Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_S13-03-586-cd

A cybersecurity approach for improved system resilience

Ravdeep Kour

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: ravdeep.kour@ltu.se

Amit Patwardhan

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: amit.patwardhan @ltu.se

Ramin Karim

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: ramin.karim@ltu.se

Pierre Dersin

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: pierre.dersin @ltu.se

Jaya Kumari

Division of Operation and Maintenance Engineering, Luleå University of Technology, Sweden.
E-mail: jaya.kumari@ltu.se

The ongoing digitalisation of industrial systems is bringing new challenges in managing, monitoring, and predicting the overall reliability performance. The overall reliability of a cyber-physical system, such as railways, is highly influenced by the level of resilience in its inherent digital items. The objective of this paper is to propose a systematic approach, based on an enhanced Cyber Kill Chain model, to improve the overall system resilience through monitoring and prediction. The proposed cybersecurity approach can be used to assess the future cyberattack penetration probabilities based on the present security controls. With the advancement in cybersecurity defensive controls, cyberattacks have continued to evolve through the exploitation of vulnerabilities within the cyber-physical systems. Assuming the possibility of a cyberattack it is necessary to select appropriate security controls so that this attack can be predicted, prevented, or detected before any catastrophic consequences to retain the resilience of the system. Insufficient cybersecurity in the context of cyber-physical systems, such as railways, might have a fatal effect on the whole system availability performance and sometimes may lead to safety risks. However, to improve the overall resilience of a cyber-physical system there is a need of a systematic approach to continuously monitor, predict, and manage the health of the system's digital items with respect to security. Furthermore, the paper will provide a case-study description in railway sector, which has been used for the verification of the proposed approach.

Keywords: Railway, Cybersecurity, Cyber Kill Chain, System Resilience.

1. Introduction

Railway systems are complex technical systems and one of the critical elements of a modern economy. On the one hand, digitalisation is changing operation and maintenance of railways significantly with respect to sustainability, availability, reliability, maintainability, capacity, safety, and security including cybersecurity. On the other hand, railway stakeholders see these changes as a challenge. Digitalisation challenges include data acquisition, transformation, processing, modelling, visualisation, safety, quality, security, and information assurance (Jägare, Karim et al., 2019). Information Assurance (IA) defines and applies "a collection of policies, standards, methodologies, services, and mechanisms to maintain mission integrity with respect to people, process, technology,

information, and supporting infrastructure" (Willett, 2008). The concept of IA also deals with aspects of cybersecurity, which is a subset of IA and is receiving significant attention with digitalisation. Cybersecurity is considered as preservation of confidentiality, integrity, and availability of information in cyberspace (ISO/IEC 27032, 2012). The overall goal of IA is to ensure the availability of the system. Dependability includes availability, reliability, maintainability, and maintenance supportability (IEC, 2015). Therefore, improved IA will have a positive impact on the overall dependability of the system.

With the adoption of ICT, the number of networked devices is rapidly increasing. The use of internet-connected sensors and devices can provide timely and accurate information about the physical world. The collected data can be integrated within the cloud computing infrastructures and enable maintenance strategies, such as predictive maintenance or Condition-Based Maintenance (CBM) (Kour et al., 2014). CBM is a strategy that warns future failures based on the condition of an asset and one can perform maintenance actions for the defective elements only (Ahmad, 2012). However, these innovative developments are not without risks. The networked devices can provide opportunities for adversaries/attackers to steal, corrupt, delete, or modify data, which can have negative effects on the physical systems.

Cyberattacks on eMaintenance solutions may have an impact on underlying data, which, in turn, will influence the data-driven model and affect its availability and, therefore, degrade System Resilience (SR).

Vugrin et al. (2010) have defined SR as: "given the occurrence of a particular disruptive event (or set of events), the resilience of a system to that event (or events) is that system's ability to reduce efficiently both the magnitude and duration of deviation from targeted system performance levels.".

According to National Academy of Science (NAS) and NIST SP 800-160, V2, resilience is "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events".

Figure 1 shows resilience curve adapted from the work of Haque et al. (2021) and Wei & Ji (2010).

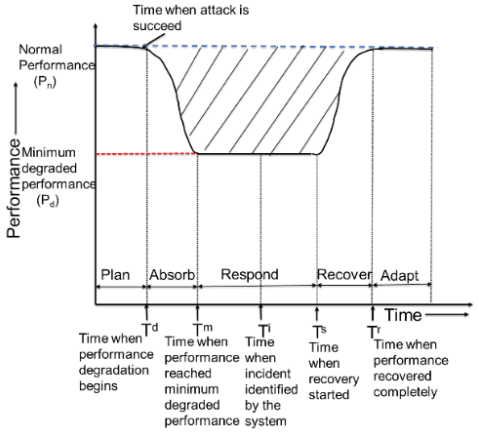

Fig 1. Resilience curve with different phases of action (adapted from Haque et al., 2021 and Wei & Ji 2010)

The resilience curve consists of different phases of cyber operations as a function of system performance over time during a cyberattack incident (Haque, 2021). The five stages shown in Figure 1 complete the resilience cycle, and the area under the curve is the quantitative measure of the system's cyber resilience (Haque, 2021). This quantitative measure will help in assessing & evaluating weak areas and developing mitigating strategies (Haque, 2021). This approach is also called a functionality-based approach (Bellini et al., 2021). Haque (2021) has proposed resilience metrics for ICS systems. These are:

$$Degrading\ time = Tm - Td;$$

$$Attack\ Identification\ time = Ti - Td;$$

$$Recovery\ time = Tr - Ts;$$

$$Performance\ degradation = Pn - Pd;$$

$$Performance\ loss = Pn\ x\ (Tr - Td) - \int_{Td}^{Tr} P(t)$$

$$Total\ loss = f(Performance\ loss, recovery\ cost, asset\ damage)$$

According to Jackson (2009), there are three phases of resilience, which are viewed as occurring before, during, and after disruption.:

(a) Avoidance: Pre-disruption phase which includes preventive aspects of SR in response to a disruption.
(b) Survival: Loss of capability during disruption
(c) Recovery: Recovery of capability after disruption

According to Bodeau (2011) and Madni & Jackson (2008), there are four goals of resilience: these are anticipate, withstand/absorb, recover, and evolve. All the above-mentioned concepts, phases, and goals of resilience are the same but are used by different researchers. These concepts and goals have also been defined within Railway Defender Kill Chain Matrix (RDKC) to enable proactive cybersecurity (Kour 2020) using Cyber Kill Chain (CKC) model (Lockheed Martin 2009).

The main aim of this research paper is to propose a cybersecurity approach for improving the SR by predicting and monitoring cyberattack penetration probabilities at each stage of the CKC model. The outline of the paper is as follows. After introduction, it defines seven stages of the CKC model; followed by the state-of-art of the currently used simulators in cybersecurity. Then, it presents a research methodology.

Finally, case study and results are presented followed by conclusions and future research directions.

2. Cyber Kill Chain (CKC) Model

An initial CKC model was developed by Lockheed Martin (2009) to trace the stages of a cyberattack within the corporate network. The CKC is one of the most widely used frameworks to detect cyberattacks based on the kill chain tactic of the US military's F2T2EA (find, fix, track, target, engage and assess) (Lockheed Martin 2009). The seven stages of the CKC model which shows attacker's steps to infiltrate the target system are:

(i) Reconnaissance (R): The first stage of the model, one of the most difficult stages to detect from a security monitoring perspective, is the planning stage of the cyberattack. The adversary searches for and gathers information about the target organization. The collected information is useful in the later stages to deliver malicious code to the target system.

(ii) Weaponize (W): In this stage attacker develops a malicious code to be sent to the targeted system.

(iii) Delivery (D): The third stage of the model is the operation launch stage where the malicious weapon is transmitted to the targeted environment.

(iv) Exploitation (E): At this stage, exploitation is triggered to silently install/execute the delivered malicious code.

(v) Installation (I): This stage involves the installation of malicious code and the maintenance of persistence inside the targeted environment.

(vi) Command & Control (C2): In this stage adversary tries to open a two-way communication channel to enable the attacker to control the targeted environment remotely. Once the C2 channel is established, the adversary has "hands on the keyboard" access inside the targeted environment.

(vii) Act on Objective (AO): In the last stage of the model, the adversary achieves the desired attack goals. These goals can be a loss of confidentiality, integrity, or availability of the assets.

3. State-of-the-Art of Currently used Simulators in railway for Cybersecurity

There are various simulators (both proprietary and open), such as Optimized Network Engineering Tools (OPNET 2019) and Network simulator (NS-3 2019) to analyze the impact of cyberattacks on the modeled networks. Researchers are active in simulating cyberattacks in critical infrastructures, using Network simulator NS2 to predict the impact of Denial of Service (DoS), malware propagation, and Man-in-The-Middle attacks on Supervisory Control and Data Acquisition (SCADA) Systems (Ciancamerla, Minichino et al. 2013). In addition, an agent-based modeling and simulation approach has been used by researchers to facilitate the assessment of critical infrastructure entities under cyberattack (Rybnicek, Tjoa et al. 2014).

Researchers are also active in game theory to model the behaviors of complex multistage cyberattacks. Intelligent Transportation Systems (ITS) have developed game-theory models to secure against the fatal cyberattacks (Alpcan, Buchegger 2010, Sedjelmaci, Senouci et al. 2016, Mejri, Achir et al. 2016, Bahamou, Ouadghiri et al. 2016, Sanjab, Saad et al. 2017). In addition to this, a combined simulation of interconnected railway network, ICT network and energy grid (using OpenTrack, SINCAL, and NS3 respectively) has been achieved in European Union Project (Ciprnet 2013).

A review of existing railway simulators shows that most of them were designed for planning and operational purposes (Grube, Nunez et al. 2011, Yao, Zhao et al. 2013, OpenTrack 1990, OpenPowerNet Version, 1. 8. 1 2019, eTrax 2016). The limitations of these simulators are that they fail to support cyberattack analysis and are very costly to adopt in railway cybersecurity research.

To overcome these limitations, another simulator, called SecureRails, was introduced; an open-source simulator for analyzing cyber-physical attacks in railway (Teo, Tran et al. 2016). This simulator is restricted to only two subsystems: the mechanical system (involving the train's motion) and the electrical system (traction power system).

In addition to this, literature does not provide simulation tools to predict cyberattack penetration probabilities in multiple stages of a cyberattack. Thus, this research provides a Cybersecurity Demonstrator (CD) to simulate cyberattack penetration probabilities at each stage of the CKC model.

4. Research Methodology

Within this research we have conducted a case study within railway. A cybersecurity approach for SR has been proposed in the form of CD. This CD has been developed by using .NET technology. This CD is based on the RDKC matrix which is a part of cybersecurity framework in railway (Kour, 2020).

The research starts with defining probabilities for the initiation of a cyberattack within the system. Afterwards, probabilities for the security controls at each stage of the CKC model have been estimated. This data has been provided by railway expert advice and their experiences of using various SCs as well as from literature review. The participating railway personnel included infrastructure owners, railway system architect, information and operational security staff and high-level managers.

Next step of the research methodology is data analysis to predict cyberattack penetration probabilities at each stage of the CKC model and compare them with the present system. The calculation of the penetration probabilities is based on a predictive model for multistage cyber-attack simulation (Kour et al., 2020). Next, cyberattack penetration probabilities have been visualized and important decisions can be taken to minimize the risk of future cyberattacks.

5. Description of Case study and Results

A Railway is a complex system-of-systems with its inherently distributed and networked nature with long lifetime of its sub-systems and components. It is interconnected with, and closely dependent on, other infrastructures. Therefore, cyberattack on any one of the infrastructures, such as ICT, electrification, or signalling, will have a cascading effect on the physical infrastructures (Kour, 2020). For example, in one of the past incidents, an "electronics genius", 14-year-old boy from Poland hacked a tramway system and derailed a tram, which then collided with a tram coming in the opposite direction causing injuries to 12 people (Baker, 2008). Hackers have targeted rail companies in UK, Germany, US, Poland, South Korea, Denmark, and Sweden (Kour 2020).

These cyberattacks led to a threat to people safety, system failures, reputational damage of the organizations, monetary loss, data inaccuracy, loss of reliability, availability, maintainability, and safety (RAMS) and hence, a threat to dependability of the system. Therefore, it is very important that the railway should adopt advanced security measures to preserve its resilience from unexpected cyber threats.

The railway organizations must move towards Predictive Security Analytics (PSA) to quickly predict and prevent cyberattacks (Hoek 2017). PSA cannot predict the attack itself, but its early indicators can be identified to statistically predict potential future cyber threats.

The case study presents a cybersecurity approach which is based on quantitative assessment for SR in the form of a Cybersecurity Demonstrator (CD) for railways. Railway infrastructure owners participated in this case study. Other railway staff includes railway system architect, information and operational security staff and high-level managers.

The CD is available online in the form of a web application and is developed by using .NET technology. Following are the main components of this demonstrator:

5.1. Cyberattack probability

It is the probability of initiation of cyberattack. Its value is typed between 0 and 1 in the given text box in CD.

5.2. Security control (SC) probability

Pc_1-Pc_7 is the probability of SC at each stage of the CKC model (Figure 2 (a)). These SCs include Intrusion Detection and Prevention System, Honeypot, Data Diode, Web Analytics, Threat Intelligence, Video Surveillance, Vulnerability Scanning, Penetration Testing, Firewall, Proxy Filter, Anti-virus, etc.

Pci is the probability of SC at stage S_i of CKC, $i = 1,2,\ldots,7$.

$P\eta_i$ is the probability of penetration at stage S_i, $i = 1,2,\ldots,7$.

Function $f(Pci, P\eta i)$ calculates the probability of propagation of cyberattack to next stage of CKC with $i = 1,2,\ldots,7$.

5.3. Resilience and CKC Model

As discussed by Haque et al. (2021) and Wei & Ji (2010), resilience curve consists of different phases of actions as shown in figure 2 (b). This resilience curve can have 3 stages of recovery: full recovery stage where the system performance will be same as required or initial performance; partial recovery stage where the system performance will be less than required; and no recovery stage where the system performance remains degraded.

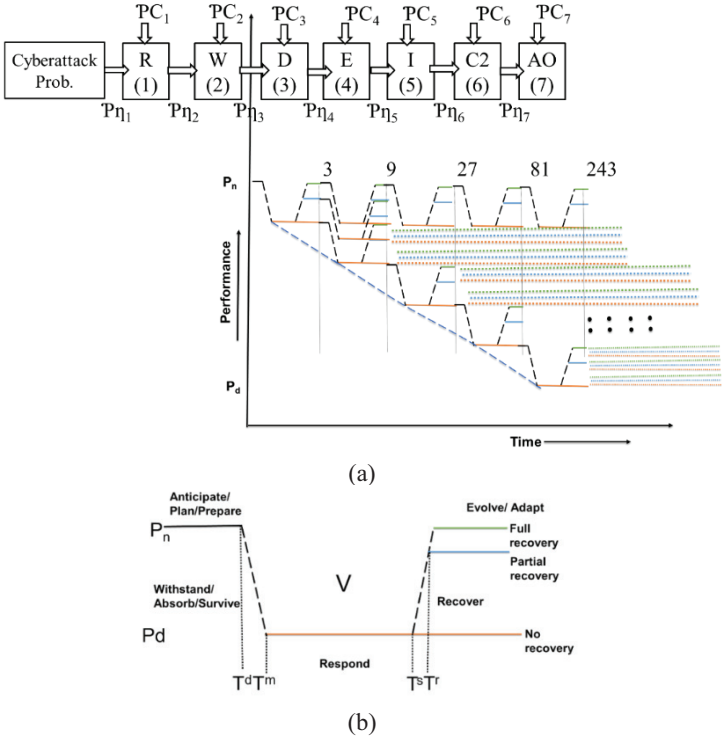

Fig.2 (a) Resilience curve within each stage of the CKC model with (b) 3 stages of recovery.

With these recovery stages, the system performance will be accumulated to the next stage of CKC. Therefore, there can be a total of 243 (3^5) resilience curves drawn from stage 3 to stage 7.

The two dashed lines of resilience curves (Figure 2 (b)) show that there can be changes in the probabilities of performance and recovery process. By using appropriate SCs at each stage of the CKC the resilience can be improved.

In this paper we are proposing an approach that will include all these phases at each stage of CKC starting with stage 3 where actual cyberattack happens with the delivery of malicious code. If system has some vulnerability that attacker can exploit, then performance will continue to degrade in the next stages. Within our approach we are providing various SCs at each stage to break the chain and recover and adapt to the required performance.

If attack propagates to the next level, then SCs at that level will help the system to recover and adapt to the required performance and cycle repeats for all the seven stages. This cybersecurity approach will help to enhance the resilience of the full system in small steps.

The V "Exploitation of Vulnerability" part of curves shows loss of performance which can be calculated as the area of a trapezoid with the assumed shape, i.e.,

$$Performance\ loss = [(Ts - Tm) + (Tr - Td)] * [(Pn - Pd)]/2$$

$$Total\ loss = f(Performance\ loss, cost\ of\ SCs, asset\ damage)$$

Whenever, there exists some vulnerability at any stage, the system will start degrading and following the curve defined by Haque et al. (2021) and Wei & Ji (2010). Our proposed approach will suggest SCs at that level so that it will start recovering and adapting to the required performance. The selection of SC can be performed through Cybersecurity Demonstrator using RDKC which is a part of cybersecurity framework in railway (Kour, 2020).

5.4. Cybersecurity Demonstrator (CD)

All the SCs used within the proposed CD are based upon predictive, proactive, active, and reactive strategies based on RDKC matrix (Kour, 2020) as shown in figure 3.

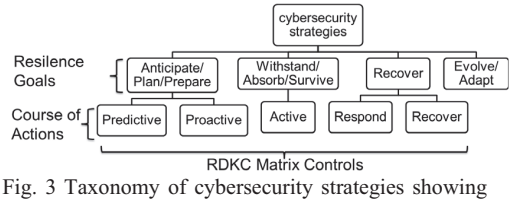

Fig. 3 Taxonomy of cybersecurity strategies showing connection of resilience (Bodeau, 2011; Madni & Jackson, 2008) with RDKC matrix (Kour, 2020).

The proposed taxonomy of cybersecurity strategies acts like a quick reference guide to mitigate cyber threats. This quick reference guide can help the railways to act proactively to implement the right security strategy to improve SR. The course of actions is grouped into four strategies: predictive, proactive, active, and reactive (Respond and Recover).

• A **predictive strategy** can detect anomalies in traffic flow and data, sounding an alert for a security threat before its occurrence. It includes the ability to escape adversarial situations using security solutions like user behaviour analytics, pattern log, machine learning, AI and self-learning, and self-healing.

• A **proactive** strategy begins with the detection of threats before their occurrence. This involves the use of threat intelligence to proactively identify high risk and weak areas.

• An **active** strategy involves the gathering of intelligence to thwart cyberattacks based on experience, knowledge, and internal and external real-time information.

• A **reactive** strategy begins with the occurrence of an incident. It involves the initiation of an incident response plan, an operations continuity plan, and a disaster recovery plan to respond to, and recover from, breaches, along with forensics for legal evidence.

The proposed CD (available at: http://emaint-cbap.azurewebsites.net/Default will predict cyberattack penetration probabilities based on the initial probability of cyberattack and probabilities of SCs at each stage of the CKC model based on research work from (Kour et al., 2020). It will compare the existing system with the predicted based on the SCs.

The defined cybersecurity strategies or SCs are the part of RDKC matrix (Kour, 2020) which are provided in the dropdown boxes, and we can select one SC at each stage of the CKC model. Figure 4 shows option to fill and select the probability of cyberattack and SCs respectively. The initial idea of the proposed CD is to select, analyse, and display information in the form of two curves in a chart. One curve is for the existing system and the other curve is for the predicted system when we enhance SCs at each level of the CKC model.

Data in the demonstrator have been assumed based on expert advice and their experiences of using various SCs. This will help in predicting future cyberattack penetrations based on real cybersecurity data within specific industry. This CD is an initial idea and is under construction. The future directions of this demonstrator are provided in the Future Work section of this paper (Section 6).

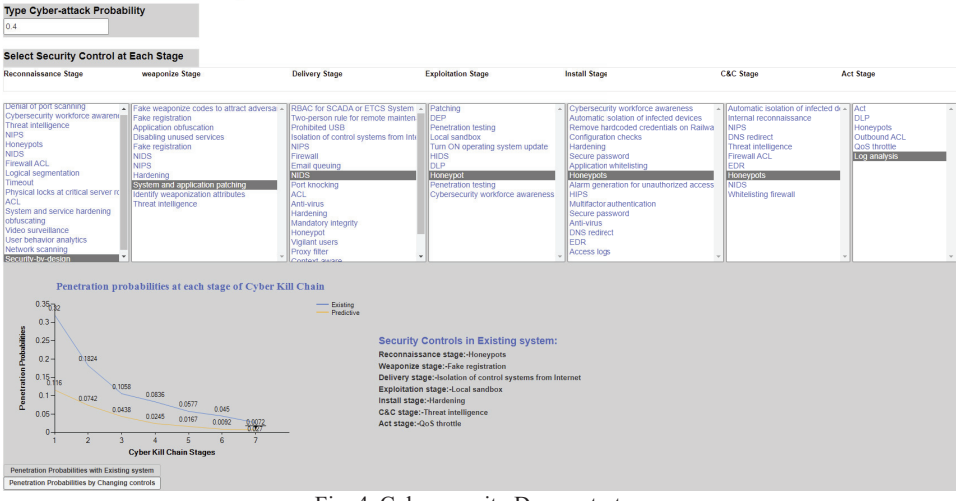

Fig. 4. Cybersecurity Demonstrator

6. Conclusions and Future Work

This paper provides a cybersecurity approach to enhance the SR towards cyberattacks. It has been concluded that with enhanced SCs we can improve the propagation effect of a cyberattack at various stages of CKC model. The proposed CD in the form of a simulator for the digitalised railway helps to enable predictive security. The demonstrator is aimed to enhance the railway's cybersecurity maturity level and to effectively predict and prevent cyberattacks. In future, the CD will incorporate real cybersecurity data, type of cyberattack, cost for each of the SC, performance degradation, and also will include self-learning and self-healing system.

Acknowledgments

The authors would like to thank Luleå Railway Research Center (JVTC) for sponsoring this research work.

References

Ahmad, R. and Kamaruddin, S., 2012. A review of condition-based maintenance decision-making. European journal of industrial engineering, 6(5), pp. 519-541.

Alpcan, T. and Buchegger, S., 2010. Security games for vehicular networks. IEEE Transactions on Mobile Computing, 10(2), pp. 280-290.

Bahamou, S., Ouadghiri, E., Driss, M. and Bonnin, J., 2016When Game Theory Meets VANET's Security and Privacy, Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media 2016, ACM, pp. 292-297.

Baker, G. 2008. Schoolboy hacks into city's tram system. The Telegraph, 11, 2008. 8.

BBC NEWS, 2020-last update, Rail station wi-fi provider exposed traveller data. Available: https://www.bbc.com/news/technology.

Bellini, E., Marrone, S., & Marulli, F. (2021). Cyber Resilience Meta-Modelling: The Railway Communication Case Study. Electronics, 10(5), 583.

Bodeau, D. J., Graubart, R., Picciotto, J., & McQuaid, R. 2011. Cyber resiliency engineering framework. MITRE Corp Bedford MA.

Cho, S., Han, I., Jeong, H., Kim, J., Koo, S., OH, H. and Park, M., 2018Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture, 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) 2018, IEEE, pp. 1-8.

Ciancamerla, E., Minichino, M. and Palmieri, S., 2013Modeling cyber attacks on a critical infrastructure scenario, IISA 2013 2013, IEEE, pp. 1-6.

CIPRNET, 2013-last update, Critical infrastructures preparedness and resilience research network. EU project. Available: https://www.ciprnet.eu/home.html.

ETRAX, 2016-last update, Railway Traction Power Analysis | Rail Power System Software. Available: https://etap.com/solutions/railways.

EUROPA, E.L., 2018-last update, EUR-Lex - 32016R0679 - EN - EUR-Lex. Available:

https://eur-lex.europa.eu/eli/reg/2016/679/oj [Jul 29, 2020].

Grube, P., Nunez, F. and Cipriano, A., 2011. An event-driven simulator for multi-line metro systems and its application to Santiago de Chile metropolitan rail network. Simulation Modelling Practice and Theory, 19(1), pp. 393-405.

Haque, M. A., Shetty, S., Gold, K., & Krishnappa, B. (2021). Realizing cyber-physical systems resilience frameworks and security practices. In Security in cyber-physical systems (pp. 1-37). Springer, Cham.

Hoek, S., 2017. Predictive security analytics.

IEC, 2015. International electrotechnical vocabulary—Part 192: Dependability. International standard IEC, , pp. 60050-60192.

ISO/IEC 27032, 2012. ISO/IEC 27032: 2012–Information technology—Security techniques—Guidelines for cybersecurity.

Jackson, S. 2009. Architecting resilient systems: Accident avoidance and survival and recovery from disruptions (Vol. 66). John Wiley & Sons.

Jägare, V., Karim, R., Söderholm, P., Larsson-Kråik, P. and Juntti, U., 2019Change management in digitalised operation and maintenance of railway, International Heavy Haul Association (IHHA) STS 2019 Conference 2019, pp. 904-911.

Kour, R., Thaduri, A., & Karim, R. 2020. Predictive model for multistage cyber-attack simulation. International Journal of System Assurance Engineering and Management, 11(3), 600-613.

Kour, R., 2020. Cybersecurity in Railway: A Framework for Improvement of Digital Asset Security, Luleå University of Technology. (PhD dissertation).

Kour, R., Thaduri, A., & Karim, R. 2021. Operational Security in the Railway-The Challenge. In International Congress and Workshop on Industrial AI (pp. 266-277). Springer, Cham.

Lockheed Martin. 2009. Cyber Kill Chain®.

Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. IEEE Systems Journal, 3(2), 181-191.

Mejri, M.N., Achir, N. and Hamdi, M., 2016A new security games based reaction algorithm against DOS attacks in VANETs, 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2016, IEEE, pp. 837-840.

NS-3, 2019-last update, Network Simulator. Available: https://www.nsnam.org/ [Jun 26, 2019].

OPENPOWERNET VERSION, 1. 8. 1, 2019-last update, Traction power supply and train performance simulation software. Available: http://www.openpowernet.com/.

OPENTRACK, 1990-last update, Simulation of Railway Networks. Available: http://www.opentrack.ch/opentrack/opentrack_e/opentrack_e.html.

OPNET, 2019-last update, OPNET IS NOW PART OF RIVERBED STEELCENTRAL™. Available: https://www.riverbed.com/se/products/steelcentral/opnet.html [Jun 26, 2019].

Rybnicek, M., Tjoa, S. and Poisel, R., 2014Simulation-based cyber-attack assessment of critical infrastructures, Workshop on Enterprise and Organizational Modeling and Simulation 2014, Springer, pp. 135-150.

Sanjab, A., Saad, W. and Başar, T., 2017Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game, 2017 IEEE International Conference on Communications (ICC) 2017, IEEE, pp. 1-6.

Sedjelmaci, H., Senouci, S.M. and Ansari, N., 2016. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology. IEEE Transactions on Intelligent Transportation Systems, 18(5), pp. 1143-1153.

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

The National Academy of Sciences. 2012. Disaster Resilience: A National Imperative

Vugrin, E. D., Warren, D. E., Ehlen, M. A., & Camphouse, R. C. (2010). A framework for assessing the resilience of infrastructure and economic systems. In Sustainable and resilient critical infrastructure systems (pp. 77-116). Springer, Berlin, Heidelberg.

Wei, D., & Ji, K. (2010, August). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. In 2010 3rd international symposium on resilient control systems (pp. 15-22). IEEE.

Willett, K.D., 2008. Information assurance architecture. CRC Press.

Yao, X., Zhao, P. and Qiao, K., 2013. Simulation and evaluation of urban rail transit network based on multi-agent approach. Journal of Industrial Engineering and Management (JIEM), 6(1), pp. 367-379.

Kour, R., Tretten, P., & Karim, R. (2014). eMaintenance solution through online data analysis for railway maintenance decision-making. Journal of Quality in Maintenance Engineering.

NIST SP 800-160, Volume 2 Revision 1 (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. In National Institute of Standards and Technology (US).