Co-creating a Railway Security Concept Against CBRNe Threats to Passenger Rail Transport Hubs

Laura Petersen
UIC
petersen@uic.org

Grigore Havârneanu
UIC
havarneanu@uic.org

Paula Fernandéz Díaz
UIC
fernandez@uic.org

ABSTRACT

Railways, as cornerstones of modern societies and open public spaces, face numerous threats, including those stemming from Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) agents. Before first responders arrive at a potential CBRNe incident occurring in the rail environment, rail staff are likely to be the first to react and may be able to provide guidance or take appropriate, live-saving actions. Yet a gap remains regarding the sector's CBRNe preparedness and response capabilities. The CBRNe4rail project aims to enhance railway stakeholders' awareness and response capabilities. Through three technical work streams deploying project reviews, a survey with railway stakeholders, study visits at several railway stations and workshops with end-users, the project's expected results include a CBRNe railway security concept and a CBRNe training curriculum, including one virtual reality scenario, all of which will take into account information systems used by the sector. By involving end-users throughout the process, the project aims to deliver practical tools, improving the resilience of passenger rail transport hubs against such threats.

Keywords

CBRNe, rail security, security-by-design, security trainings, codesign

INTRODUCTION

Railways are cornerstones of modern societies, enabling the free movement of people and goods. The rail environment is huge, open and interconnected, with UIC, the International Union of Railways, reporting 1,151,314 line-kilometres[1] in the world (UIC, 2024). Moreover, railway stations can be considered public spaces with low barriers to entry, a key component of public transport.

Unfortunately, due to their importance to societies and economies, railways are also targeted by malicious actors wishing to cause harm (Strandberg, 2013). Attacks can cause many casualties, serious transport disruptions and significant financial and economic losses. Malicious actors may employ a variety of means including Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) plots, as demonstrated by past attacks. Indeed, using the key word "rail" on the Global Terrorism Database (2024) finds over 2,200 incidents between 1970 and 2020 as a result. The majority of these terrorist attacks are listed as having been carried out with the modus operandi of 'bombings', via Improvised Explosive Devices (IEDs). Some iconic, historic examples include the 2004 Madrid, 2005 London and 2016 Brussels attacks, all of which led to many deaths and casualties.

In addition, chemical attacks have already been deployed in the rail environment, the most nefarious of which is the 1995 Tokyo attack, whereby sarin vapour was intentionally spread through stations and trains (OPCW, 2020). While not yet employed, recent Europol (2019) reports indicate that IEDs could be combined with toxic chemicals or radioactive materials to make what are known as 'dirty bombs', significantly enhancing their lethal impact.

[1] UIC assess the size of a network in line-kilometers. For 1 line, you can have 1 or 2 or more tracks. For example, in freight terminals, there many tracks.

Beyond terrorism, railways are also targets for hybrid warfare actions like sabotage (Luxton & Marinov, 2020), such as the recent (November 2025) attack in Poland (Ciobanu & Burrows, 2025). Furthermore, sabotage could perhaps target trains transporting dangerous goods. Non-malicious incidents involving hazardous goods trains derailing near the population demonstrate their impact, as for example the 2023 Ohio, USA incident, which led to the evacuation of the town of East Palestine (Welsh et al., 2024). Hence, CBRNe material(s) being used to carry out a major criminal or terrorist attack is therefore a serious threat for railway stakeholders.

Railway premises and rolling stock are potentially conducive for a CBRNe attack as they provide a favourable environment for mass casualty and cross-contamination (Havârneanu et al., 2022). This is due to some inherent characteristics of rail premises as public spaces, including high density, anonymity of persons, easy access for perpetrators, combination of both open and closed areas, use of ventilation systems, presence of commercial areas equivalent to shopping centres, among others, with many rail stations being listed as historic monuments and therefore unable to deploy security-by-design 'best practices' (Havârneanu et al., 2024). Furthermore, a completely hardened approach to security, with strict access control measures and protection of all assets, is neither desirable for public transport which inherently needs to be open, nor feasible for such a vast infrastructure. Additionally, modern railway stations increasingly rely on interconnected information systems for traffic management, passenger flows, surveillance, etc., adding another layer of complexity when preparing for or responding to CBRNe attacks. Such systems introduce new interdependencies and vulnerabilities while also offering opportunities to enhance preparedness and response strategies through improved situational awareness, reduced response times or more effective evacuation strategies (e.g., Schreiber et al., 2023; Unger et al, 2023).

Authorities such as law enforcement and fire brigades are responsible for responding to security incidents which may occur on railway premises and railway stakeholders have a complementary role to play (Strandh, 2015; Strandh, 2017; Díaz & Petersen, 2024). For example, during the 'golden minutes' following a CBRNe attack, whereby protective actions would have highly life-saving implications but First Responders (FR) like firefighters and Law Enforcement Agencies (LEAs) are not yet on-scene, railway staff would be the first point of contact for those affected and could act as 'immediate responders', providing guidance or taking appropriate, live-saving actions (Havârneanu et al., 2022). Once FR and specialised responders arrive on site, railway staff could further contribute in a supporting role, by for example facilitating evacuation or providing detailed knowledge of the rail environment, which can be considered an important part of multi-stakeholder cooperation (ibid).

Despite this, the transport sector's role in crisis management is often overlooked by both first responders and the sector (Edwards and Goodrich, 2014; Strandh, 2017). Making things even more complex, CBRNe incidents may demand diverse and sometimes contradictory preliminary response actions (e.g., evacuation vs. shelter-in-place). Havârneanu et al. (2022) revealed five core skills that railway staff need to develop or improve: 1) understand the specific characteristics of the CBRNe threat, 2) develop basic response measures, 3) cooperate with authorities and train with specialised First Responders, 4) improve public awareness about this threat, and 5) optimise crisis communication. Petersen et al. (2023) found that targeted support to the rail sector could help close CBRNe preparedness and response capabilities gaps and recent research examining railway stakeholders' security training needs identified CBRN basic 'Do's and Don'ts' (Havârneanu et al., 2024).

THE CBRNE4RAIL PROJECT

In line with the above challenges, the EU co-funded CBRNe4rail (CBRNe preparedness for passenger rail transport hubs) project aims to enhance railway stakeholders' awareness and response capabilities by improving security plans and providing targeted training for effective management of CBRNe emergencies. It tackles the whole CBRNe threat spectrum including explosives (e) as a means of delivery for CBRN agents. The project focuses on railway stations, as both a critical element of railway infrastructures and a key vulnerability element of public spaces, and on railway staff, as a key leverage of security and preparedness, due to the crucial role they could have in the first phase of a potential CBRNe incident.

The CBNRe4rail project is being implemented in partnership with the security services of major European railway companies and LEAs from Italy, Poland, Slovenia, Spain, and Sweden, technical experts from universities and research organisations and UIC – the worldwide railway association. Furthermore, additional rail stakeholders and specialised FR are being included in the Advisory Board. The project began in June 2025 and will run for a duration of 30 months.

The core methodology of the project is based on the high and regular involvement of end users in the co-design and implementation of all project activities. The project is being carried out over three phases, whereby: Phase 1 entails co-creating a railway CBRNe security concept, Phase 2 comprises the design and delivery of a CBRNe training programme for the railway sector and Phase 3 designs and delivers in-situ training exercises.

This paper presents the methodology which is being deployed in the CBRNe4rail project in order to achieve its

outcomes in further details and also shares the expected results.

CBRNe4RAIL PROJECT METHODOLOGY

Phase 1: co-creating a railway CBRNe security concept

The first technical work phase aims to co-create a railway CBRNe security concept by: (1) assessing rail CBRNe threats, current security plans, existing security-dedicated hardware and cooperation protocols; (2) creating operational scenarios revealing how the terrorist attack could be conducted and what impact it could bring upon the public; and (3) providing a guideline with recommendations to increase the CBRNe security level. These activities also consider the role of existing information systems used in stations and control centres, ensuring that operational procedures and communication tools are aligned with the proposed CBRNe concept. To achieve this, a co-creation-based methodology will be applied, combining desk research and end user engagement, through social science and humanities methodologies such as questionnaires, study visits and validation workshops.

First, a survey will be designed and tested by the end-users in the project before being sent out to railway stakeholders at large. The survey will address the following themes: the profile of respondents and participating organisations; awareness of CBRNe threats and hazards; existing security governance and operational practices; organisational capabilities and gaps in the railway security system; and expected improvements and training needs related to CBRNe protection.

It is planned to allow for both open and closed questions, allowing respondents to provide qualitative explanations, additional examples, and contextual elements. The survey findings are intended to reveal self-reported perceptions, practices and expectations from the railway sector rather than expert-verified assessments. Data analysis will combine quantitative and qualitative approaches.

At the same time, the project will carry out a state-of-the-art review of past and ongoing EU-funded CBRNe projects, aiming to review between 12 and 20 projects. Project results will be analysed in order to perform a gaps, needs and recommendations analysis, using a template-based approach to ensure harmonisation across reviews.

Following the survey, study visits will be conducted at railway stations, structured in two phases: an information-gathering phase and a physical site visit. Five visits are currently planned: one each in Poland, Italy, Spain, Slovenia and Sweden. For the information gathering phase, the railway end-users will share with expert partners documentation, procedures, existing protection measures, etc., which will then be reviewed.

Concerning the physical site visit, this is intended to be carried out by a multidisciplinary expert team composed of 6-9 members, covering key domains such as CBRN, IED, general security, law enforcement, fire and rescue services. The visits themselves will combine structured interviews with railway management, security personnel and technical staff, followed by physical inspection of the facilities. The assessment will focus on critical infrastructure elements, vulnerable systems (including HVAC, water and gas installations) and information systems, as well as the organisation and effectiveness of security measures.

Drawing from expert knowledge contained within the consortium, CBRNe-related scenarios will also be developed and validated. In a first stage, at each study visit, and in a second stage, at the validation workshop.

The survey results, review of past projects, scenarios and study visit results will then be validated by end-users in a workshop, using a problem-based learning methodology. This method involves participants solving areal, open-ended problems by independently planning actions and acquiring knowledge, rather than listening to ready-made lectures or solutions. The use of this method should enable workshop participants to focus on critical thinking and creative problem solving.

All these activities will provide a solid background for the next two work phases of the project and will produce a first exploitable output to be used by end-users after the project: ‘Guideline for improvement of railway security level and response to CBRNe incidents.’

Phase 2: designing and delivering a CBRNe training programme for the railway sector

The second technical work phase will develop a harmonised CBRNe training programme for the railway sector and for better cooperation with the involved FR. Indeed, a pivotal element of the CBRNe4rail project is the boosting of collaboration between railways and FR in emergency response. The project envisages the delivery of joint training sessions involving both railway operators and FRs to contribute to inter-agency coordination and communication in case of emergency. Specifically, training activities target railway staff due to their crucial role in the first phase of emergency response in case of CBRNe threats. On the other side, since prompt and effective coordination with FRs is crucial in emergency response, representatives from national FR organisations will also

join the training activities. The inclusion of VR training sessions to train operators on CBRNe emergency response will represent an innovative methodology complementing theoretical and practical sessions to ensure the achievement of training objectives as well as contributing to increasing the interactivity and immersion of the trainee's experience.

It will draw from the ISF RESIST project (2019), which developed a standardised CBRNe training curriculum for the establishment of "CBRNe Intervention Groups" within public and private operators of critical infrastructure / public spaces. Hence, CBRNe4rail's design and development process will be based on their training format and content, but taking into account the results of the first work phase in co-creating the security concept, fine-tuning it to the rail sector. This will be achieved through an initial workshop held with the consortium expert training developers, followed by a validation workshop with the end-users.

Once validated, the CBRNe rail training program will be delivered in a controlled environment to minimum 40 railway staff coming from companies from at least 4 different EU Member States (MS). In addition, at least one national FR will be trained per MS.

Phase 3: designing and delivering in-situ training exercises

The third technical work phase will consist of the actual implementation and evaluation of the training program by railway end-users in an operational environment to apply the staff's knowledge and skills in simulated incidents at actual railway stations. Five in-situ training exercises will be organised (one by each railway end-user) therefore involving railway staff, firefighters and LEAs. Based on the evaluation results, the training programme and materials will be fine-tuned and updated.

CBRNe4RAIL PROJECT EXPECTED RESULTS

By the end of the project, the rail sector is expected to have access to new, tangible outputs such as:

- Guidelines for improvement of railway security level and response to CBRNe incidents, including how to foster cooperation between the private and public sectors;
- Combined recommendations on a CBRNe security concept for railway and public transport stations;
- Security-by-design checklist that all railways can easily adopt in their preparedness and protection plans;
- Harmonised CBRNe training curriculum and associated training materials, complete with a CBRNe certification programme / label;
- VR training scenario to train railway operators in CBRNe emergency response, supporting the use of information sytems within training activities.

As a long-term impact of the CBRNe4rail project, railway companies will be more resilient and capable to respond to CBRNe emergencies in a prompt and effective manner. Notably, the CBRNe4rail project will set the base for enhancing the cooperation among railways and FRs in responding to CBRNe emergencies. Moreover, the CBRNe label for certification programme for railway companies will pave the way to harmonising CI capabilities in responding to CBRNe risks large beyond the project partners.

CONCLUSION

The CBRNe4rail project uses codesign methodologies to build a CBRNe security concept and training curriculum for the rail sector and also first responders intervening in railway premises. It deploys questionnaires, interviews, workshops, physical visits and reviews of past projects to develop a railway CBRNe security concept, and then develop, pilot and test a CBRNe training curriculum. As part of the security concept, attention will be given to how information systems used in stations and control centres contribute to situational awareness during CBRNe events. Furthermore, the inclusion of VR demonstrates the growing importance of information systems in such preparedness activities. This should help close the gap between CBRNe preparedness and response capabilities in the rail sector all while maintaining the openness and accessibility inherent in public transport, ensuring resilience against the evolving CBRNe threat landscape.

ACKNOWLEDGMENTS

The CBRNe4rail project, Grant Agreement: N° 101190621, is co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

Ciobanu, C., & Burrows, E. (2025). Poland blames sabotage for railway blast on Ukraine delivery line. *Associated Press.* https://apnews.com/article/poland-sabotage-explosion-rail-track-warsaw-97dae3045d4e1ff329780526c6279c0f

Edwards, F. & Goodrich, D. (2014). Exercise Handbook: what Transportation Security and Emergency Preparedness Leaders Need to Know to Improve Emergency Preparedness. *Mineta Transportation Institute, San José*. Report Number: CA-MTI-14-1103. Available at: https://rosap.ntl.bts.gov/view/dot/34153

EUROPOL. (2019). *European Union terrorism situation and trend report (TE-SAT)*. European Union Agency for Law Enforcement Cooperation. Available at: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat

Fernández Díaz, P. & Petersen, L. (2024). Trends for Rail Security Frameworks. *UIC*, ISBN 978-2-7461-3459-1. Available at: https://uic.org/IMG/pdf/trends_for_rail_security_frameworks_final.pdf

Havârneanu, M., Petersen, L., Arnold, A., Carbon, D., & Görgen, T. (2022). Preparing railway stakeholders against CBRNe threats through better cooperation with security practitioners. *Applied Ergonomics*, 102, 103752, ISSN 0003-6870*,* DOI: 10.1016/j.apergo.2022.103752.

Havârneanu, G.M., Petersen, L., De Rosa, B., Arnold, A., Niesse, C., Görgen, T & Bonneau, M. (2024). Design of the IMPRESS training for railway staff and awareness program for the general public. *Médecine de Catastrophe - Urgences Collectives,* Volume 8, Issue 3, 2024, Pages 215-221, ISSN 1279-8479. DOI: 10.1016/j.pxur.2024.07.003.

Luxton, A., & Marinov, M. (2020). Terrorist Threat Mitigation Strategies for the Railways. *Sustainability*, 12(8), 3408. DOI:10.3390/su12083408.

OPCW, 2020. The Sarin Gas Attack in Japan and the Related Forensic Investigation. Available at: https://www.opcw.org/media-centre/news/2001/06/sarin-gas-attack-japan-and-related-forensic-investigation.

Petersen, L., Havârneanu, G.M., Arnold, A., Carbon, D., Görgen, T., Gavel, A., Kroupa, T., & Kardel, D. (2023). Applicability of PROACTIVE recommendations on CBRNe risks and threats to passenger rail and metro sectors. *Journal of Transportation Security*, 16, 4 (2023). DOI: 10.1007/s12198-023-00263-3

Schreiber, D., Bauer, D., Hubner, M., Litzenberger, M., Opitz, A., Veigl, S., & Biron, B. (2023). MOBILIZE—Maintaining the operational safety and security of large railway systems in emergency situations. *Elektrotech. Inftech.* 140, 590–601 (2023). DOI: 10.1007/s00502-023-01154-0

Strandberg, V. (2013). Rail bound traffic – a prime target for contemporary terrorist attacks? *Journal of Transportation Security*, 6(3), 271-286. DOI: 10.1007/s12198-013-0116-0

Strandh, V. (2015). Preparing and responding to mass-casualty terrorist attacks: a comparative analysis of four terrorist attacks targeting rail bound traffic. *Int. J. Emerg. Manag*. 11 (3), 262–281. DOI: 10.1504/IJEM.2015.071709

Strandh, V. (2017). Exploring vulnerabilities in preparedness-rail bound traffic and terrorist attacks. *Journal of Transportation Security*, 10(3), 45-62. DOI: 10.1007/s12198-017-0178-5

UIC. (2026). RAILISA (RAIL Information System and Analyses). Available at: https://uic.org/support-activities/statistics/.

Unger, S., Heinrich, M., Scheuermann, D., Katzenbeisser, S., Schubert, M., Hagemann, L., Iffländer, L. (2023). Securing the Future Railway System: Technology Forecast, Security Measures, and Research Demands. *Vehicles* 2023, 5, 1254–1274. DOI: 10.3390/vehicles5040069

Welch S, Youn S, Nichols A, Na S, Shen R. (2024). Transportation of hazardous material via railroad: Incident investigation and a case study of derailment in 2023. *Process Saf Prog.* 2024;43(3):570-578. DOI:10.1002/prs.12598