(Online) ISSN 2744-1741
Defense and Security Studies *Original Research*
Vol. 6, No. 2, 2025, pp.122-131
https://doi.org/10.37868/dss.v6.id295

Vulnerability analysis of critical infrastructures with the Event Tree Technique

Francesco Trinchillo[1*]
[1] Independent researcher, Naples, Italy

*Corresponding author E-mail: francesco.trinchillo.1987@gmail.com

Received: Nov. 4, 2025
Revised: Nov. 20, 2025
Accepted: Nov. 26, 2025
Online: Nov. 26, 2025

Abstract

The vulnerability analysis of a critical infrastructure is certainly a complex and articulated study; therefore, it requires the use of reliable decision support tools. In this article, after a brief review of the state of the art on risk analysis studies for critical infrastructures, a vulnerability analysis will be performed on a railway infrastructure under the hypothesis of an intentional attack by a criminal group. Specifically, the aim of this paper is to show how the application of the event tree technique - derived from the more well-known fault tree analysis - can allow to define the different scenarios. For each one, a probabilistic assessment will be carried out through numerical simulations with the Monte Carlo method in order to calculate the security level of this infrastructure.

Keywords: Critical infrastructure, vulnerability analysis, defense of the country, event tree technique, Monte Carlo method, railway system

1. Introduction

A critical infrastructure – according to the current European legislation – is defined as an element, a plant, a piece of equipment, a network, a system, or a part thereof necessary for the provision of an essential service. Thus, protecting national critical infrastructures is necessary to guarantee the continuity of essential services, i.e., those that are fundamental for the maintenance of vital functions of society, economic activities, public health and safety, or the environment. The operation of critical infrastructures can be disrupted in the most varied ways that can range from a small inconvenience to total destruction; a natural catastrophic event (e.g., earthquakes, tsunamis, floods) or an indirect anthropogenic event (e.g., landslide, blackout), or a terrorist/criminal attack.

The study of the vulnerability of critical infrastructures starts from their identification in order to define an appropriate level of protection that guarantees, for each typology, not only its conservation but also the maintenance of the supply of essential services, limiting the inconvenience for the population involved.

The context of the operation of critical infrastructures has seen, during the years, a regulatory evolution [1]; now the critical infrastructures can be divided into 11 sectors:

1. Energy
2. Transport

3. Banking
4. Financial market infrastructure
5. Health
6. Drinking water
7. Waste water
8. Digital infrastructure
9. Public administration
10. Space
11. Production, processing, and distribution of food.

It is clear, therefore, that the railway system of a European Union Country is classified as a critical infrastructure; indeed, also the first forms of regulation of the European Commission drawn up at the beginning of the 2000s already include transport systems (roads, railways, ports, and airports) in the macro-categories of national critical infrastructures [1].

In the literature, there are several studies dedicated to the risk and vulnerability analysis of critical infrastructures, but only a few of these refer to the transport sector and specifically to railway systems. An interesting article [2] provides a complete and updated overview of the scientific research conducted, from 2008 to 2019, on the topic of railway resilience, showing a constant increase in the number of articles published in recent years. Railway infrastructure is made up of many interconnected and interdependent elements; understandably, since in practice it is not possible to protect all elements of the system, the approach often chosen is to protect key elements. Indeed, extensive research [3] aims to explore theoretical approaches to rail system vulnerability: identifying key elements can guide administrators in contributing to increasing resistance and in appropriately developing investments for the management and protection of railway system infrastructure.

Natural disasters, operational accidents, and terrorist attacks pose growing threats to railway systems, and their vulnerability and resilience have become major concerns for researchers and practitioners around the world. Thus, the importance of transport resilience and the related concepts of risk and vulnerability are also addressed from the perspective of shocks that transport systems may experience, which can be internal or external, natural or man-made, intentional or involuntary [4]. In this context, a very interesting article 6 focuses on the resilience of rail freight operations in the event of extreme weather events. Drawing on a British case study of rail network disruption following the closure of a key line in early 2016, the analysis considers the impacts on rail freight service provision and broader supply chains; the information provided is used to formulate a series of recommendations for the national rail sector. A recent study [5,6] analyzes the vulnerability and resilience of railway systems to disruptions from a conceptual, methodological, and practical perspective. It presents methodologies for assessing railway system vulnerability and resilience based on accessibility theory and examines the case study of the railway systems of two Chinese cities, Shanghai and Shenzhen, using the proposed methodologies. Another research [7] considers the emergency management of the transport of dangerous goods in the event of a terrorist attack by analyzing the evolution of the accident scenario using advanced georeferencing tools.

2. Vulnerability analysis of the case study

This article will conduct a risk analysis of the vulnerability of a critical railway infrastructure, starting from an event similar to a terrorist attack deliberately carried out with the aim of causing serious consequences to the infrastructure in question. This analysis is part of the broader discipline known as Security Risk, which studies the analysis of risks related to human actions aimed at producing catastrophic damage; one of the first studies on this topic [8] extends risk analysis methodologies to such incident scenarios, offering a methodology for the quantitative assessment of terrorism-related risks with the aim of supporting the decision-making process.

An interesting study [9] focused - very clearly - on the analysis of business impacts and the quantification of different risks, in order to define the acceptable risk level/threshold. Moreover, a recent research [10] has already considered similar critical infrastructures by adopting a time-based dependency risk analysis methodology, integrating and evaluating the effect of recovery controls. In that case, the proposed analysis methodology, based on awareness-based restoration, was integrated with a decision support system that enables the prediction of risk due to natural events to identify vulnerable and disrupted assets (e.g., electrical substations, telecommunications components).

Risk analysis methods are numerous and can be divided into two macro categories: qualitative and quantitative [11]; to determine the logic of attack sequences and consequently the reactions of security services/systems, more than one method can be used; among these, an inductive method called Event Tree Analysis (ETA) has been chosen, a methodology derived from the more well-known fault tree analysis technique, widely used in maintenance engineering [12]. The event tree technique can certainly be applied to intentional attacks (terrorist attacks, demonstrations, industrial sabotage, etc.); in this case, the event tree's final event is the achievement of a specific objective (damage, destruction, disruption of service, etc.), while the events that define the tree's structure are sabotage actions or actions by security personnel/police; each event is associated with a duration and probability of occurrence.

This article aims to carry out an analysis that shows the possible vulnerabilities of a critical infrastructure, hypothesizing the various attack scenarios and quantifying in probabilistic terms the risk of their occurrence. Consequently, useful insights can be gleaned into the "easiest" scenarios for attackers, thus defining the actual vulnerability level of the analyzed critical infrastructure. Therefore, based on the results obtained, it will be possible to determine how to improve the security level, perhaps by introducing new systems designed to thwart attackers' actions or, at least, react in a timely manner and thus reduce the damage.

2.1. Railway infrastructure

The critical infrastructure under consideration is a railway electrical substation, a "node" connected to a high-voltage electrical grid capable of transforming and converting high voltage into a form suitable for powering train drives and motors. It is clear that the decommissioning of a substation will result in the failure of a section or even an entire railway line, resulting in the disruption of one of the country's essential services. Furthermore, if the affected line is a high-speed/high-capacity line, the disruptions can be truly impactful for the Country.

Typically, a railway substation is located immediately outside a residential area and - in this case - it is assumed to be within an area of approximately 2000 m^2, which can be accessed through an automatic sliding steel gate overlooking a main road. The gate leads to a yard containing a building containing electronic equipment that controls the electrical energy conversion systems. Outside, adjacent to the building, are the conversion and transformation systems, as shown in Figure 1.

Figure 1. Example of a railway electrical substation

The area has a polygonal shape and is bordered on two sides by thick, tall vegetation that prevents the passage of vehicles and/or people; on the other sides, however, there are 3-meter-high metal fences topped with hooked gates. The area is equipped with a CCTV system consisting of cameras, some fixed and some pan/tilt, positioned around the yard's perimeter and at the single entry/exit point, as well as those that monitor the entrances to the building housing the electronic equipment. The cameras are oriented so that the same point can be framed by multiple devices, and all are connected to the control room via a fiber optic backbone. The control room is located at the security department of the company that manages the country's railway network, while the nearest police patrol station is approximately 4 km from the substation.

2.2. Attack scenarios and event tree construction

This study hypothesizes an intentional attack by a criminal group aimed at damaging the electrical substation systems that power the transmission line for high-speed trains (Tables 1 and 2). It is assumed that the group is already aware of the types of defense systems (active and passive) present and, specifically, knows the exact point to access to interrupt the fiber optic link that powers the CCTV system. The possible scenarios envisioned for the case study in question all involve two sequences: one for the actual attack process, consisting of the criminal activities undertaken by the attackers; the second, however, is the sequence represented by the defense actions implemented first by the company security service and then by the police.

Both sequences, which then trigger the various scenarios, begin with the cutting of the fiber optic backbone, which causes the instantaneous deactivation of the CCTV system; therefore, this action can be defined as the top event of the event tree, meaning it relates to an attack directed at a specific target. The duration of this action, although quantifiable as an average time, is deliberately excluded from the risk analysis because it is precisely by virtue of its identification as the top event, or initiator, from which the subsequent steps arise. In other words, if one were to hypothesize the introduction of the NOT operator for this event, the subsequent sequences would lose their meaning.

Table 1. Average time for attack actions

ACTIVITY	AVERAGE TIME (minutes)
Reaching the substation	3
Entry into the substation	8
Reaching the equipment area	5
Sabotaging the equipment	7
Leaving the equipment area	2
Leaving the substation and beginning the escapement	5
Complete escapement	5

Table 2. Average time for defense actions

ACTIVITY	TIME (minutes)
Security personnel interpret the situation	4
Security personnel call the police	2
Police action	22

The attack sequence can be summarized as follows:

1. Reaching the substation
2. Entry into the substation
3. Reaching the equipment area
4. Sabotaging the equipment
5. Leaving the equipment area
6. Leaving the substation and beginning the escapement
7. Complete escapement

The defense sequence can be summarized as follows:

1. Security personnel interpret the situation.
2. Security personnel call the police.
3. Police action.

For each activity, whether attacking or defending, an average time expressed in minutes has been identified. Sequences can also be represented in the form of Gantt charts (Figs 2 and 3).

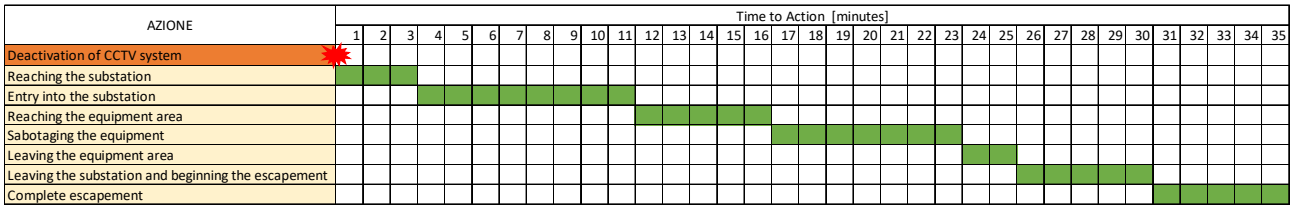

Figure 2. Gantt chart with attack sequence

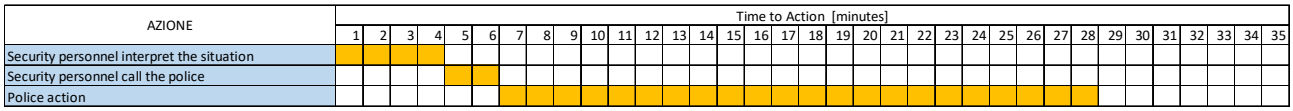

Figure 3. Gantt chart with defense sequence

To better contextualize the sequences just described, it is necessary to draw up hypotheses that allow us to properly define the event tree and understand the infrastructure's actual vulnerability level. Specifically, we will assume that:

• The CCTV system was fully functional at the time of the attack.
• The criminal group is informed of the nature of the CCTV system and the location of the access point to the fiber optic backbone that powers it.
• Cutting the backbone will certainly deactivate the CCTV system, but will also—with equal certainty—activate an alarm located at the company security guard post.
• Company security cannot intervene in the event of this type of attack and must request and await the intervention of the police.

The success of the attack is confirmed by the sabotage of the equipment and the complete disappearance of the criminal group. This final event—which, as mentioned, corresponds to the complete success of the operation—can also be imagined as a consequence, involving the arrest of the group and, possibly, the prevention of the sabotage of the equipment. It is therefore assumed that police action could occur in the following phases:

- After exiting the substation but before the group has completely disappeared (Scenario 2)
- After the sabotaged equipment has been removed from the area, but before exiting the substation (Scenario 3)
- After the sabotage of the equipment but before reaching the exit (Scenario 4)
- After reaching the area where the equipment to be sabotaged is located, but before its sabotage (Scenario 5)
- After entering the substation but before reaching the area where the equipment to be sabotaged is located (Scenario 6)

It is clear that the event tree will foresee a total of 6 possible scenarios: the 5 just described in addition to the one that, obviously, foresees the success of the attack, which can be identified as scenario 1.

For simplicity of discussion and based on the hypotheses made, it is assumed that reaching the substation and entering it (with the related break-in and tampering with the automation of the access gate) are certain actions, that is, that they occur with probability 1 and that the police cannot intervene before or during their execution; this allows us to limit the number of scenarios to those that are actually the most realistic.

Based on the above assumptions, it is possible to construct the event tree. (Fig. 4).

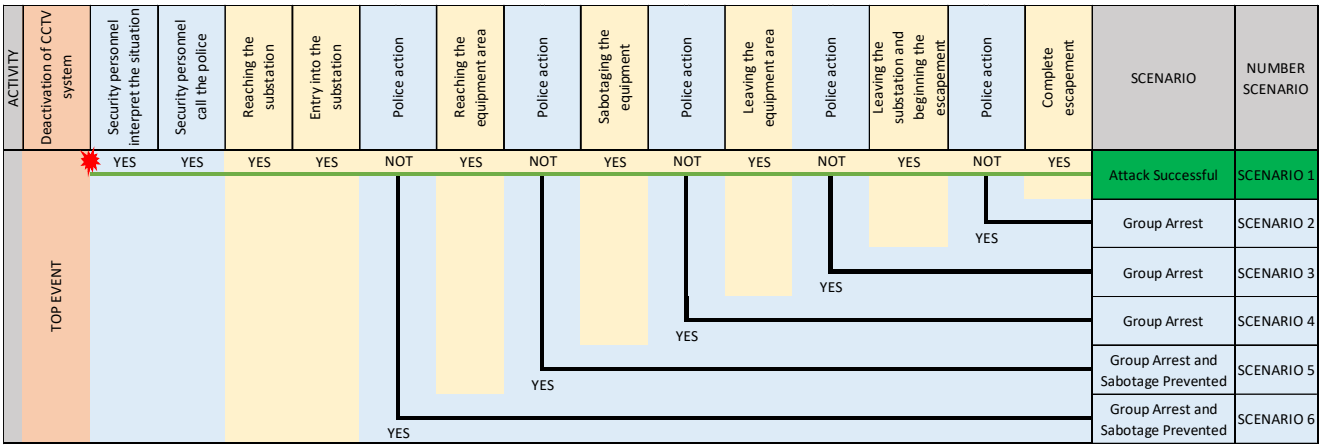

Figure 4. Event tree with possible attack scenarios

For simplicity, but without losing its meaning, it is assumed that both the corporate security service and the police cannot make significant errors in the execution of their tasks and that their interventions are 100% effective (meaning they completely block attack action) and are also detectable within an exact time frame. Based on this further hypothesis, while the execution times of individual actions for the criminal group's activities remain variable, those relating to defensive actions become exact values.

Focusing on attack actions, the times of each of them can be considered random variables characterized by their own probability density distribution: for each action, therefore, the average time T already indicated in Table 1 has been associated with a relative standard deviation σ, which, again for simplicity, is assumed equal to 30% of the average value. Otherwise, based on the assumption made, the times of the defense actions (Table 2) will be deterministic; therefore, we should not speak of mean time or standard deviation but only of action time.

Table 3. Average time and standard deviation times for attack actions

ACTIVITY	AVERAGE TIME (minutes)	STANDARD DEVIATION
Reaching the substation	3	0,9
Entry into the substation	8	2,4
Reaching the equipment area	5	1,5
Sabotaging the equipment	7	2,1
Leaving the equipment area	2	0,6
Leaving the substation and beginning the escapement	5	1,5
Complete escapement	5	1,5

Table 4. Exact time for defense actions

ACTIVITY	TIME (minutes)
Security personnel interpret the situation	4
Security personnel call the police	2
Police action	22

2.3. Probability calculation

Having defined the six possible attack scenarios, the next step is to understand the probability of one scenario occurring over another, in order to determine the actual level of vulnerability of the infrastructure. The solution to the presented problem begins by defining the total time required to complete the generic attack sequence, which will undoubtedly be the sum of the completion times for each criminal activity.

Thus, indicating the total time for the generic scenario as T_{Si} , we have:

$$T_{Si} = T_{a1} + T_{a2} + T_{a3} + \ldots + T_{an}$$

Table 5. Average time for each attack scenario

SCENARIO	AVERAGE TIME (minutes)
SCENARIO 1 (Attack Successful)	35
SCENARIO 2 (Group Arrest)	30
SCENARIO 3 (Group Arrest)	25
SCENARIO 4 (Group Arrest)	23
SCENARIO 5 (Group Arrest and Sabotage Prevented)	16
SCENARIO 6 (Group Arrest and Sabotage Prevented)	11

As already mentioned, however, the times of the individual attack actions are random variables, meaning they can assume different values each time one approaches the resolution of the problem under analysis. They are characterized by their own probability density function, which, for events of this type, can be considered lognormal.

Therefore, the total time of each scenario will also be a random variable whose probability density can be determined from the times of the individual activities.

By applying the variable transformation method [13], it is possible to calculate the probability density associated with the generic scenario. The application of this methodology allows closed-form analytical solutions only for particular cases, that is, for those cases in which the probability densities are normal. In general, however, to obtain the solution, it is necessary to resort to numerical methods or Monte Carlo simulation.

For the case study in question, the solution to the problem is obtained in two steps: the first objective is to calculate the probability of success of the attack (scenario 1), that is, to calculate the probability with which the total time required to carry out the entire attack sequence is less than the intervention time of the police:

$$P_{\text{attack successful}} = P\ (\text{total time of attack sequence} < \text{time for police action})$$

The second part of the problem consists in determining the probability of occurrence of all the other scenarios (from 2 to 6) that foresee the failure of the attack and therefore the arrest of the group due to the intervention of the police before the complete disappearance of the attackers; for these cases, the probability of occurrence can be determined as follows:

$$P_{\text{scenario } i} = [1 - P\ (\text{total time of attack sequence } i < \text{time for police action})],\ \text{for } i = 2 \text{ to } 6$$

Applying the Monte Carlo method leads to the solution shown in Table 6.

Table 6. Average time and probability of occurrence for each attack scenario

SCENARIO	AVERAGE TIME (minutes)	PROBABILITY OF OCCURRENCE
SCENARIO 1 (Attack Successful)	35	0,332
SCENARIO 2 (Group Arrest)	30	0,668
SCENARIO 3 (Group Arrest)	25	0,357
SCENARIO 4 (Group Arrest)	23	0,234
SCENARIO 5 (Group Arrest and Sabotage Prevented)	16	0,153
SCENARIO 6 (Group Arrest and Sabotage Prevented)	11	0,001

Reporting the values in the event tree allows us to gain a more systematic view of the case study, as shown in Fig. 5.

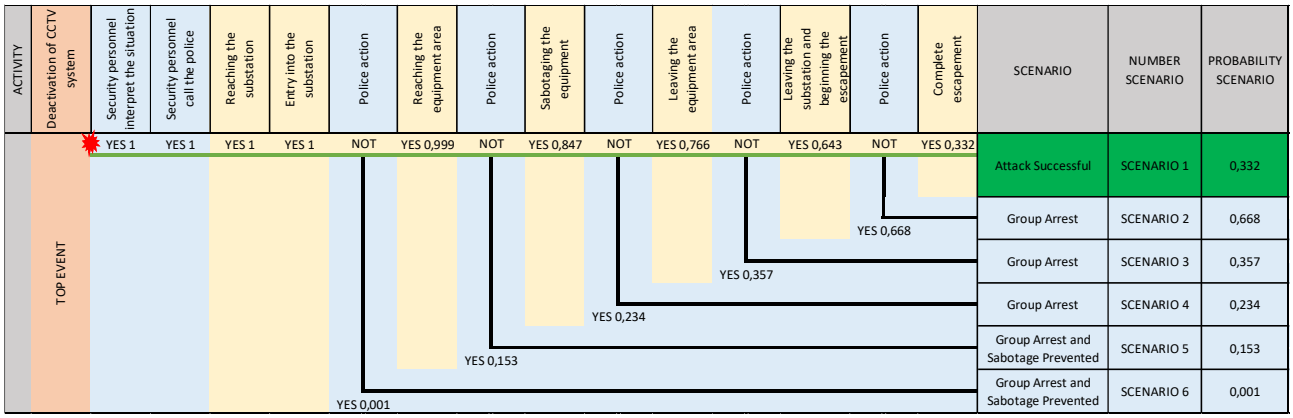

Figure 5. Event tree with possible attack scenarios and probability of occurrence

3. Results Analysis

The risk analysis conducted on this case study demonstrates how the event tree technique is able to provide a clear and systematic view of the problem. Specifically, it is shown that, based on the assumptions made, the complete success of the attack occurs with a probability of approximately 33%. This provides an objective measure of the vulnerability of the critical infrastructure considered. However, there are five alternative scenarios, all of which involve the failure of the attack with the arrest of the group, and between these two, even the prevention of the sabotage of the equipment. In Figure 6, the graph shows the trend in the probability of occurrence of each of the scenarios.

The success of the attack (scenario 1) is not the most likely scenario; in fact, its alternative (scenario 2) - consisting of the complete evolution of the criminal action but characterized by police intervention immediately before the escape - is the most likely scenario, with a probability of occurrence around 67%. The other hypothesized scenarios, obviously, have a decreasing probability of occurrence; this is because the probability of the police intervening quickly is low. It is interesting to note that the probability of the attack's complete success is almost equivalent to scenario 3, which involves the group being arrested before leaving the substation; this highlights that, based on the protection systems in place, the final outcome is quite uncertain.

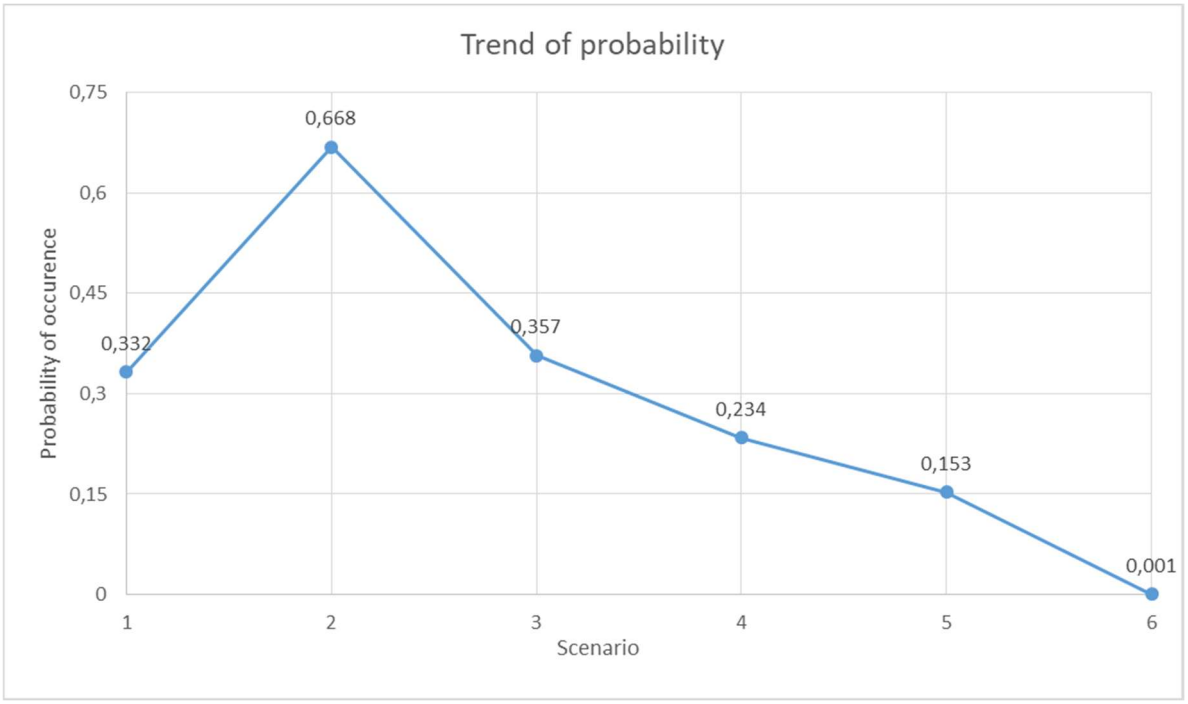

Figure 6. Trend of the probability of occurrence for each scenario

4. Conclusions

This article conducted a vulnerability analysis for a critical infrastructure within the railway system of a European Union Country. Specifically, it considered an electrical substation that supplies power to a high-speed train line. A power outage would lead to a halt in rail traffic, with significant impacts on transportation and, consequently, the national economy. A deliberate attack by a criminal group was hypothesized, characterized by successive actions that corresponded to corresponding reactions from existing security systems or the intervention of the police, with the aim of preventing sabotage of the equipment or, at least, arresting the criminal group. The case study, although linear and not complex in its outline, is extremely realistic and sufficiently comprehensive to maintain its generality. The event tree technique allowed us to identify the evolutionary path of the hypothesized dangerous condition, thus obtaining a clear attack sequence that, as previously mentioned, could be accompanied by responses aimed at reducing the damage. Unfortunately, however, the method does not allow for exact solutions in terms of the probability of occurrence of each scenario, so a computational analysis using the Monte Carlo method was used. The application of the numerical method allowed for tangible results, enabling the definition of the most likely scenario and the prioritization of risks. This allows for the development of strategies aimed at preventing such actions, using resources (financing, labor, time, etc.) that can improve both passive (alarm systems, gates, etc.) and active (police action) security systems.

An important aspect that this article aims to highlight is that vulnerability analysis is essentially independent of the causes of the attack (terrorist attack, demonstration, industrial sabotage, etc.). What matters is the attack's evolution and its modalities, in order to understand how to intervene to limit the damage or even prevent the attack. The purposes of this sabotage can be extremely varied, from a terrorist attack to a demonstration, but this is completely beyond the scope of this analysis. For this reason, the article will not address the hypothetical causes that could drive this criminal group to carry out such an attack.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

References

[1] F. Trinchillo, “Critical infrastructures: European context and evolution of the law,” *Journal of Defense Resources Management*, vol. 16, pp. 319–330, 2025. https://doi.org/10.64404/JoDRM.2025.1.15

[2] N. Bešinović, “Resilience in railway transport systems: A literature review and research agenda,” *Transport Reviews*, vol. 40, pp. 457–478, 2020. https://doi.org/10.1080/01441647.2020.1728419

[3] Z. Urbancová and E. Sventeková, “Assessing vulnerability of key elements of railway infrastructures,” *Transportation Research Procedia*, vol. 40, pp. 1597–1603, 2019. https://doi.org/10.1016/j.trpro.2019.07.221

[4] E. Jenelius and L. G. Mattson, “Resilience of transport systems,” in *International Encyclopedia of Transportation*, pp. 258–267, 2021. https://doi.org/10.1016/B978-0-08-102671-7.10719-5

[5] A. Woodburn, “Rail network resilience and operational responsiveness during unplanned disruption: A rail freight case study,” *Journal of Transport Geography*, vol. 77, pp. 59–69, 2019. https://doi.org/10.1016/j.jtrangeo.2019.04.006

[6] L. Qing-Chang, X. Pengcheng, *et al*., “Railway vulnerability and resilience,” in *Rail Infrastructure Resilience*, Woodhead Publishing Series in Civil and Structural Engineering, pp. 5–35, 2022. https://doi.org/10.1016/B978-0-12-821042-0.00020-4

[7] F. M. Milazzo, G. Ancione, *et al*., "Risk management of terrorist attacks in the transport of hazardous materials using dynamic geoevents," *Journal of Loss Prevention in the Process Industries*, vol. 22, pp. 625–633, 2009. https://doi.org/10.1016/j.jlp.2009.02.014

[8] J. B. Garrick, J. E. Hall, *et al*., "Confronting the risks of terrorism: Making the right decisions," *Reliability Engineering & System Safety*, vol. 86, pp. 129–176, 2004. https://doi.org/10.1016/j.ress.2004.04.003

[9] D. Pleškonjić, F. Virtuani, and O. Zoggia, "Security risk management for critical infrastructures," in *Proc. 8th Conf. Italian Chapter of AIS*, Rome, Italy, Oct. 7–8, 2011. https://doi.org/10.13140/2.1.3846.8800

[10] G. Stergiopoulos, P. Kotzanikolaou, *et al*., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures," *Int. J. Critical Infrastructure Protection*, vol. 12, pp. 46–60, 2016. https://doi.org/10.1016/j.ijcip.2015.12.002

[11] D. C. Simmons, R. Dauwe, *et al*., "Qualitative and quantitative approaches to risk assessment," in *Understanding Disaster Risk: Risk Assessment Methodologies and Examples*, pp. 44–130, 2017. [Online]. Available: https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/ch02/ch02.pdf

[12] J. A. B. Geymayr and N. F. F. Ebecken, "Fault-tree analysis: A knowledge-engineering approach," *IEEE Trans. Reliability*, vol. 44, no. 1, pp. 37–45, 1995. https://doi.org/10.1109/24.376519

[13] L. Fabbris, *Statistica multivariata: Analisi esplorativa dei dati*. Milan, Italy: McGraw-Hill Libri Italia, 1997, ISBN: 9788838607653.