tool.

Assessment Outputs We run the evaluation for scenario 3.1 under two system configurations: with and without the SCADA firewall between the station switch and RTU. Figure 6 shows the resulting graph for both assessments. Althought it is not easy to interpret the meaning of nodes and edges without the tool's GUI, the graph uses information about vulnerabilities and mitigations for the modelled devices to produce a system-level probability that represents the specified attacker's chance of causing the failure.

Table 3 lists the assessment results, i.e., the probability of the specified adversary reaching the failure state, for each scenario. For scenario 3.1, *compromised HMI sends malicious commands to devices* adding a SCADA firewall has a significant impact on the system security level, reducing the success probability from $16 - 35\%$ depending on the threat model. As expected, the Nation State adversary poses the largest threat, followed by insiders.

However, depending on the device, SCADA firewalls can introduce potentially serious vulnerabilities into the system [12]. In some cases, a denial of service attack on a firewall may be worse, operationally speaking, than an incorrect or malicious command to a device. The results from scenario 3.2 indicate that the threat actors that are of utmost concern for a rail operator (Nation State, Insider) have a significantly higher chance of causing an operational issue by exploiting a vulnerable firewall than they do of compromising an HMI and sending malicious commands (scenario 3.1). This is due to the small number of attack steps for scenario 3.2—there are few opportunities for mitigation. In this case, the operator may be better off hardening the HMI than introducing a SCADA firewall device. Ultimately, the onus is on system operators to carefully evaluate their security strategy and ensure that systems are implemented in a manner that achieves their goals. By systematically conceiving, documenting, and analyzing failure scenarios, operators can have greater confidence that their system will perform.

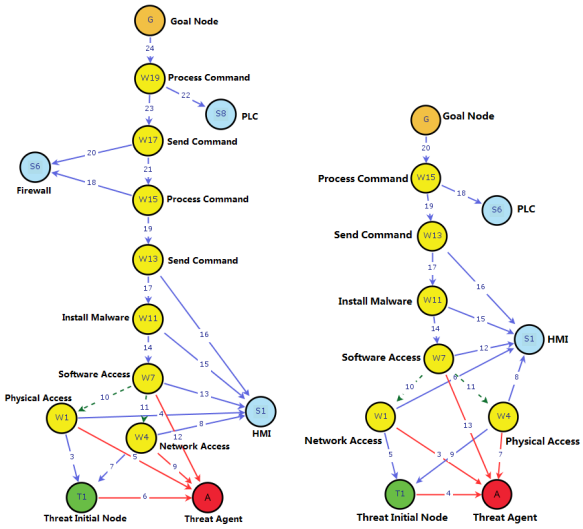
	Scenario 3.1			Scenario 3.2
Attacker	**Before Firewall**	**After Firewall**	**Improvement**	**After Firewall**
Insider	0.0119993	0.00953225	21%	0.387352
Contractor	0.00499653	0.00322911	35%	0.0177942
Nation State	0.015291	0.0128755	16%	0.573079

Table 3: Attacker success probability for failure scenarios 3.1 and 3.2

4.3 Discussion

The example failure scenarios and the case study presented above touch on only a small portion of the railway infrastructure. The large scope and interconnected nature of railways, spanning communications, power, control devices, and mechanical systems necessitates thorough and repeated risk assessment as the cyber threat landscape changes. Our team, as part of an ongoing project, has developed failure scenarios for certain railway subsystems, but we recognize the need for broader involvement from the rail industry and other research organizations to make this type of analysis more systematic and impactful in the industry.

While there is much to learn from the electric power grid failure scenario effort, there are several challenges that emerged. First and foremost, the original NESCOR scenarios are slanted toward physical impact, which is domain and often subsystem-specific. A consequence of this is that similar cyber failures may appear for different subsystems, but those failures may have very different impact. It is our belief that more work should be done to assess the impact of cyber failures in railway, particularly as they vary with time, commuter traffic, and geographic location. This is an area of future work for our project [7].



(a) With firewall (b) Without firewall

Fig. 6: Annotated graphs generated for failure scenario 3.1

5 Related Work

In recent years there have been several research projects focusing on security (physical or cyber) and safety for the rail industry [1, 5, 6]. Unfortunately the results and outcomes of many of those projects are not publicly available. One of those projects released a white paper [10] recommending, among other things, interoperability of risk assessment methodologies and creating a knowledge repository. Similarly, the American Public Transportation Association (APTA) recently published a series of recommended practice documents [11] for securing control and communication in transit environments. Those documents examine common features of transit systems, classify security zones, and suggest cyber risk assessment practices such as attack tree modeling. Our work shares the intent of the above efforts to elevate cyber security awareness within the industry, and suggests one possible approach for sharing knowledge and risk assessment practices that has been implemented in another industry.

From a research standpoint, there is a rich literature focusing on risk assessment frameworks, tools, and processes [22]. Techniques such as failure mode and effects analysis [18], hierarchical holographic modeling [17], HAZOP studies [26], and the CORAS method [15] are intended to support decision makers in the identification of potential risks from system failure or malicious activity. Ultimately, practitioners will decide which method, or combination of methods, best meets their needs. Perhaps the most similar work to our own analyzes the European Rail Traffic Management System (ERTMS) [14]. The authors refer to two confidential technical reports analyzing attack scenarios on this system. Their scenarios included some elements found in NESCOR-style failure scenarios, such as vulnerabilities exploited, potential mitigations, and impact. Our work advocates a broader adoption of this practice, and extends tool support for failure scenario analysis to the railway industry.

6 Conclusion

In this work, we demonstrate how the practice of failure scenario analysis can be readily adapted from the power grid sector and applied to railway infrastructure. Using a case study focusing on railway SCADA systems, we model two failure scenarios with a software tool and provide metrics that can help guide railway operators as they harden their systems. We then discuss opportunities for further enhancing and adapting failure scenario analysis to suit the railway domain.

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. It was also supported in part by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR).

References

1. ARGUS. www.secret-project.eu/IMG/pdf/20150128-02-uic-argus.pdf.
2. CyberSAGE portal. https://www.illinois.adsc.com.sg/cybersage/index.html.
3. Drools business rule management system. www.drools.org/.
4. Repository of industrial security incidents. www.risidata.com/Database.
5. Secured urban transportation project. www.secur-ed.eu/.
6. Security of railways against electromagnetic attacks. www.secret-project.eu/.
7. SecUTS: A Cyber-Phyiscal Approach to Securing Urban Transportation Systems. www.secuts.net.
8. Smart grid protection against cyber attacks. https://project-sparks.eu/.
9. Trustworthy cyber infrastructure for the power grid. https://tcipg.org/.
10. SECRET project white paper. www.secret-project.eu/IMG/pdf/white_paper_security_of_railway-against_em_attacks.pdf, Nov. 2015.
11. Apta security for transit systems standards program. http://www.apta.com/resources/standards/security/Pages/default.aspx, Jul. 2016.
12. Moxa EDR-G903 vulnerabilities. https://ics-cert.us-cert.gov/advisories/ICSA-16-042-01, May 2016.
13. UK rail cyber attacks. http://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/, Jul. 2016.
14. R. Bloomfield, R. Bloomfield, I. Gashi, and R. Stroud. How secure is ertms? *Proc. of SAFECOMP*, 2012.
15. F. den Braber, I. Hogganvik, M. Lund, K. Stølen, and F. Vraalsen. Model-based security analysis in seven stepsa guided tour to the coras method. *BT Technology Journal*, 25(1):101–117, 2007.
16. Electric Power Research Institute. Smart Grid Resource Center - NESCOR. http://smartgrid.epri.com/NESCOR.aspx.
17. Y. Y. Haimes, S. Kaplan, and J. H. Lambert. Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis*, 22(2):383–397, 2002.
18. IEC 60812. Analysis techniques for system reliability - procedure for failure mode and effects analysis (FMEA), 2006.
19. Industrial Control Systems Cyber Emergency Response Team. ICS-CERT Year in Review. https://ics-cert.us-cert.gov/Year-Review-2014.
20. S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol. Model-based cybersecurity assessment with nescor smart grid failure scenarios. In *Proc. of IEEE PRDC*, 2015.
21. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group (TWG) 1. Electric Sector Failure Scenarios and Impact Analyses, version 3.0, 2015.
22. A. Refsdal, B. Solhaug, and K. Stølen. *Cyber-risk Management*, pages 33–47. Springer International Publishing, Cham, 2015.
23. G. Sindre. Mal-activity diagrams for capturing attacks on business processes. In *Requirements Engineering: Foundation for Software Quality*. Springer Berlin Heidelberg, 2007.
24. K. Stouffer, J. Falco, and K. Scarfone. Guide to industrial control systems (ics) security. *NIST special publication 800-82*, 2011.
25. 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 QEST*, 2014.
26. R. Winther, O.-A. Johnsen, and B. A. Gran. Security assessments of safety critical systems using hazops. In *Proc. of SAFECOMP*, 2001.