*19th WORLD CONFERENCE OF THE ASSOCIATED RESEARCH CENTRES FOR THE URBAN UNDERGROUND SPACE*
*Belgrade, Serbia, November 4-7, 2025.*

ACUUS BELGRADE 2025

***Paper No: 4.10.154***
***DOI: 10.46793/ACUUS2025.4.10.154***

# ADAPTABLE SAFETY CONCEPTS FOR UNDERGROUND RAIL, TRANSIT, AND ROADWAY APPLICATIONS

**Bernd Hagenah, Petr Pospisil**

**Abstract:** This paper discusses the rapid advancements in rail and transit operation, with a focus on the transition towards driverless systems and automatic train operation. This shift necessitates a close integration between rail systems and tunnel safety systems to mitigate risks and ensure passenger safety. The paper proposes a safety concept that goes beyond the traditional approach of relying solely on specific fire and life safety standards. This concept aims to achieve cost savings and higher safety levels by considering additional elements and human factors. The outlined methodology can be adapted for various underground applications, including safety concepts during construction and for road tunnels.

**Keywords:** Safety Concept, Driverless Systems, Rail Systems, Tunnel Safety Equipment

## 1. INTRODUCTION

The landscape of underground rail and transit is undergoing a significant transformation, driven by rapid technological advancements. However, a concurrent revolution in safety philosophy, driven largely by European standards, provides a critical framework for managing this change. The European Technical Specifications for Interoperability (TSI) have spearheaded a move away from purely prescriptive safety rules towards more dynamic, performance-based approaches. Specifically, the TSI for Safety in Railway Tunnels (TSI-SRT) provides a structure for developing comprehensive safety concepts built on modern principles.

This framework enables the application of Quantitative Risk Assessments (QRA), allowing designers and operators to systematically evaluate scenarios, differentiate between acceptable and unacceptable risks, and implement targeted, effective mitigation measures. The power of this approach was demonstrated in landmark European projects such as the Gotthard Base Tunnel, where for the first time, rail operating systems and tunnel safety infrastructure were deeply interconnected. This integration created a holistic safety environment where the tunnel and the train act as a single, coordinated system during an incident.

This paper addresses current gaps in traditional safety philosophies by explicitly targeting four categories of risks often underrepresented in prescriptive standards:

- Operational risks (loss of train control, derailments, unexpected stops in tunnels).
- Technological risks (failure of automation, inadequate system integration across signaling, ventilation, and communications).
- Human-factor risks (absence of onboard staff, passenger misperception of safety, reliance on centralized operators).
- Emerging risks (cybersecurity vulnerabilities, extreme weather impacts, and resilience against prolonged outages).

To mitigate these risks, the proposed safety concept extends beyond traditional fire-centric approaches. It incorporates non-traditional elements such as:

- System integration of vehicle, signaling, and tunnel equipment into a single safety logic.
- Quantitative Risk Assessment (QRA) as a design driver, replacing prescriptive distances and capacities with proven, project-specific safety targets.

- Defense-in-depth layering (Prevention, Mitigation, Evacuation, Rescue) applied consistently across construction, operation, and maintenance phases.
- Consideration of socio-technical factors like public acceptance, user guidance in unattended operations, and AI-supported incident detection.

The methods adopted in this study include risk analysis frameworks (both qualitative and quantitative), comparative benchmarking against reference projects (e.g., Gotthard and Loetschberg Base Tunnels), and systems engineering approaches that integrate civil, rolling stock, and safety equipment into one coherent operational model.

Validation of this approach is achieved through demonstrated precedents from European base tunnels where risk-based concepts have already been accepted by authorities; simulation studies (fire dynamics, evacuation, system response times) verifying safety targets; and lifecycle feedback, where the concept is iteratively updated based on operational data and emergency training and drills.

This paper argues that these types of integrated safety concepts are no longer just best practice but a fundamental requirement for the next generation of transit: driverless and automatic train operation. As the human operator's role is reduced or eliminated, the seamless interaction between the vehicle and its environment becomes the primary guarantor of safety. An adaptable safety methodology is proposed, built on the principles proven in projects like the Gotthard Base Tunnel, that can be applied to the unique challenges of automated systems to achieve higher safety levels and cost-efficiencies. This framework's flexibility also allows its adaptation for safety planning during construction and for road tunnel applications.

## 2. A PARADIGM SHIFT IN EUROPEAN RAILWAY SAFETY

Building on the introduction of the TSI framework, which harmonized safety standards across Europe, this section highlights how these principles now underpin cross-border railway design and safety integration. Previously, the continent's rail network was a fragmented landscape of national systems, each developed in relative isolation. This resulted in significant disparities in technology, operating procedures, and underlying safety requirements. A train crossing a border often had to be compatible with entirely different signaling, power, and safety philosophies, creating what were effectively "technical islands."

This lack of harmonization was a major barrier to a truly integrated European rail network. The introduction of the TSIs established a common basis for both technical equipment and safety concepts. For the first time, there was a shared methodology for defining safety targets and a common language for demonstrating compliance. This forced a convergence of national standards towards a unified, higher benchmark, fundamentally changing how cross-border projects were designed and how system-wide safety was managed. It is this revolutionary, integrated approach that now provides the foundation for tackling the next generation of railway challenges.

## 3. THE CHANGING LANDSCAPE OF RAIL AND TRANSIT OPERATION

The evolution in rail and transit operation is best understood through the internationally recognized framework of Grades of Automation (GoA), outlined in standards like IEC 62290 (see [3]). This scale categorizes systems based on the division of responsibility between human operators and technology. The progression from manual to fully automated systems represent the most significant operational shift in modern railway history.

The transition from GoA1 (manual) to GoA4 (fully unattended) represents a shift in safety responsibility from human operators to integrated systems. While GoA1–GoA2 retain human oversight, GoA3 removes driving duties but maintains onboard staff for emergencies, and GoA4 eliminates all staff presence, relying entirely on system automation.

The global transit industry shows a clear and accelerating trend towards implementing GoA3 and GoA4 systems for new lines and major upgrades. The drivers for this are compelling: increased line capacity through reduced headways, improved service regularity, greater operational flexibility, and lower long-term staffing costs.

However, this transition has profound implications for safety design. In GoA1 and GoA2 systems, the driver serves as the ultimate real-time sensor, capable of identifying and reacting to a vast range of unexpected hazards. In GoA3 and especially GoA4 systems, this human layer of response and mitigation is removed from the vehicle. The responsibility for ensuring safety shifts entirely to the integrated system of the train, the signaling, and the tunnel infrastructure itself.

## 4. LIMITATIONS OF TRADITIONAL SAFETY CONCEPTS

For decades, safety in underground transit has been guided by robust and well-established prescriptive standards, with North America's NFPA 130 being a prominent example (see [2]). These documents have been instrumental in establishing a strong safety baseline, codifying lessons learned from past incidents and creating a common set of requirements for system designers. However, the foundational philosophy of many of these traditional standards is inherently prescriptive, and they were developed around an operational paradigm that assumes the presence of a human driver. As the industry pivots to driverless (GoA3) and unattended (GoA4) operations, the limitations of this approach become critically apparent. The primary weaknesses of these traditional, prescriptive concepts are:

Implicit Reliance on Human Intervention: Prescriptive rules often assume the presence of an onboard operator (driver) to perform crucial functions during an emergency. This includes stopping the train at a designated location, communicating with passengers and the control center, assessing a hazard, and directing an evacuation. In a GoA4 system, these intelligent actions must be fully automated and integrated into the system's logic. A simple prescriptive rule, for example, may not specify how a driverless train should detect a fire and decide whether to proceed to the next station or initiate an immediate stop and evacuation – a decision that is fundamental to a safe outcome.

Rigid, "One-Size-Fits-All" Requirements: Prescriptive standards provide clarity but often lack flexibility, such as specifying a maximum distance between emergency exits (e.g., 250 meters or 800 feet). While this "deemed-to-satisfy" approach is easy to enforce, it lacks adaptability. It does not inherently account for project-specific conditions. For instance, a rigid spacing requirement may be insufficient in a very deep tunnel with long evacuation times, or conversely, it may be overly conservative and unnecessarily costly in a shallow tunnel with a highly advanced ventilation system. This rigidity stifles innovation and prevents the implementation of more effective, performance-based solutions where designers can demonstrate an equivalent or higher level of safety through engineering analysis rather than by simply checking a box.

A Siloed Approach to Safety Subsystems: Traditional standards often specify requirements for various subsystems – such as ventilation, communications, and signaling – in separate chapters or sections. They are treated as independent domains rather than as components of a single, integrated safety system. This is a significant drawback for automated systems, where the emergency response depends entirely on the seamless, coordinated interaction between these very subsystems. A GoA4 train system must communicate its status to the ventilation system to manage smoke, to the signaling system to protect the area, and to the central control system to coordinate the response. A safety concept that treats these as separate entities fails to address the most critical aspect of automated safety.

Therefore, while these standards provide a valuable foundation, relying on them alone for GoA4 systems is insufficient. The shift to driverless operation demands a corresponding shift from a prescriptive, siloed safety philosophy to a holistic, performance-based, and deeply integrated one, as outlined by the TSI framework.

## 5. UNDERSTANDING THE THREATS, RISKS, AND PROTECTION GOALS

To create an applicable safety concept, it is essential to identify the threats, analyze the associated risks, and clearly formulate the protection goals. Without this fundamental analysis, the result is not a true safety concept, but merely a loose collection of regulations that will likely fail to achieve the required level of safety.

### 5.1. Threats and Risks

A systematic identification of threats is required to understand what the system must be protected from. For railway operations, these threats include, for example:

- Collisions: These include collisions with objects on the track (e.g., debris lost by preceding trains), other trains, people, or fixed infrastructure elements (e.g., noise barriers, partition walls, tunnel portals, bridge piers, etc.).
- Derailments: While derailments can have a probability of occurrence similar to that of vehicle fires, their specific dynamics are often given less consideration in the early stages of tunnel safety planning.
- Toxic Gas Release and Explosions: This describes the dangers that originate from freight traffic.
- Fires: Train fires (passenger and freight trains), and fires of technical equipment (e.g., in tunnels).

### 5.2. Protection Goals

To understand what and who must be protected, key protection goals must be defined. The frequently encountered protection goals listed here are typical; they are generally refined and supplemented for the specific project during its course. The examples are:

- Protection of life and limb for all persons (passengers, staff).
- Protection of life and limb for rescue forces, as well as providing environmental conditions that allow them to carry out their work.
- Protection of the infrastructure asset against loss (i.e., avoid collapse).
- Ensuring insurability of the asset.
- Preservation of prestige and brand reputation.
- Rapid resumption of revenue service.
- No negative impact on flora and fauna, both during revenue service and in the event of maintenance or an incident.

### 5.3. Risk Evaluation

For the risk evaluation, it is sensible to proceed as simply and transparently as possible. Generally, two different approaches can be found, a Quantitative Risk Assessment and a Qualitative Risk Assessment.

- Qualitative Risk Analysis: The object being investigated (e.g., a rail tunnel) is compared with a typical (average) rail tunnel regarding its risks.
- Quantitative Risk Analysis: The available data on the operation and the object itself are collected and analyzed. It is important to know and be able to assess the accuracy of the data and assumptions, as well as their limits; for example, Which assumptions were made and under which conditions are they valid?

## 6. SAFETY CONCEPT

To manage the complexities of modern underground transit systems, which involve a deep integration of civil, mechanical, electrical, and systems engineering, an overarching safety strategy is essential. The proven approach championed by the European TSI-SRT (see [1]) provides a uniquely flexible and robust framework. Applications for long rail tunnels are outlined in [5] and [6]. The safety philosophy is built upon a "defense in depth" model, structuring safety measures into four distinct layers. If a hazard breaches one layer of defense, the next is there to contain it. This ensures there is no single point of failure and builds system-wide resilience. The four layers are:

Prevention**:** This is the first and most critical layer. It encompasses all measures taken to prevent an incident from occurring in the first place. For underground systems, this includes passive measures like fire-retardant materials and active measures guided by a formal RAMS (Reliability, Availability, Maintainability, and Safety) process, as defined in standards like EN 50126 (see [4]). This process ensures the high reliability of rolling stock, the implementation of robust maintenance regimes, and the integrity of Automatic Train Protection (ATP) systems to prevent incidents.

Mitigation: If a hazardous event does occur, this second layer aims to limit its consequences and control its escalation. Key mitigation measures include advanced fire and smoke detection systems that can quickly identify an incident's location and intensity. It also includes active fire suppression systems, like water mist or sprinklers, and – most critically – the tunnel ventilation system, which is used to control smoke flow, maintain tenable conditions, and create a clear path for evacuation.

Evacuation: This layer focuses on ensuring passengers and staff can safely perform self-rescue and move to a place of ultimate safety (e.g., an adjacent tunnel or the surface). This is enabled by a combination of passive and active systems, including clear emergency signage, reliable emergency lighting, dedicated walkways, and frequent, easily accessible cross-passages between tunnel bores. The design of the train itself, with wide doors and clear gangways, is also a critical component of this layer.

Rescue: The final layer consists of measures that facilitate effective intervention by external emergency services. Beyond access, this layer ensures responders can work safely. It includes the provision of dedicated access shafts and adits for firefighters, secure and reliable communication systems that work deep underground, high-capacity water supplies (hydrants), and well-defined emergency procedures that are coordinated between the transit operator and local first responders.

By structuring a safety concept around these four layers, designers can ensure all aspects of a potential incident are considered, from its initial cause to its final resolution. This holistic approach is fundamental to ensuring safety in driverless systems where technology, not a human operator, must manage the entire chain of events.

## 7. IMPLICATIONS OF THE MODERN SAFETY CONCEPT ON GOA4 SYSTEM DESIGN AND OPERATION

### 7.1. Impact on Safety Planning and Design

In the planning phase, the safety concept forces a fundamental shift away from simply following a checklist of standards toward a holistic, analysis-driven design process.

- Front-Loaded Safety Analysis: Unlike traditional projects where safety compliance can be a check-box exercise, this modern approach requires comprehensive Risk Assessments at the earliest stages of planning. The results of this analysis directly influence fundamental design decisions, such as tunnel alignment, ventilation system capacity, and vehicle specifications.
- Mandatory System Integration: The concept invalidates the traditional "siloed" approach to engineering. It is no longer possible for the vehicle designers, signaling engineers, and civil/tunnel engineers to work independently. The safety concept requires them to design the train and the tunnel as a single, coordinated system. For example, the vehicle's on-board fire detection system (Mitigation layer) must be designed from the outset to communicate seamlessly with the tunnel's ventilation control system and evacuation times.
- From "Deemed-to-Satisfy" to "Proven Safe": A designer cannot simply state that a fixed egress distance of 250 meters is safe because it's in a rulebook. Instead, they must use the risk analysis to prove that the combination of vehicle fire resistance, smoke control, and evacuation procedures will achieve the defined Protection Goals (e.g., protecting human life ) for that specific project. This allows for—and requires—more innovative and efficient solutions.

### 7.2. Impact on Systems Operation

For a GoA4 system, where there is no driver to manage unforeseen events, the safety concept becomes the operational playbook.

- Automated, Pre-Defined Emergency Scenarios: The entire response to an incident (like a fire or derailment) must be pre-engineered and automated. The "human layer of response" is replaced by a technological one. When a GoA4 train detects a fire, the integrated system must automatically execute a pre-defined sequence: report the incident, activate the appropriate ventilation scenario, adjust the operation of other trains, and provide clear evacuation guidance, all without human intervention.
- Centralized and Enhanced Human Supervision: The role of the human operator is shifted from the vehicle to a central control room. The safety concept dictates that these operators must have advanced tools to supervise the system's health and manage complex, automated emergency responses. Their role changes from direct intervention to high-level supervision and exception handling.
- Maintenance Becomes a Core Safety Function: In this model, the "Prevention" layer is paramount. The reliability of every component underpins the entire safety case. Therefore, the operational phase must include robust, predictive maintenance and continuous system health monitoring to ensure the risk levels calculated during the design phase remain valid throughout the system's life.

## 8. EXAMPLE GENERIC TABLE OF CONTENTS FOR A GENERIC SAFETY CONCEPT

| Chapter | Content | Comment |
|---|---|---|
| 1 | Introduction | Short description of the asset/infrastructure for which the safety concept is developed |
| 2 | Objectives | Compiling the objectives of the safety concept. |
| 3 | Basics | Compile all information about the asset/infrastructure such as: owner, operators, operational concept, geography, |

| | | |
|---|---|---|
| | | temporal and geographical delimitations, status of the project/planning phase, standards, etc. |
| 4 | Threats, Risks and Protection Goals | Compile all reasonable threats and risks, as well as the protection goals and conduct a safety assessment. |
| 5 | Safety Concept | Formulate the safety concept based on the threats, risks, and protection goals, |
| 5.1 | First Priority: Prevention | Describe the prevention methods |
| 5.2 | Second Priority: Mitigation | Describe Mitigation Methods |
| 5.3 | Third Priority: Evacuation | Describe Evacuation Methods |
| 5.4 | Fourth Priority: Rescue | Describe Rescue Methods |
| 6 | Derived Requirements for Operations and Equipment | Based on the safety concept, recommendations are drawn for the operational concept, technical equipment, safety protocols in case of incidents, and training for staff and responders, etc. |
| 7 | Lifecycle Management of the Safety Concept | Based on operational experience, a safety concept must be regularly reviewed and adapted if necessary. Furthermore, training for operations and for responders must also be adapted |

## 9. ADAPTABILITY TO OTHER APPLICATIONS

The strength of the risk-based, four-layered safety concept lies in its philosophical approach rather than a rigid set of rules, making its core principles highly adaptable. While this paper has focused on its application to automated rail systems, the framework's flexibility allows it to be effectively applied to other complex underground environments, such as road tunnels and construction sites.

### 9.1. Application to Road Tunnels

When applied to road tunnels, the methodology remains the same, but the specific inputs change. The initial step is to identify the unique threats and risks associated with road traffic, such as the wider variety of vehicle types, potential for hazardous materials from freight traffic, and the behavior of non-professional drivers. The protection goals, such as the protection of life and the infrastructure asset, are then defined for this specific context.

The four layers of defense are subsequently tailored to these risks:

- Prevention: Measures would focus on traffic management, vehicle monitoring, and robust maintenance of tunnel systems to prevent incidents from occurring.
- Mitigation: This layer is critical and would involve advanced fire detection and powerful ventilation systems designed to manage smoke from various fire sources, controlling the incident's escalation.
- Evacuation: The strategy would focus on providing clear guidance and safe passage for drivers and passengers who are unfamiliar with the environment, using systems like emergency lighting and signage.
- Rescue: This involves ensuring efficient and safe access for external emergency services, a principle shared with rail applications.

### 9.2. Applications to Construction Phases

The safety concept is also a valuable tool for managing risk during the construction phase of a tunnel project. The process again begins with identifying the specific threats, which in this context include risks from construction machinery, temporary electrical installations, and fires involving building materials. The primary protection goal is ensuring the safety of all construction personnel and protecting the partially completed structure against catastrophic loss.

The four-layered strategy would be applied as follows:

- Prevention: This is the most critical layer, enforced through strict site safety protocols, worker training, and management procedures to prevent accidents.
- Mitigation: Measures would include fire detection and suppression systems suitable for a construction environment and plans to contain events like water ingress or localized collapse.
- Evacuation: This requires establishing and maintaining clearly marked and unobstructed escape routes that are adapted as the construction progresses.

- Rescue: The plan must ensure that emergency responders can access a potentially complex and changing site and requires well-defined emergency procedures coordinated with local first responders.

## 10. FUTURE CHALLENGES AND EMERGING CONSIDERATIONS

As automated transit systems evolve, the safety landscape will continue to face new and complex challenges. One key concern is cybersecurity, which becomes critical as GoA4 systems rely heavily on centralized communication, remote diagnostics, and data-driven control. Protecting safety-critical systems against cyber threats is no longer a purely IT issue – it is integral to operational safety.

Another emerging consideration is artificial intelligence (AI) in incident detection and decision-making. While AI holds potential for faster and more nuanced responses, its deployment raises questions of transparency, reliability, and accountability, especially in life-critical scenarios.

Additionally, public trust and user acceptance of fully unattended systems remain a sociotechnical hurdle. Despite the high safety performance of GoA4 systems, passengers may perceive them as less safe without onboard staff – underscoring the importance of user-centered design, transparent communication, and emergency support systems.

Finally, climate resilience must be addressed in future safety planning. Underground infrastructure is increasingly vulnerable to extreme weather events, including flash flooding and power outages. Safety concepts must evolve to incorporate adaptive strategies that ensure system robustness under changing environmental conditions.

## 11. SUMMARY

As the transit industry transitions toward fully driverless (GoA4) operations, traditional prescriptive safety standards – designed around the presence of a human operator – are no longer sufficient. To address this, this paper advocates for the adoption of an adaptable, performance-based safety concept.

This approach is already proven in practice; and successfully applied to major European infrastructure projects, including high-speed lines and landmark tunnels like the Gotthard and Loetschberg Base Tunnels. Rooted in the European TSI framework, this approach uses risk analysis to structure safety measures into a four-layered "defense in depth" model: Prevention, Mitigation, Evacuation, and Rescue. Adopting this framework fundamentally reshapes projects by requiring:

- Deep system integration, treating the train, tunnel and operation as a single, coordinated system from the start of design.
- A shift from rigid rules to "proven safe" solutions validated by risk analysis.
- Automated emergency responses and centralized human supervision in place of on-board staff.

Beyond these established benefits, the contribution of this paper is to clearly identify four categories of risks (operational, technological, human-factor, and emerging) and demonstrate how they can be mitigated through a non-traditional, layered approach. The study introduces methods such as quantitative and qualitative risk assessment, systems engineering integration, and benchmarking against European base tunnel precedents. Finally, the proposed safety concept is validated through simulation studies, proven precedents, and lifecycle feedback mechanisms, ensuring that the approach is not only innovative but also practical and reliable.

This holistic approach provides a robust path to achieving superior safety and efficiency, with a flexible framework readily adaptable to other underground applications.

## 12. BIBLIOGRAPHY

[1] The European Technical Specifications for Interoperability for Safety in Railway Tunnels (TSI-SRT)
[2] NFPA 130, Standard for Fixed Guideway Transit and Passenger Rail Systems.
[3] IEC 62290, Railway applications – Urban guided transport management and command/control systems
[4] EN50126, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[5] Hagenah, B., Cassady, S., Ciancia, M., Zlatanic, S., Vetsch, H-P., Safety Challenges in Long Rail Tunnels, North American Tunneling Conference (NAT), United States, 2021
[6] Hagenah, B., Cassady, S., Pospisil, P., Vetsch, H.-P., Ockajak, R., Safety in Long Rail Tunnels, UC (ITA - AITES), Prague, 2023