Methodology for resilience assessment for rail infrastructure considering cyber-physical threats

Corinna Köpke[1], Johannes Walter[1], Eros Cazzato[2], Catalin Linguraru[2], Uli Siebold[2], and Alexander Stolz[3]

[1] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Am Klingelberg 1, 79588 Efringen-Kirchen, Germany.
Corinna.Koepke@emi.fraunhofer.de
[2] CuriX AG, Zugerstrasse 76B, CH-6340 Baar, Switzerland.
eros.cazzato@curix.ai
[3] Albert-Ludwigs-Universität Freiburg, Emmy-Noether-Straße 2, 79110 Freiburg im Breisgau, Germany. alexander.stolz@mail.inatech.uni-freiburg.de

Abstract. In the EU project SAFETY4RAILS, the project partners developed a collaborative toolkit that is able to assess and eventually improve the resilience of rail and metro transportation and its infrastructure against various cyber, physical and combined cyber-physical threat. In general, to improve a property of a system such as resilience, it is necessary to assess that property first. Therefore, in this paper, we focus on the aspect of assessing the resilience by the synergistic collaboration of two tools out of this toolkit: CuriX, which is a tool for monitoring and detecting abnormal behaviour of infrastructure in the presence of threats, and CaESAR, which can asses propagation of performance losses over distributed systems that reflects its resilience. We showcase a resilience assessment for an exemplary scenario of combined cyber-physical threats which is applied to a metro system. In this assessment, the main functionalities and results of both tools as well as their combined usage will be described to demonstrate how their collaboration can contribute to an improved resilience assessment.

Keywords: Resilience · Cyber-physical threats · Detection · Impact propagation.

1 Introduction

Resilience is the ability of a system to withstand certain crisis events. Typically, the life cycle of the system including crisis events is formulated in a resilience cycle that includes time before, during and after the crisis (see e.g. [5], [22] and [9]). The monitoring and quantification of resilient behavior can be performed e.g. by the nine-step resilience management process [10], which is an adaptation of the ISO 31000:2018 [11]. Especially in the cyber domain, certain resilience phases are defined, namely 'identify', 'protect', 'detect', 'respond' and 'recover' [19].

The quantification of resilience gets especially challenging when crisis events happen simultaneously and the system under consideration represents an interconnected critical infrastructure. A prominent example is a public transport network including different types of transportation modes which is the focus of this paper.

In rail operation, an increasing, number of disruptions have happened over the last years with an increasing total duration [1]. As the problem has grown in importance, also the scientific output on rail infrastructure resilience has increased. For example, different sources for disruptions in rail operations of the New Haven Line NYC such as electricity outages and unavailability of cars and ways to increase the system's resilience by taking appropriate actions, is discussed in [4]. The focus of most of the works is on quantifying the resilience using different means such as data-driven, topological, simulation and optimization approaches [1]. One example for a topology based analysis is the resilience assessment of London's metro system [3]. By analyzing the graph structure of the metro grid, the authors were able to identify critical edges and unexpected dependencies in the network.

In the EU project SAFETY4RAILS, a toolkit is developed to monitor rail infrastructure before, during and after a crisis and in each resilience phase to provide decision support (see e.g. [18]). Various risks for the infrastructure are considered and discussed based on the threat taxonomy presented by the European Union Agency for Cybersecurity (ENISA) [6].

One of the tools brought to SAFETY4RAILS is CuriX (Cure Infrastructure in XaaS), a software solution that follows a general approach to holistically monitor technical systems (albeit with a focus on IT infrastructure). CuriX gathers and analyses provided key performance indicators as time series data and log files to detect abnormal behaviour to either warn from upcoming threats or to alert current issues from threats. Another tool brought to SAFETY4RAILS is CaESAR (Cascading Effect Simulation in Urban Areas to Assess and Increase Resilience) which is designed to predict cascades in connected infrastructure systems. To this end, different simulation techniques are employed to represent the propagation of impact in infrastructure networks. The coupling of a network model and an Agent-Based Model (ABM) (see e.g. [15], [13] and [14]) is here further explored and applied to metro and rail networks in Ankara. For the full list of all the tools brought into the project and the overall architecture of the toolkit, we refer to reference [20].

Given the capabilities of the two tools, we aim to showcase a resilience assessment conducted by CaESAR following a threat which impacts a certain infrastructure and is detected previously by CuriX. We investigate a scenario in which the aim of an attack is to physically access the premises to cut the electricity supply to all the systems in the station, leaving it fully inoperable. In this scenario, the power supply system with the connected Supervisory Control and Data Acquisition (SCADA) system, responsible for controlling the electric power and its distribution to the station, is impacted and leads to a power outage. Two variants of the power outage scenario are considered. In one variant,

CuriX detects the physical access by monitoring, for instance, door sensors protecting the SCADA system and manages to warn the system manager ahead of the power outage, which gives the system manager the chance to act ahead of the power outage and to therefore reduce the chance of propagating the impact. In the other variant, the power outage happens abruptly (which CuriX manages to detect but without pre-warning) and the loss of power is unavoidable and immediate.

In the context of this scenario, we assess the impact when considering detecting and recovering capabilities for a single station in a first step and how this affects the passenger flows in surrounding stations in a second step. The structure of the paper is as follows: First, in section 2 a station asset network is modeled and the topology is presented. In section 3 the methodology for threat detection in the station is outlined. A resilience assessment for the station is performed in section 4 considering varying conditions. Further, in section 5 the impact on the single station is propagated in a larger public transportation grid. Finally, in section 6 the findings are summarized and an outlook is provided.

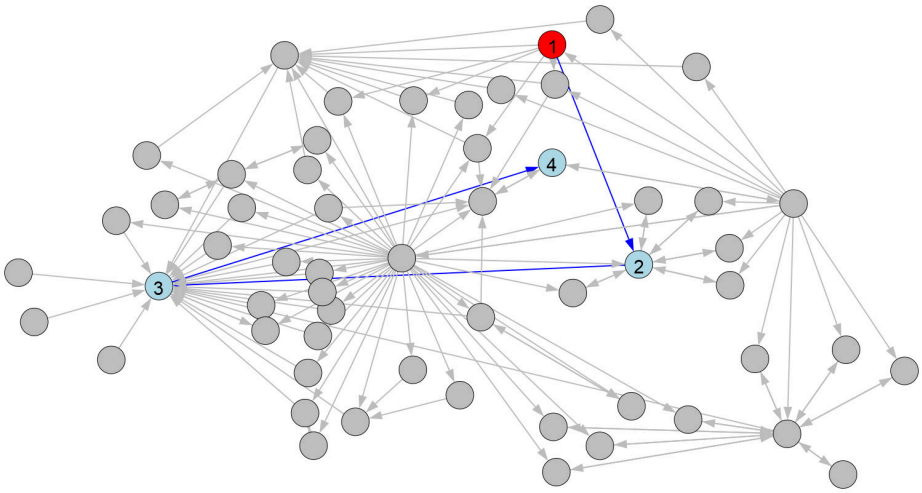


Fig. 1. Network topology for a single station. A scenario is highlighted with an initial impact on the SCADA (1), then equipment for electricity supply is manipulated (2), the functionality of the station is reduced (3) and finally the trains are impacted (4).

2 Metro station model

Each train or metro station is composed of assets that are essential for the function it needs to fulfill. These assets can be computers, signaling, tracks, electricity supply but also employees and passengers. All these assets are interrelated and

either exchange e.g. information or they impact each other in case of a failure. Based on this assumption, an asset topology model is established. Note, as this information is critical only an anonymised asset network is presented in this work.

The topology model consists of assets as nodes and relations as edges. Nodes have certain properties such as an identifier, a name, a system they belong to and a list of nodes which they impact. This model enables to identify critical assets based e.g. on centrality measurements. Further, the shortest path between nodes can reveal attack or damage paths and thus the network structure enables to model cascading effects in the system. A similar approach has been presented for airport infrastructure in [15].

The network topology given in Fig. 1 consists of different systems. Typically, those would be highlighted in different colors but for confidentiality reasons they are colored grey. Once a threat is detected, the paths in the network from the entry point to vulnerable assets such as trains and passengers can be computed using the shortest path. The detection is described in section 3. Further analysis of the asset topology model, cascading effects and resilience assessment is given in section 4.

3 Threat detection

There are various detection and monitoring system types to protect assets from cyber threats. A few of them are mentioned in reference [12]:

- intrusion detection and prevention systems for the IT network;
- endpoint detection and response for end devices;
- Security Information and Event Management systems to analyse and detect attacks on the IT infrastructure by analysing collected log and event data from devices, and applications;
- and also observability tools to monitor the infrastructure from rather an operational aspect.

While many of these systems employ threshold detection and pattern matching methods to known signatures, most of these systems are also capable of employing anomaly detection methods which do not require known signatures [12]. Methods based on anomaly detection can derive insights from the behaviour of systems without the need of known signatures. In addition, these methods are applicable to heterogeneous systems and are suited for both cyber and physical threat detection such as discussed in, e.g., [2, 16, 17]. Anomaly detection methods can provide additional capabilities, e.g., to detect up to then unknown threats. CuriX is one of those tools aiming at the detection of known and unknown threats in a variety of infrastructures and therefore makes use of anomaly detection methods. CuriX employs statistical and machine learning-based techniques on time series data and log files to perform anomaly detection. Examples of the used the techniques can be found in [21, 7]. CuriX creates a model of normal system behaviour from the data, i.e. the regular behaviour of the system when

used in its daily operation, and compares it to the observed behaviour. When the observed behaviour differs significantly from the created model of normal system behaviour, an anomaly is identified, i.e. abnormal behaviour. Since not every anomaly indicates a problematic state of the system which could be due to the impact of a manifested threat, CuriX provides the possibility to define customisable criteria for critical anomalies.

Given the scenario of a physical intrusion with the intention of cutting the electricity supply in the station by manipulating the SCADA system responsible for electrical power in the station, which is outlined in the introduction, we define gaining physical access to the SCADA system's room as a precondition for the intruders. Considering an intelligent access system for the room, where the access is being granted and logged based on an employee card or password entry, CuriX might be able to identify and detect any abnormal access to the SCADA system's room by monitoring the access data from the specific door. However, in the case that intruders study the behaviour such as the usual entering/leaving times to the server room and decide to act within those time frames, finding abnormal behaviour is more challenging for CuriX. Therefore, CuriX would benefit from additional data than just the entering/leaving times, for instance, by adding which persons are entering and leaving at which times.

In the first variant of this scenario, we assume that a potential intrusion to the SCADA system's room is detected by CruiX ahead of the power outage. In this variant, security personnel has the chance to take measures to prevent or system managers the chance to mitigate the impact of a power outage. CaESAR exploits this detection by conducting a resilience assessment to simulate the potential consequences of a power outage on the train and metro network. So far, we considered that CuriX is able to detect the physical intrusion as part of the kill chain, however we could also consider other parts of a possible kill chain that would lead to the same scenario outcome, for instance, cyber related events such as port scanning for reconnaissance activities or brute force attack for privilege escalation with the intention to perform a cyber attack on the SCADA system instead. In such cases, CuriX would then rather analyse the systems log files for abnormal requests in the login attempts as an example.

In the second variant of the scenario, intruders have gained physical access to the SCADA system controlling the power supply of the station without any prior detection from CuriX or any other detection system. They manipulate the SCADA system to cut the electricity supply. The consequence is the loss of availability of electrical power within the station, which could, for instance, be identified from the station's electric power consumption data or the power supply's voltage or current. We show CuriX' identification of an anomaly as a consequence of the power outage based on data motivated by reference [8] as an example in Fig. 2, which again can be used by CaESAR in its resilience assessment.

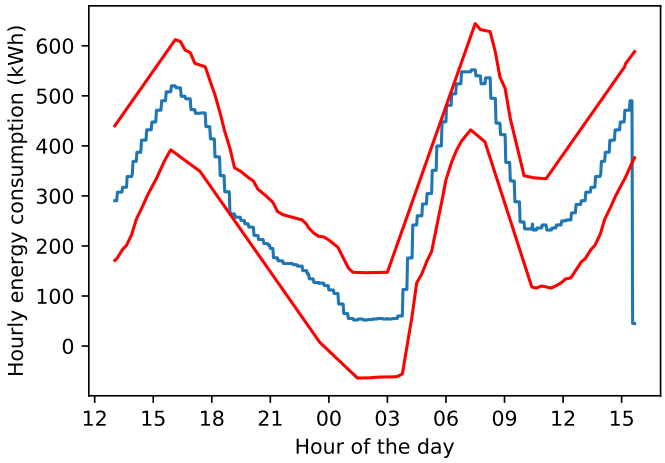


Fig. 2. The representative electric power consumption for an example station throughout the day exhibits an abnormal drop due to the outage of the main power supply.

4 Resilience assessment

Given a threat detection for the power outage scenario from CuriX, either prior to or at the time of the power outage, CaESAR is capable of performing a resilience assessment for the impacted SCADA which controls the power supply.

The detected threat impacts a certain node in the asset network model. From there it can propagate in the network based on the edges, given the assigned propagation probability and the impact delay (see Table 1). The propagation methodology adopts models used in epidemology. Further, we remark that in this resilience assessment we assess the impact on the network in the worst case scenario when redundancy from an uninterruptible power supply is failing. The recovery of impacted nodes is controlled by restoration times, also given in Table 1. Impact delay and recovery times vary based on a normal distribution with a given standard deviation.

Based on the parameter settings and network setup along with triggering events, repeated Monte Carlo simulations are performed considering the specified uncertainties. For each simulation a performance curve is obtained which describes the performance of the network as a function of time before, during and after an incident.

The performance p ranges between 0 and 1 and at one specific time step is defined as

$$p = \frac{\sum_{n=1}^{N} p_n}{N} \tag{1}$$

with N being the total number of nodes in the network.

Table 1. Network model specifications

Parameter	**Value**
Iterations	1000
Time steps T	120
Time step length	1 minute
Propagation probability	75%
Propagation probability after detection	25%
Mean of restoration time $mean(t_{res})$	60 minutes
Standard deviation of restoration time $std(t_{res})$	10 minutes
Mean of impact delay time	1 minute
Standard deviation of impact delay time	1 minute

The area A for any performance curve $p(t)$ where t is the time is given relative to the reference area A_{ref} as

$$A_{ref} = \int_0^T p_{ref}(t)dt \tag{2}$$

$$A = \frac{100 * \int_0^T p(t)dt}{A_{ref}} \tag{3}$$

with $p_{ref} = 1$ for all t and T being the number of time steps considered. Practically, the integral is approximated by the trapezoidal rule. The estimate of A enables to compare quantitatively different situations. In the following we compare simulations with varying detection times $t_d = \{-1, 0, 1, 2, 6, 12, 25, 50, 100\}$, restoration times $mean(t_{res}) = \{2, 6, 12, 25, 50, 100\}$ and corresponding $std(t_{res}) = \{0.3, 0.6, 1.3, 2.5, 5.0, 10.0\}$.

Dependent on when the attack/incident has been detected and most importantly has been identified, the probability for propagation in the network is reduced (see Table 1). This reduction in propagation represents the ability to react more specifically as the threat is identified by the detection. For example, if an intruder is detected security personal can be activated or if a malware is detected IT equipment can be isolated to reduce further propagation.

Fig. 3 presents some example simulation results for the resilience assessment of a single station. Repeated simulations lead to several resilience curves with different parameter settings. If the detection time is negative (see Fig. 3(a)) the early detection enables to avoid the impact. However, the uncertainty in the impact propagation leads to simulation runs with minimal damage to the system even with early detection. With a detection time of $t_d = 6$ (see Fig. 3(b)) the maximum detection time is reached. With larger t_d no further increase in resilience is achieved. This is also demonstrated in Fig. 4(a).

For a mean restoration time of $mean(t_{res}) = 6$ a large impact in the system but with a short duration can be observed (see Fig. 3(c)). An increasing mean restoration time leads to larger duration of the degraded status of the assets (see Fig. 3(d)).

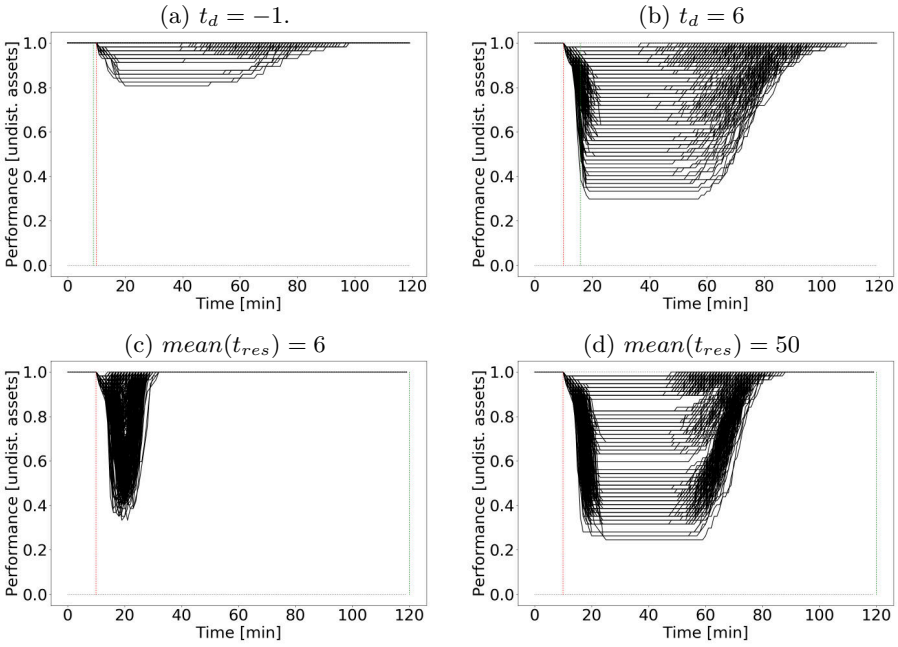


Fig. 3. Example resilience curves for 1000 repeated simulations with varying (a, b) detection time and (c, d) repair time mean and standard deviation. Performance is based on the number of undisturbed assets. Parameter settings not specifically adapted/mentioned in the headers are given in Table 1.

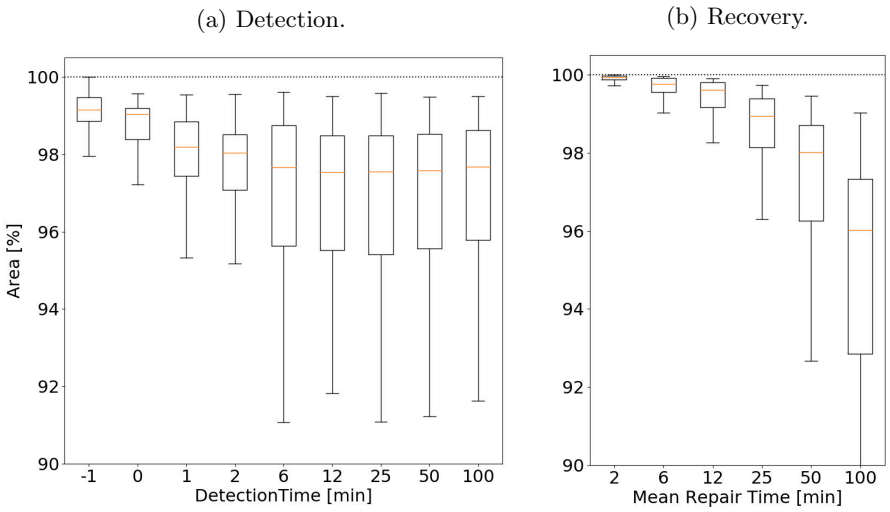


Fig. 4. Area for 1000 repeated simulations with varying (a) detection time and (b) repair time mean and standard deviation. The horizontal line in the box is the median. The upper and lower outer bounds of the box represent the upper and lower quartile. The whiskers present all data within 1.5 times the interquartile range. Outliers are discarded in this plot. The horizontal dotted line presents the maximum area to be expected when the system is not impacted. The measurement unit is performance times minute.

Comparing different parameters for detection and restoration enables to find the optimal settings to maximize the area below the curves and thus to maximize the system's resilience. The summary of these findings is given in Fig. 4. Note, that with increasing mean restoration time also the standard deviation of the restoration time is increased. This explains the larger uncertainty in cases with larger mean repair time (4(b)).

5 Metro and train infrastructure network

5.1 Metro grid

In this section, the previously analyzed impact on a single station, given by its asset topology model, is now propagated and studied in the context of the train and metro network for the Ankara public transportation system as an example. The network topology is derived from publicly available sources such as metro line maps. Fig. 5 presents metro and train lines for the example network with stations defined as nodes and lines defined as edges.

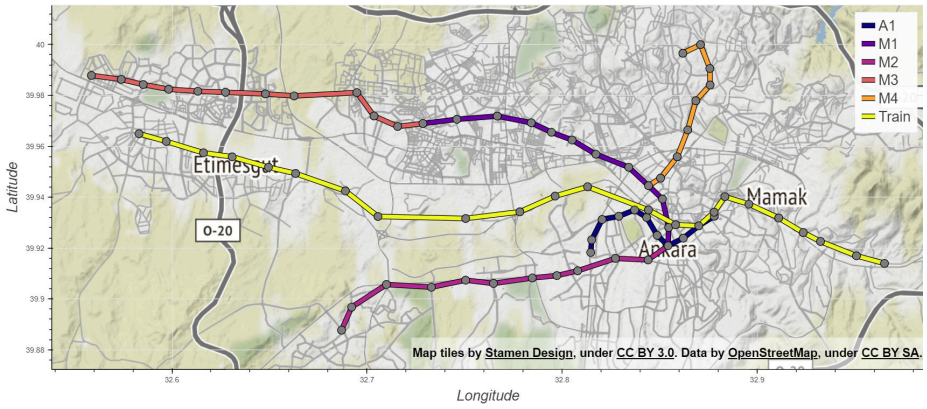


Fig. 5. Ankara metro and train map.

5.2 Agent-based model

On the network structure given in Fig. 5, an ABM is developed. Generally, ABM is a bottom-up modeling approach that starts by defining agents and their properties [23]. The next step in developing an ABM is the definition of internal rules [23]. Here, on each line several trains are defined which travel from node to node along the full length of the line before returning. In each timestep a certain number of passengers is generated with random start positions and target stations. They generate a route in the network and switch trains if needed.

Table 2. ABM specifications

Parameter	**Value**
Iterations	1
Time steps	23,040
Time step length	15 seconds
New passengers per time step	appox. 2.7
New passenger per day	approx. 15,700
Impact on time step	8,000
Restore on time step	8,900
Trains per line	2
Maximum number of passengers per train	400

Once a Station is impacted, no train will move in or out of the station. This effectively stops all traffic going through this station and passengers will look for an alternative route. In this example the impact on a very central node would sever many routes from each other, making the impact especially severe.

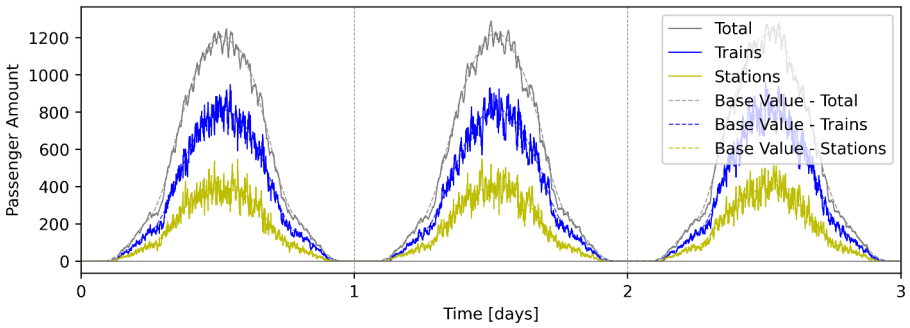
Fig. 6(a) shows an incident-free period. During three days passengers are 'generated' by a simple sine-wave. In the night, there are no spawns, so the system has time to flush all passengers. Fig. 6(b) presents passenger numbers with an impact in the morning of day two which blocks the station 'Kızılay' for about one hours. This leads to a huge passenger build-up and an increase of the total passenger amount in the peak. Still, the system manages to clear all passengers before the next day starts.

In Fig. 6(c) the (total) difference between the current number of passengers in the network and the usual number of passengers at the same time given by a base value is presented. The base values are smoothed curves for normal operation (see 6(a)). The variation from the base value is arising from the uncertainty in route generation per spawning passenger. The impact on the second day leads to a sharp increase in the passenger amount, surpassing the usual amount by a huge margin.

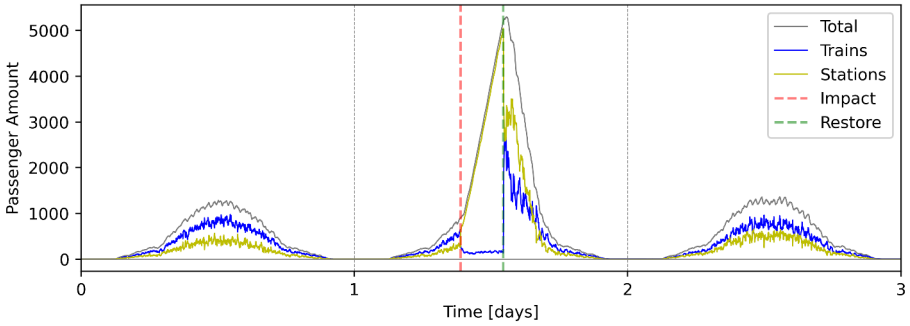
To enable the estimate of economic loss based on the passenger deviations during a disruptive event, the time spent per person in the system can be measured. Fig. 7 shows the amount of time passengers 'waste' waiting for trains which do not arrive due to the impact or are simply filled to their capacity (which does not happen in the simulation for normal operation).

Note, if a station is not connected any more in the network it cannot be reached by passengers. This leads to disrupted routes for the passengers. Here, the assumption is made that passengers without possible route wait in the system. However, in disrupted metro and train systems measures would be taken to transport passengers in alternative means such as buses. Thus, the simulation results underline the need for rerouting options to recover the system faster.

(a) Normal operation.



(b) Disturbed operation.



(c) Deviation from normal.

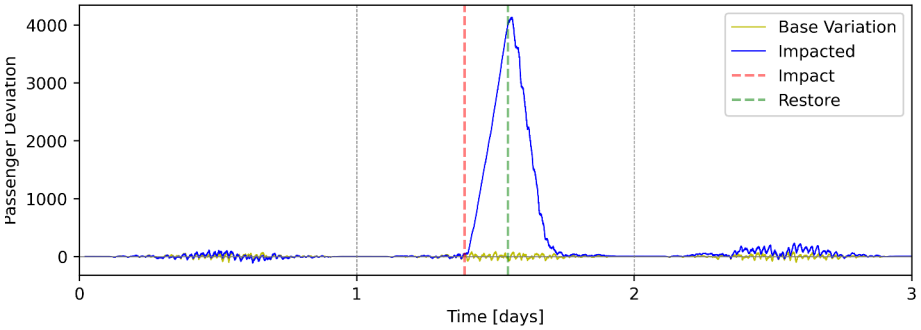


Fig. 6. Passenger numbers over three days estimated by the ABM for (a) normal operation, (b) disturbed operation and (c) the deviation between the base values of (a) and (b).

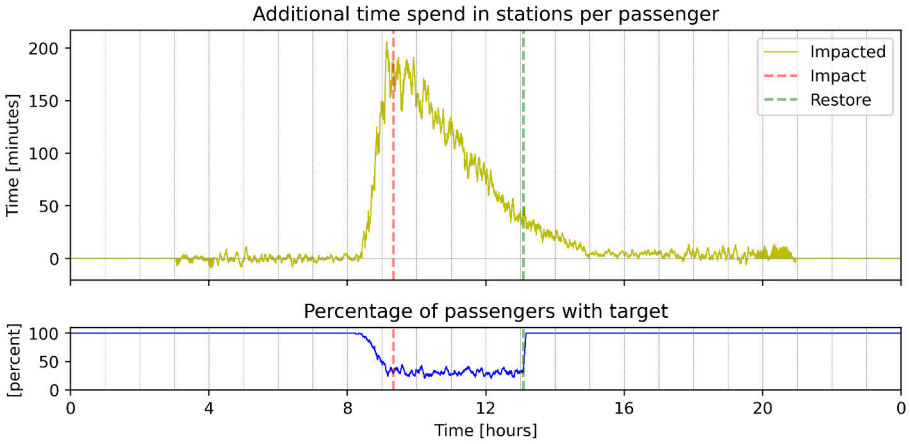


Fig. 7. Top: Additional minutes that the passengers spend in the metro and train network due to the disruption. Bottom: Percentage of passengers that reach their target.

6 Conclusion and outlook

In this work, a methodology has been presented to quantify network resilience for public transport infrastructure based on different impact propagation approaches and for different degree of detail embedded in the development of the CaESAR software. The approaches are combined with anomaly detection methods from the CuriX software to improve the networks resilience, which is together with CaESAR part of the SAFETY4RAILS toolkit. First, a single metro station is modeled as asset topology and based on the edges attack paths can be visualized and analyzed. Further, threat propagation in this network and the resulting degradation of the station functionality can be simulated. The simulation also enables to quantify that the earlier an attack/threat is detected, the larger are the chances to avoid further damage propagation. Furthermore, a range of ideal detection times can be quantified from the topology and the resilience assessment. In this work, it ranges between early detection with negative values, which means there is a good chance to avoid the impact altogether, and 6 minutes. After that time the whole system is already impacted by the attack/threat. In the latter case, recovery is another parameter to reduce the impact and thus increase the resilience. Finally, we found that the interplay between detection and recovery governs the response of the system and both parameters contribute to the optimization of infrastructure resilience.

The second approach for impact propagation employed in this work is an ABM which operates in Ankara's metro and train network as example use-case. It enables to quantify the passenger amounts during normal and disturbed operation. Based on the additional time passengers spend in the network under disturbed conditions, the economic loss could be estimated.

Finally, the detection and single station resilience assessment can be coupled with the ABM metro and train model to estimate predictions for real-time decision support. This framework is presented in this paper exemplary and could be employed to the assessment of infrastructure resilience in various domains.

This paper showed that the combination of the main functionalities anomaly detection, cascading effects analysis and ABM can contribute to resilience assessments of critical infrastructures. Anyway, there are aspects worth to be considered candidates for improvements: The anomaly detection described above was conducted in a univariate way without taking into account system knowledge. In future work, we would like to consider the system model of CaESAR within CuriX to enhance the quality (accuracy, precision) of the anomaly detection. Furthermore the simulation results of the ABM shows that time-series of passenger flow data could enrich the anomaly detection to widen the range of phenomena that could be recognized. Within the project SAFETY4RAILS we have build a platform in which several tools collaborated while in this article we exemplified the collaboration of only two tools with the additional ABM of that platform. In future articles we plan to report also about the collaboration of other tool-combinations.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein. For more information on the project see: https://safety4rails.eu/.

References

1. Bešinović, N.: Resilience in railway transport systems: a literature review and research agenda. Transport Reviews **40**(4), 457–478 (2020)
2. Bezemskij, A., Loukas, G., Anthony, R.J., Gan, D.: Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. In: 2016 15th international conference on ubiquitous computing and communications and 2016 international symposium on cyberspace and security (IUCC-CSS). pp. 61–68. IEEE (2016)
3. Chopra, S.S., Dillon, T., Bilec, M.M., Khanna, V.: A network-based framework for assessing infrastructure resilience: a case study of the london metro system. Journal of The Royal Society Interface **13**(118), 20160113 (2016)
4. Delgado, D., Aktas, C.B.: Resilience of rail infrastructure in the us northeast corridor. Procedia Engineering **145**, 356–363 (2016)
5. Edwards, C.: Resilient nation demos (2009)
6. European Union Agency for Cybersecurity: Threat taxonomy (2016), `https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view`
7. Fernandez, S., Schneider, C.: Neuronales netzwerk zur vorhersage von schwellwertverletzungen in zeitreihen (2021), `https://web0.fhnw.ch/ht/informatik/ip6/21fs/21fs_imvs04/index.html`

8. Guan, B., Liu, X., Zhang, T., Wang, X.: Hourly energy consumption characteristics of metro rail transit: Train traction versus station operation. Energy and Built Environment (2022)
9. Hiermaier, S., Hasenstein, S., Faist, K.: Resilience Engineering-how to handle the unexpected. In: 7th REA Symposium. p. 92 (2017)
10. Häring, I., Sansavini, G., Bellini, E., Martyn, N., Kovalenko, T., Kitsak, M., Vogelbacher, G., Ross, K., Bergerhausen, U., Barker, K., Linkov, I.: Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht pp. 21–80 (2017)
11. Risk management - guidelines. Standard, International Organization for Standardization, Geneva, CH (2018)
12. IT Security Association Germany - TeleTrusT Task Force "State of the art": IT Security Act (Germany) and EU General Data Protection Regulation: Guidline "State of the art" Technical and organisational measures (2021), https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/
13. Köpke, C., König, L., Faist, K., Fehling-Kaschek, M., Finger, J., Stolz, A., Burke, K., Georgiou, E., Mantzana, V., Chosiotis, I., Praca, I., Maia, E., Papagiannopoulos, N., Filipe, A., Escravana, N.: Security and resilience for airport infrastructure. In: Baraldi, P., Di Maio, F., Zio, E. (eds.) Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. pp. 1191–1198. Research Publishing, Singapore (2020)
14. Köpke, C., Srivastava, K., König, L., Miller, N., Fehling-Kaschek, M., Burke, K., Mangini, M., Praça, I., Canito, A., Carvalho, O., Apolinario, F., Escravana, N., Carstengerdes, N., Stelkens-Kobsch, T.: Impact propagation in airport systems. Cyber-Physical Security for Critical Infrastructures Protection **12618**, 191–206 (2020)
15. Köpke, C., Srivastava, K., Miller, N., Branchini, E.: Resilience quantification for critical infrastructure: Exemplified for airport operations. In: European Symposium on Research in Computer Security. pp. 451–460. Springer (2021)
16. Luo, Y., Xiao, Y., Cheng, L., Peng, G., Yao, D.: Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR) **54**(5), 1–36 (2021)
17. Marino, D.L., Wickramasinghe, C.S., Amarasinghe, K., Challa, H., Richardson, P., Jillepalli, A.A., Johnson, B.K., Rieger, C., Manic, M.: Cyber and physical anomaly detection in smart-grids. In: 2019 Resilience Week (RWS). vol. 1, pp. 187–193. IEEE (2019)
18. Miller, N., Satsrisakul, Y., Faist, K., Fehling-Kaschek, M., Crabbe, S., Poliotti, M., Naderpajouh, N., Setunge, S., Ergün, S., Kanak, A., et al.: A risk and resilience assessment approach for railway networks. Proceedings of ESREL-2021 (2021)
19. National Cyber Security Centre: Nis compliance guidelines for operators of essential service (oes) (2019), https://www.ncsc.gov.ie/pdfs/NIS_Compliance_Security_Guidelines_for_OES.pdf
20. SAFETY4RAILS: Deliverable d2.3: System specifications and concept architecture (2021), https://safety4rails.eu/wp-content/uploads/2022/03/S4R_RPT_D2.3_V1_6.pdf
21. Siebold, U., Ziehm, J., Häring, I.: Terror event database and analysis software. In: Future Security, 4th Security Research Conference (2009)

22. Thoma, K.: Resilien-Tech:Resilience by Design: a strategy for the technology issues of the future. Herbert Utz Verlag (2014)
23. Van Dam, K.H., Nikolic, I., Lukszo, Z.: Agent-based modelling of socio-technical systems, vol. 9. Springer Science & Business Media (2012)