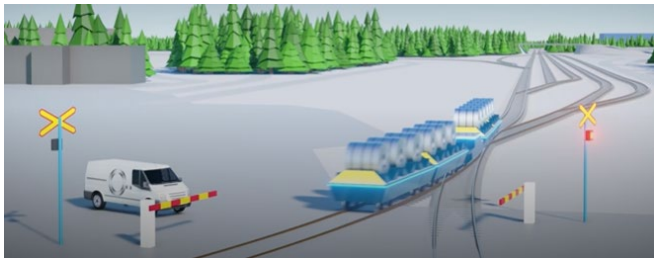
RESEARCH REPORT

VTT-R-00375-23



Safety concepts to enable autonomous train operations in semi-restricted industrial areas

Authors: Risto Tiusanen, Risto Öörni

Confidentiality: VTT Public

Version: 3.10.2023

VTT

beyond the obvious

Report's title Safety concepts to enable autonomous train operations in semi-restricted industrial areas	
Customer, contact person, address	**Order reference**
Project name Proxion autonominen juna	**Project number/Short name** 131001 / BF-Proxion
Author(s) Risto Tiusanen, Risto Öörni	**Pages** 26/10
Keywords Autonomous train, safety, safe path, rail traffic control	**Report identification code** VTT-R-00375-23

Summary

The work performed has been enabled by Business Finland, which provided funding for a research project 'Autonominen juna -kehityshanke' - VTT (45715/31/2020), which included collaboration with Proxion Oy, Electric Power Finland Oy, and Steel Wheel Oy for the development of autonomous train in industrial sites. Typically, these sites have small internal rail network for low-speed transportation of raw materials, semifinished goods, and final products. Since most of the traffic within these sites is caused by the trucks and trains of the industrial site itself, and since the vehicles and persons from outside would need permission to enter, many of such sites can be described as semi-restricted.

The study considers other (manual) train traffic in semi-restricted industrial areas but does not consider the driving of an autonomous train on the public main line. The study had two main research objectives. The first objective was to identify and analyse safety risks related to the daily operation of the autonomous train on its route in a semi-restricted industrial area: charging / refuelling station, loading / unloading places, railway switches and level crossings. The second objective was to define concepts to secure the path of an autonomous train and principles to control level crossings and their safety-related systems in three different train traffic control concepts:

- An autonomous train has a static local permit in a semi-restricted industrial area
- The autonomous train has a dynamic local permit in a semi-restricted industrial area
- The rail yard traffic control sets the access permit for the autonomous train in a semi-restricted industrial area

This report summaries the analysis of new safety risk related to autonomous train operations in semi-restricted industrial areas, including the concepts for safe pathways and safe level crossing controls for autonomous train operations.

Confidentiality	VTT Public

Tampere 3.10.2023

Written by	**Reviewed by**
Risto Tiusanen Senior scientist	Pertti Peussa Principal scientist

VTT's contact address
Visiokatu 4, PL 1300, 33101 TAMPERE

Distribution (customer and VTT)

Business Finland: (PDF)
VTT: Archive (Print copy + PDF); Pertti Peussa, Risto Tiusanen, Risto Öörni, Timo Malm (PDF)
Proxion Oy: Kimmo Kolehmainen, Tomi Lankinen and Reijo Viinonen (PDF)
Electric Power Finland Oy: Jani Tupitsa, Kia Tupitsa and Heikki Niemelä (PDF)
Steel Wheel Oy: Timo Saalasti (PDF)

Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date:	3 October 2023
Signature:	Pilli-Sihvola Eetu 91293002J Digitally signed by Pilli-Sihvola Eetu 91293002J Date: 2023.10.03 10:39:18 +03'00'
Name:	Eetu Pilli-Sihvola
Title:	Research Manager

Contents

1. Introduction

Autonomous train is a concept, which is getting increasing attention. Some examples already exist in purpose-built or isolated rail network, e.g., AutoHaul™ in Western Australia for iron ore transportation, SkyTrain in the Vancouver region in Western Canada for rapid transit, and several automatic subways in large cities.

The work performed has been enabled by Business Finland, which provided funding for a research project ‘Autonominen juna -kehityshanke’ - VTT (45715/31/2020), which included collaboration with Proxion Oy, Electric Power Finland Oy, and Steel Wheel Oy for the development of autonomous train in industrial sites. Typically, these sites have small internal rail network for low-speed transportation of raw materials, semifinished goods, and final products. Since the majority of the traffic within these sites is caused by the trucks and trains of the industrial site itself, and since the vehicles and persons from outside would need permission to enter, many of such sites can be described as semi-restricted.

This report summaries the analysis of new safety risk related to autonomous train operations in semi-restricted industrial areas, including the concepts for safe pathways and safe level crossing controls for autonomous train operations.

2. Objectives and Limitations

The aim of this study on safety concepts to enable autonomous train operations in semi-restricted industrial areas was to answer the following two research questions:

- How to ensure safe fully automatic material transfer and organization concepts in a partially or completely closed industrial area, when there are a) one b) several autonomous trains?
- How to ensure safe functionality of the ‘virtual coupling’ concept together with access control and collision prevention in a closed area?

This study had two main research objectives. The first objective was to identify and analyze safety risks related to the daily operation of the autonomous train on its route in a semi-restricted industrial area: charging / refueling station, loading / unloading places, railway switches and level crossings.

The second research objective was to define concepts to secure the path of an autonomous train and principles to control level crossings and their safety-related systems in three different train traffic control concepts:

- An autonomous train has a static local permit in a semi-restricted industrial area.
- The autonomous train has a dynamic local permit in a semi-restricted industrial area.
- The rail yard traffic control sets the access permit for the autonomous train in a semi-restricted industrial area.

This study considers other (manual) train traffic in semi-restricted industrial areas but does not consider the driving of an autonomous train on the public main line.

3. Methods

3.1 Discussions with company experts

Background information about the concept of an **autonomous train (AutoCar)** as well as information and limitations about the case system under study and its operating environment were collected in discussions with Electric Power Finland Oy and Proxion Oy.

Jani Tupitsa, Kia Tupitsa and Heikki Niemelä from Electric Power Finland Oy and Pertti Peussa, Risto Öörni and Risto Tiusanen from VTT participated in the discussion with Electric Power Finland Oy on 8 December 2022. Kimmo Kolehmainen and Tomi Lankinen from Proxion Oy and Pertti Peussa, Risto Öörni and Risto Tiusanen from VTT participated in the discussion with Proxion Oy on 15 December 2022.

3.2 Preliminary risk analysis

The safety risk analysis of the AutoCar concept was conducted in spring 2023 at the system level by using the Preliminary Risk Analysis (PHA) method (Vincoli, 2006).

The aim of the risk analysis was to identify the most important hazards and foreseeable exceptional situations related to the operation of an autonomous train and to assess safety risks caused by them. The study was done in a conceptual level focusing on the autonomous driving and of the AutoCar train unit. The detailed technological aspects of the AutoCar unit, its cargo, or the infrastructure are excluded from this study.

Daily operation of the autonomous train was divided in the following phases in the analysis:

- arriving and leaving the charging or refueling station
- moving autonomously on the tracks within the industrial area
- arriving and leaving the loading place and the unloading place
- arriving and leaving railway switches
- arriving and leaving level crossings

The main safety hazards identified for the analysis were focused on the autonomous driving. Among other the following hazards were analyzed:

- overrunning a person
- crushing a person
- collision with a vehicle, collision with a train
- collision with another obstacle on the track, e.g., material or an animal
- derailment from the track or from railway switch
- falling cargo from AutoCar
- fire hazards related to the diesel engine, the fuel, or refueling station
- electrical hazards or electrical fire hazards related to the battery or charging station

Among others the following possible causes for a hazardous situation were considered in this study:

- unexpected start-up or direction of movement of the autonomous train
- failure of rail traffic control or train control system, e.g., wrong speed, over speed, positioning errors
- other system faults affecting safe operation
- human errors or carelessness of rail traffic control operators
- human errors or carelessness of vehicle drivers, workers in the area, pedestrians, or cyclists
- system faults affecting the transportation process or train traffic, e.g., error in AutoCar's task control, wrong loading or unloading place

Estimation of the severity of the safety effects and the magnitude of the losses were done by using four categories of severity:

- death of a person/persons, permanent injury, reportable injury
- direct material damage
- disruption/interruption of the transportation process
- disruption/interruption of other train traffic/vehicle traffic

Estimation of the probability of hazardous situations or events in daily operation was done by using three categories:

- rare
- possible
- probable

Assessment of the magnitude of the risks (risk = probability X severity) was done by using three categories and color codes highlighting them (Figure 1).

High = Unacceptable risk. Changes must be done before the use of the system.
Medium = Undesirable risk. Changes must be made to minimize the risk.
Low = Tolerable risk. Changes must be made to minimize the risk if it is possible.

Figure 1. The three categories assigned for the magnitudes of the risks.

It is important to notice that this rough PHA methodology used in this study for hazard identification and categorizing risks is a methodology that has been used in early conceptual design phase of autonomous machinery and other industrial systems (see e.g., Tiusanen, 2014). In the future, when autonomous train applications are planned and commissioned for semi restricted industrial areas and track yards, it is important to follow and apply the European train safety procedures and risk assessment principles.

European Railway Agency has published 2008 ‘Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive’ (Anon, 2008). The following EN standards define requirements for performing RAMS management (Reliability, Availability, Maintainability and Safety) and for the demonstration of reliability and safety in railway applications:

- EN 50126-1:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
- EN 50128:2011 Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems
- EN 50129:2018 Railway applications - Communication, signaling and processing systems - Safety related electronic systems for signaling
- EN 50159:2010/A1:2020 Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems

VTT’s team ,conducting the safety risk analysis of the AutoCar concept was Risto Tiusanen, Timo Malm and Pertti Peussa.

3.3 Concepts to secure the path of an autonomous train

The concepts to secure the path of an autonomous train and principles to control level crossings and their safety-related systems were defined by Risto Öörni in three different train traffic control principles:

- An autonomous train has a static local permit in a semi-restricted industrial area.
- The autonomous train has a dynamic local permit in a semi-restricted industrial area.
- The rail yard traffic control sets the access permit for the autonomous train in a semi-restricted industrial area.

4. Background information

Discussions with Electric Power Finland Oy and Proxion Oy gave a good starting point for this study and gave information of ongoing activities and future needs in this context. In this chapter the main topics and views are summarized from the discussions.

Class II traffic areas have been thought of as the operating environment for the automated solution, which means both rail yards and less trafficked track sections from either the public or private side. Until now, the starting point has been to reserve the entire area for automatic traffic. Any outside train arriving in the area is scheduled and, if necessary, reserved operating time for a limited number of tracks. When leaving a private track and switching to a public track network, a departure permit, which can be applied for via voice radio, is required for an automatic train unit to reserve a safe passageway. This is now the practice in second-class traffic areas.

In the current situation, the "Finnish Transport Infrastructure Agency's (FTIA) " traffic control does not have the possibility to issue a start permit in electronic form. Official permission is therefore verbal, but confirmation can sometimes come by email. The development of local access permit communication has not been among the goals of this project. In the next automation development phase, novel solutions will also be needed from the direction of the Finnish Transport Infrastructure Agency and Traficom. In the future, the goal is to operate with the automatic train also on tracks owned by the Finnish Transport Infrastructure Agency, so no longer only on private track areas. When operating in the state rail network, you must also apply for rail capacity. Access reservation alone is not enough. The Finnish Transport Infrastructure Agency participates in developing solutions for operation when moving in class II traffic areas and private areas. If several automatic train units operate in the same area, the complexity of the system increases.

In heavily trafficked areas, there should also be warning devices at level crossings located in industrial areas. When reserving a passageway for a train, the level crossing must also be considered, whether it has booms or not. Proxion Oy's current concept uses an axle counter. Axle calculation does not consider whether it is an automatic train or a regular train. Based on the current automatic train concept it is assumed that the automatic train is better integrated into the track infrastructure than the VR freight train.

There may be other rail traffic in the factory area. An external user (e.g., coming from a public track) can also drive deep into the automatic train area. In other words, the connection surface to the public railway is not limited to a short section of railway. The railway switch may need the possibility of local control for an external operator, i.e., turning the railway switch with a push button locally at the railway switch. How to ensure a safe passage in this case? The starting point in the concept is that the automatic train avoids other rail traffic.

The requirements related to the local permit are defined in the 'Safety regulations for train traffic and shift work' (Anon, 2021)

A local permit for one destination may only be issued to one person at a time. Those who have received a local permit must notify traffic control of the return of the local permit. No other traffic may be directed into the area affected by the local permit, unless the traffic has been agreed with the person who received the permit.

If other units need to operate in influence of the local permit (=over railway switches or track closures belonging to the local permit), traffic control must contact the person who has obtained the local permit and verify whether other units can operate in effect of the local permit. If this is possible, permission can be given for exchange work to other units. After this, the person who received the local permit and the shift work units agree on turning the railway switches in the area affected by the local permit.

Traffic control informs the person with a local permit of the units' IDs.
When requesting a local permit, the required local permit groups or the tracks to be used are indicated. Traffic control determines the required local permit groups based on this information.

Railway switch turning devices are not "foolproof"; e.g., a stone that has fallen between the moving parts of the railway switch and the rails can prevent the railway switch from working. Snow can also get packed between the moving parts. Up to 16kW of heating power is used to melt the switches of the main railway lines.

The railway switch control system can fail. If the power goes out at the railway switch when the route is reserved, and the traffic is stopped. The automatic train must be able to react to a failure situation. safe Fail-safe principles should be applied in the system level. The railway switch could turn to wrong direction. The location information of the automatic train must be verified to notice this type of failures. Now, the ‘control of the switch being free’ function indicates in which direction the switch was driven over.

One operational risk of an automatic train is positioning errors. The positioning should be based on at least two different technologies. For example, landmark positioning with sensors is one complementary method. (Traffic signs can be erected in the yard to provide enough features for reliable positioning. However, the freight trains that happen to be on both sides of the automatic train limit the observation field to a narrow one). The axle counter at a railway switch is one additional way to confirm the location (the information from the railway switch is whether the counter is active or not).

5. Case system description

The autonomous train concept and its operating environment under study were defined together with Proxion Plan Oy and Electric Power Finland Oy.

5.1 Operating environment

The following aspects describe and characterize the concept of the autonomous train system and the operating environment in a semi-restricted industrial area. See also Figures 2, 3, 4 and 5.

- The area is a semi-restricted industrial area or a railway yard including loading and unloading places, tracks and railway switches, roads, and level crossings.
- There can be other rail traffic and there is other traffic in the area such as cars, trucks, work-machines, cyclists, and pedestrians.
- There can be a rail traffic control, level crossings control, railway switches control and autonomous train control system in the semi-restricted industrial area.
- There can be rail traffic controller, remote train operator, supervisor of the autonomous train.
- Options for reserving a passageway to the AutoCar are locally by the manual user, dynamically by the AutoCar system or automated by the rail traffic control system.

- In this concept the AutoCar train unit has a locomotive and wagons
- There must be a wireless communication system available in the operating area.

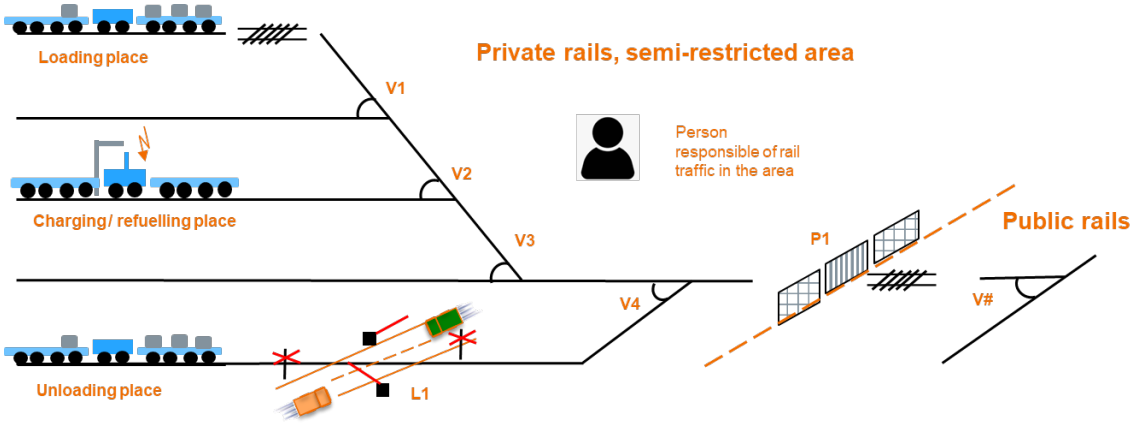


Figure 2. Outline of the rail yard in the semi-restricted industrial area in this study.

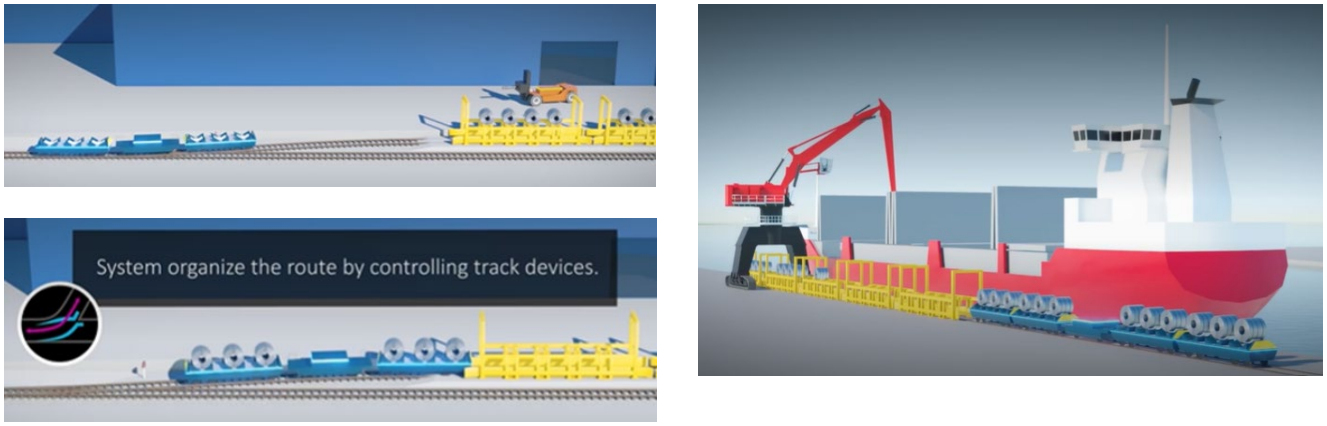


Figure 3. Illustrations of loading and unloading places in the Proxion concept (Anon, 2022).

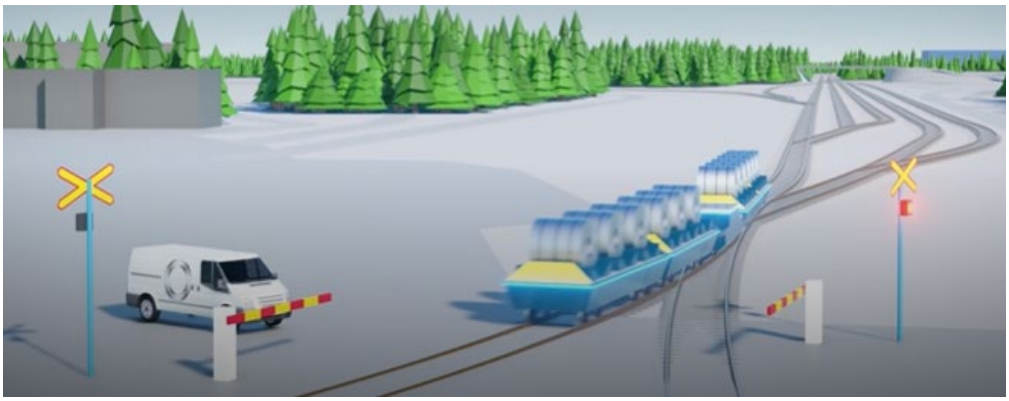


Figure 4. Illustration of a level crossings in the Proxion concept (Anon, 2022).

Figure 5. An illustration of rail switches in the Proxion concept (Anon, 2022).

5.2 Definition and characteristics of the AutoCar

The following aspects characterize the AutoCar system in the Proxion concept (Anon, 2022).

- AutoCar is a battery driven train. Its battery capacity is about 200 kWh.
- The locomotive unit has two electric motors, each of them about 100 kW.
- The traction capability of the locomotive unit is about three hundred tons.
- The AutoCar train unit includes 1 – 4 wagons, each of them about ninety tons. In this concept the configuration is fixed. This means there is no need for shunting work with the wagons (Figure 6).
- AutoCar's speed is limited to 20 km/h and its working distance is up to 20 km:
- AutoCar has onboard sensors such as a radar, thermal and visual cameras, and their fusion.
- Positioning of AutoCar is based on D/RTK GNSS and inertia information, and reference points.
- AutoCar's communication is based on wireless communication networks.

- AutoCar operates on fully digitalized tracks.
- AutoCar's control System is an automatic train operation (ATO) based on European Train Control System (ETCS). It is a subset of it including only relevant parts needed on private tracks.
- System is used on private tracks on which SIL requirements are not as high as on public tracks.

Figure 6. An outline of the autonomous train unit in the Proxion concept (Anon, 2022).

6. Results

6.1 Safety risks related to autonomous operations

The aim of the risk analysis was to identify the most important hazards and foreseeable exceptional situations related to the operation of an autonomous train and to assess safety risks caused by them. Description of the main safety risks and proposals for safety measures are structured according to the assessed risk categories: high, medium, and low risks. The detailed analysis results are presented in the Risk analysis EXCEL document in Appendix 1 and the summary of the proposed safety measures are presented in Appendix 2.

6.1.1 High risks identified in the analysis

AutoCar runs over a person

AutoCar runs over a person who is standing or walking on the tracks, or a person is walking across the tracks in the marked crosswalks, in a level crossing, loading, or unloading places or in a random location on the tracks (Figures 7 – 10). A person could come unexpectedly from behind a building, a fixed structure or behind a vehicle to the tracks. It could also be possible that the person does not notice the coming AutoCar.

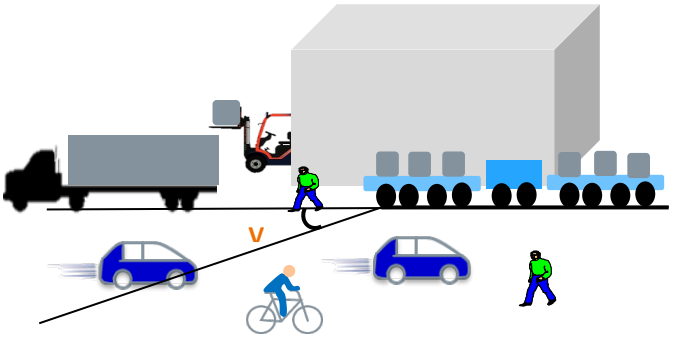


Figure 7. Autocar moving autonomously among other traffic.

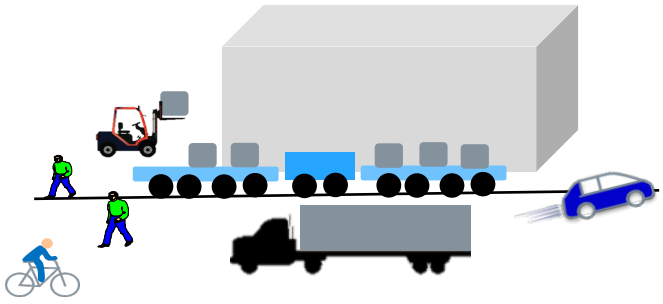


Figure 8. Outline of a loading or an unloading place.

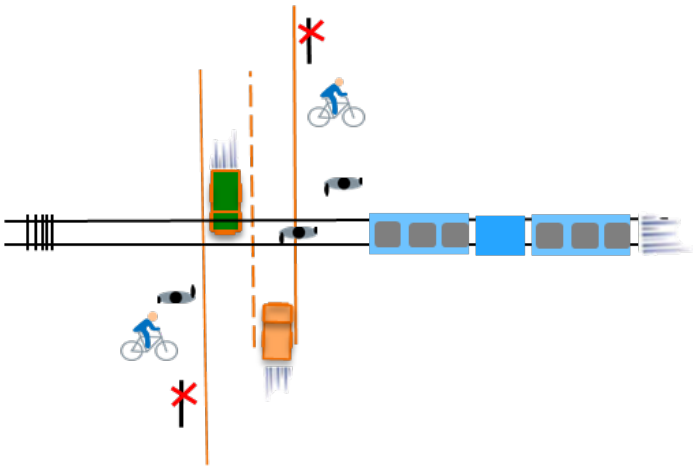


Figure 9. A level crossing without traffic lights and level crossing safety system.

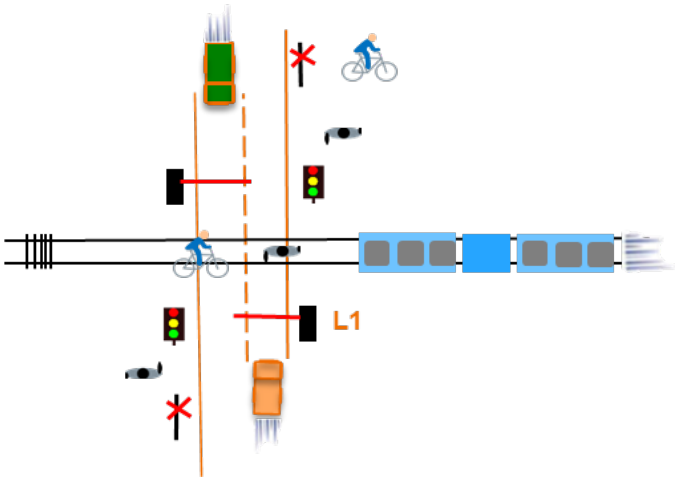


Figure 10. A level crossing with traffic lights and level crossing safety system.

To prevent the overrunning accidents or minimize the risk of overrun the following safety measures are proposed:

- The speed of the AutoCar must be slow, max. 20 km/h.
- AutoCar's safety system must be capable of detecting a pedestrian or cyclist on the tracks and near the tracks from such a distance that it is able to stop under all circumstances. Performance and functional safety (SIL / PL) requirements for the AutoCar control system must be defined.
- Failure in the AutoCar's safety system, its control system or in the communication system must stop the train and prevent the train from moving. Functional safety (SIL / PL) requirements for the safety related parts of the AutoCar control system must be defined.
- AutoCar must have audible and visual warning signals when it is moving.
- Level crossings should have safety-related systems preventing access to the tracks when the automatic train is moving through the crossing. Functional safety (SIL / PL) requirements for the level crossing safety systems must be defined.
- Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.
- Walking on the tracks must be prohibited and there must be marked walkways and warnings of the automatic train.
- Making the track more visible and directing light traffic (pedestrians and cyclists) to certain routes

AutoCar crushes a person

AutoCar crushes a person (e.g., against a structure) in a charging or refueling station or in a loading or in an unloading station (Figure 11). The person is standing near the tracks, or a person could come unexpectedly near the tracks from behind a structure or behind a vehicle. It could also be possible that the person does not notice the coming or leaving AutoCar when working in the station area.

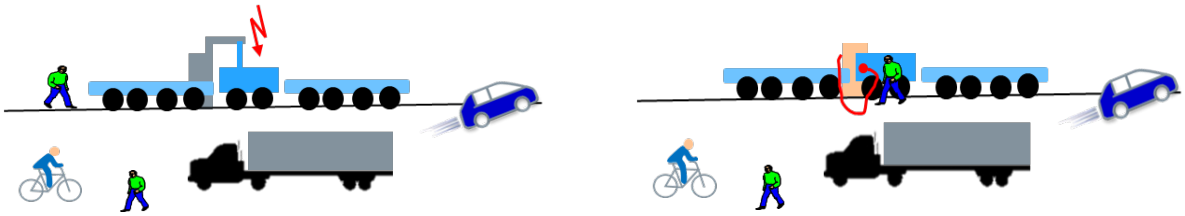


Figure 11. Outlines of charging and refuelling stations.

To prevent the crushing accidents or minimize the risk of crushing at the stations the following safety measures are proposed:

- The speed of the AutoCar must be slow near the stations.
- AutoCar's safety system must be capable of detecting a person near the tracks from such a distance that it is able to stop under all circumstances at the stations to prevent an accident.
- Failure in the AutoCar's safety system, its control system or in the communication system must stop the train and prevent the train from moving.
- Unexpected moving of the AutoCar must be prevented at the stations.
    - Functional safety (SIL / PL) requirements for the safety related parts of the AutoCar control system
- AutoCar's reliable positioning to a right place must be ensured.
    - Is the current positioning technology based on D/RTK GNSS, inertia and reference points reliable enough?
- AutoCar must have audible and visual warning signals when it is moving.

- Hazardous points at the stations station must be safeguarded and access to hazardous areas near the tracks must be prevented.
- In the design of loading and unloading docks, the risks of crushing must be considered.
- Possible crushing hazards should be considered in vehicle parking arrangements.
- Persons working or visiting the station area must follow the safety rules and instructions.

Falling cargo from AutoCar

A heavy cargo falls from the AutoCar wagon at a loading or unloading station, at a level crossing or near the walkways or vehicle routes.

To prevent the crushing accidents or minimize the risk of falling cargo the following safety measures are proposed:

- The workers must follow safety instructions for loading and unloading and instructions for ensuring the cargo.
- The workers should inform if they see anything out of the ordinary related to the AutoCar or its cargo.
- There must be marked walkways and warnings of automatic train.
- Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.

Electric shock and electrical fire hazard

A maintenance person gets an electric shock while servicing AutoCar or the charging station.
Electric batteries or electric circuits in AutoCar catches fire

To prevent the electrical hazards the following safety measures are proposed:

- The AutoCar electrics and the charging station must fulfill electrical safety requirements.
- Maintenance persons must follow the safety rules and instructions (SFS 6002:2015 + A1:2018:en Safety at electrical work).
- AutoCar could be equipped with an automatic fire extinguisher system.

6.1.2 The medium risks identified in the analysis

AutoCar collides a vehicle

AutoCar collides a vehicle (car, forklift truck, lorry) or its trailer in the level crossing when a vehicle is moving across the tracks or a vehicle or its trailer is stopped on the tracks in the level crossing. It could be possible that the vehicle driver does not notice that the AutoCar is coming to the level crossing (Figure 12).

AutoCar collides a vehicle or its trailer on the tracks (not in a level crossing) because a vehicle or its trailer is parked on the tracks or a vehicle or its trailer is stopped on the tracks. It could be possible that the vehicle driver does not know or notice that the AutoCar is using the track (Figures 13 and 14).

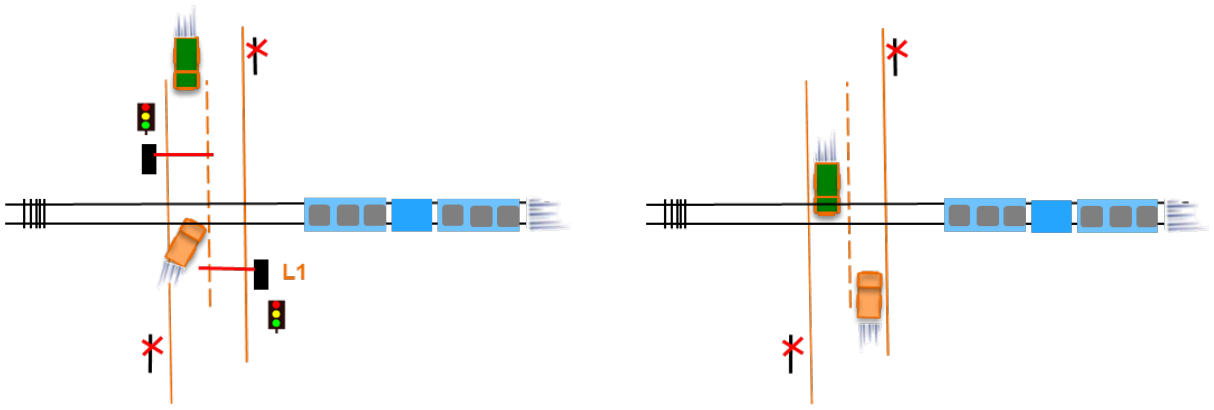


Figure 12. A level crossing with and without traffic lights and level crossing safety system.

Figure 13. Collision with a vehicle too close to the tracks.

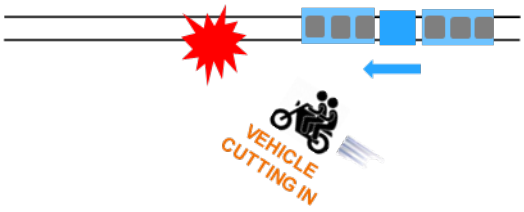


Figure 14. Collision with a vehicle failing to cross tracks before the approaching train unit at a random place.

To prevent collisions in the level crossings the following safety measures are proposed:

- AutoCar's safety system must be capable of detecting an obstacle on the tracks and near the tracks from such a distance that it is able to stop under all circumstances to prevent an accident.
- Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving.
- AutoCar must have audible and visual warning signals when it is moving.
- Vehicle drivers must follow the traffic rules and safety instructions in the industry area.
- Level crossings should have safety-related systems preventing access to the tracks when the automatic train is moving through the crossing.
- The rail traffic control system must ensure safe passage through the level crossings for the AutoCar.
- See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2).

To prevent collisions on tracks in other places other than level crossings the following safety measures are proposed:

- AutoCar's safety system must be capable of detecting an obstacle on the tracks and near the tracks from such a distance that it is able to stop under all circumstances to prevent an accident.
- Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving.
- Directing vehicle traffic and light traffic to safe routes.
- Vehicle drivers must follow the traffic rules and safety instructions in the industry area.
- There must be warnings of automatic train.
- AutoCar must have audible and visual warning signals when it is moving.

A vehicle collides AutoCar

A vehicle collides AutoCar when it is stopped in the loading or unloading station or in the charging or refueling station or when AutoCar is moving in the level crossing (See Figures 8, 11 and 12).

To prevent collisions with AutoCar the following safety measures are proposed:

- Vehicle drivers must follow the traffic rules and instructions in the industry area.
- There must be marked vehicle routes and warnings of automatic train.
- Area maintenance must ensure that access roads, level crossing areas and loading/unloading areas are safe to drive, especially in winter conditions.

AutoCar collides a train

AutoCar moves on the same track where another train is moving or stopped and collides the train (Figure 15). AutoCar collides a train which is stopped in a wrong place at a railway switch (Figure 16). AutoCar moves to a railway switch at the same time with a train (Figures 17 and 18).

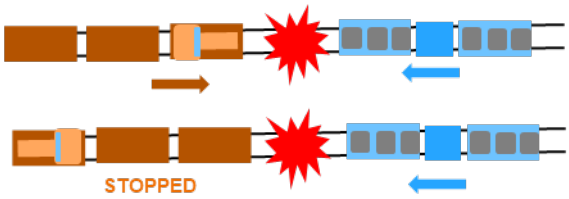


Figure 15. Collision scenarios with another train on the track.

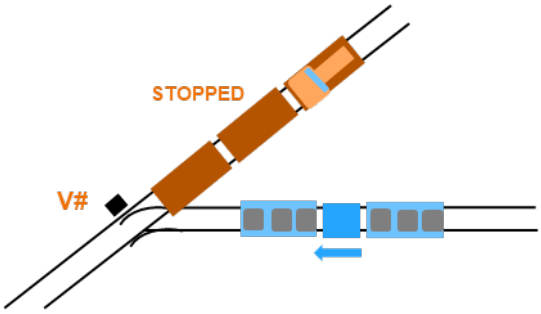


Figure 16. Collision scenarios with a train stopped in a wrong place at a railway switch.

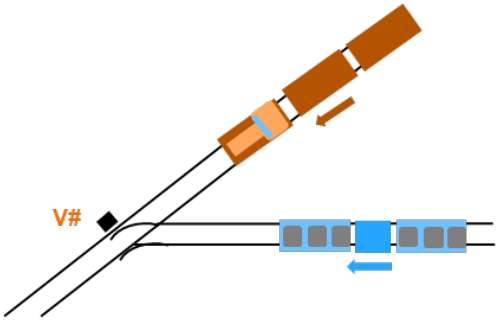


Figure 17. AutoCar and a train are moving to the same railway switch.

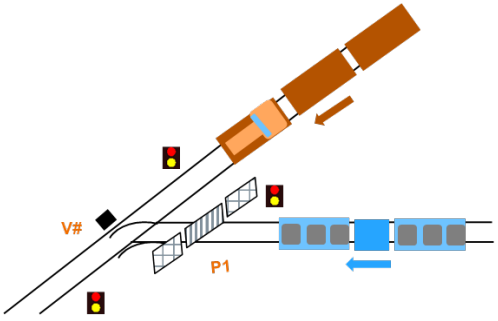


Figure 18. AutoCar and a train are approaching the rail switch to public rail.

To prevent collisions with AutoCar the following safety measures are proposed:

- Positioning of a train to a right place must be ensured at the railway switches.
- Failure in the AutoCar's control system or in the communication system must stop the AutoCar and prevent the AutoCar from moving.

- See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2).

A train collides the AutoCar

A train moves to the same rails where the AutoCar is moving or is stopped and collides the AutoCar (Figure 19). A train moves to a railway switch at the same time with AutoCar (Figure 17 and Figure 18).

A train collides AutoCar which is stopped in a wrong place at a railway switch (Figure 20).

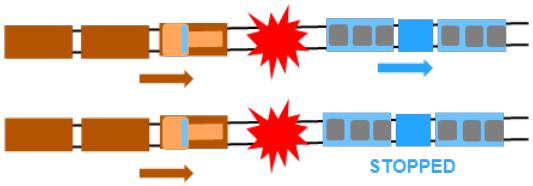


Figure 19. Collision scenarios where a train collides AutoCar on the track.

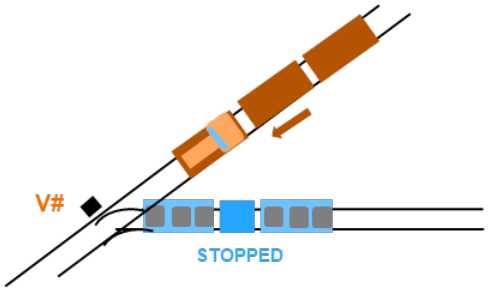


Figure 20. Collision with AutoCar stopped in a wrong place at railway switch.

To prevent collisions with train the following safety measures are proposed:

- AutoCar's positioning to a right place must be ensured at the railway switches.
- Failure in the AutoCar's control system or in the communication system must stop the train and prevent the train from moving.

- See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2).

An object falls from AutoCar

An object falls from the AutoCar wagon at a loading or unloading station, at a charging or refueling station, at a level crossing or near the walkways or vehicle routes.

To prevent the crushing accident or minimize the risk of falling objects the following safety measures are proposed:

- The workers must follow safety instructions for loading and unloading and instructions.
- The workers should inform if they see anything out of the ordinary related to the AutoCar.
- There must be marked walkways and warnings of automatic train.
- Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.

6.1.3 Low risks identified in the analysis

The AutoCar collides an unexpected (heavy) obstacle on the rails

A heavy object has been left on the rails or has dropped e.g., from a forklift or from a truck on the rails and the AutoCar collides with it.

To prevent collisions with an object on the track the following safety measures are proposed:

- The AutoCar's safety system should be capable to detect an obstacle on the rails from such a distance that it is able to stop the AutoCar to avoid a collision.
- The workers must follow safety instructions for loading and unloading and instructions.
- The workers should inform if they see anything out of the ordinary on the track
- Persons working or visiting the area must follow the safety rules and instructions in the industry area.

Derailment hazards due to the material on the tracks

There can be ice, a lot of snow, sand, debris, or extra material on the tracks. The AutoCar drives over the material and the train wheels can come off the rails and train can derail and crash.

To prevent derailment or minimize the risk of derailment due to the material on the tracks the following safety measures are proposed:

- Area maintenance must ensure that tracks are safe to drive, especially in winter conditions.

6.2 Safe path securing concepts for semi-restricted areas

The concepts of securing a path for AutoCar automated train and controlling level crossing safety equipment in an industrial area were studied based on three different train traffic control principles:

- The AutoCar has a static local permit for operation in a semi-restricted industrial area
- The AutoCar has a dynamic local permit for operation in a semi-restricted industrial area
- Rail yard traffic control system sets a train path for AutoCar unit in a semi-restricted industrial area.

6.2.1 Static local permit for operation in a semi-restricted industrial area

In the first option, the AutoCar has a static local permit for operation in a semi-restricted industrial area (Figure 21). When AutoCar is in operation, the area is closed for other railway traffic. In other words, (1) entry of other trains or other railway equipment to the area is not allowed when AutoCar is in operation and (2) AutoCar must be in passive state when the area is open for other railway traffic.

Entry of other trains or railway equipment to the operation area of AutoCar can be prevented e.g., with a locked gate. In a solution based on mechanical locks, there would be only a single key for operating the

AutoCar power switch and the lock in the gate. Inserting the key and turning it in the lock would be required to open the gate or to set AutoCar to active state. The lock of the AutoCar power switch would allow removing the key only in a position in which the AutoCar is in a passive state (with power switched off). The lock in the gate would allow removing the key only when the gate is closed and locked. In addition to opening and closing the gate, a human operator will set a path for the AutoCar, e.g., by turning the switches on the railyard or other industrial area.

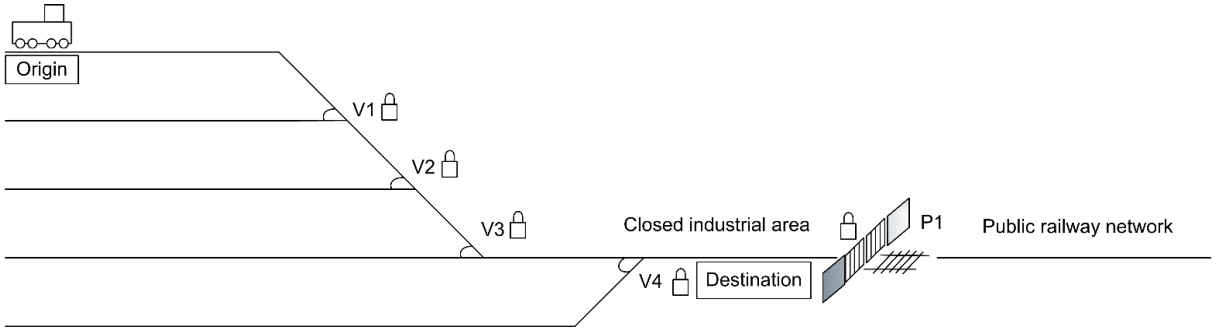


Figure 21. The AutoCar has a static local permit for operation in a closed industrial area.

In case of the static local permit, switches are locked to their positions by a human user, and they are not controlled by an automatic or manual rail yard traffic control system. Therefore, the route used by the automated unit must remain static over time. In other words, the AutoCar must be able to travel between the locations used for loading, unloading, charging, and parking without a need to turn any switches on the railyard. The human user will set the route for the AutoCar, e.g., by manually turning the switches on the rail yard and locking them to the correct position.

Before the AutoCar can start movement, it needs to receive a permission. The permission will be given by communicating the “start” signal to the AutoCar. The “start” signal will be given when the following conditions exist:

- loading or unloading of the AutoCar has been completed
- entry of other trains to the semi-restricted industrial area has been prevented (e.g., gate P1 between the area and the public railway network is locked)
- switches V1, V2, V3, V4 … VN have been set to correct position establishing the route for the AutoCar.

If any level crossings exist in the area, train detection by the level crossing safety equipment will be based on track circuits. In Finland, solutions based on axle counters are not recommended for use in areas where shunting operations are conducted. The train detection technology used in level crossing equipment has also to be interoperable with other trains and railway equipment (e.g., work machines) which may enter the area when the gate is open and the AutoCar is not in use.

In case of the static local permit described above, the following key assumptions were made:

- The AutoCar has a single route which can be travelled both ways without turning any switches.
- Only one AutoCar is in use at a time.
- No visiting units will be operating in the area when the AutoCar has power switched on.
- Level crossing safety equipment in the area will operate as isolated units and use track circuit for train detection.
- Level crossing safety equipment will not be installed in areas used for storing rolling stock.
- Level crossing safety equipment will not be installed in an area used for shunting operations not reaching the level crossing, unless the level crossing safety equipment has an elimination function operated by a human user during shunting operations.

6.2.2 Dynamic local permit to operate in a semi-restricted industrial area

In the second operational concept, the AutoCar requests a dynamic local permit to operate in a semi-restricted industrial area (Figure 22). The dynamic local permit may be possessed either by the AutoCar or by the human user responsible for rail yard traffic control in the area. The dynamic local permit covers the semi-restricted industrial area and has a defined start time a defined end time. Before starting to move, the AutoCar will request from a dynamic local permit from the local permit management system.

In the example presented in Figure 22, a dynamic local permit will be granted to the AutoCar to operate if all following conditions are fulfilled:

- The human user (rail yard traffic controller) has not requested a local permit for the time period covered by the permit request.
- The human user (rail yard traffic controller) has no valid dynamic local permit for the time period covered by the permit request.
- Switches V1, V2 ja V3, V4 … VN have been set and locked to the positions corresponding the route of the AutoCar.
- Entry of visiting units to the area has been prevented (in the example: gate P1 is in locked state).
- Level crossing L1 is ready to operate (the level crossing is not in state “fault” or “unknown”).

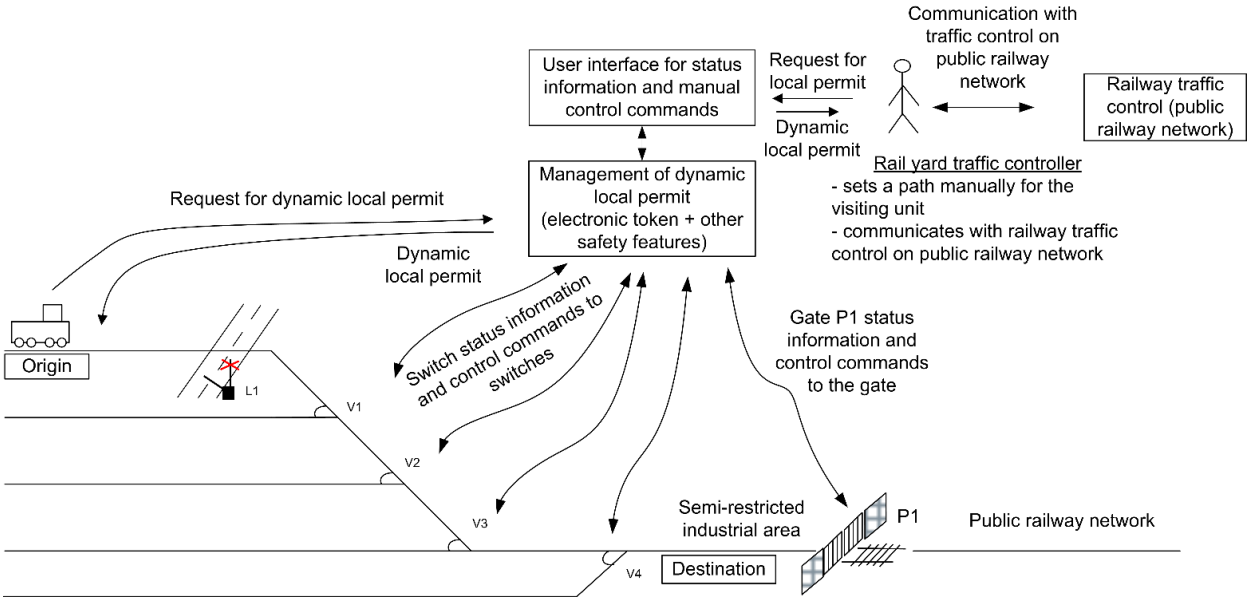


Figure 22. The AutoCar has a dynamic local permit for operation in a semi-restricted industrial area.

The route to be used by the AutoCar will be set manually by the human user. This can be done by entering control commands via the user interface, e.g., to change the position of switches on the rail yard and to open or close and lock the gate between the semi-restricted industrial area and the public rail network.

Before the AutoCar can start movement, two conditions must be met:

- The AutoCar has requested and obtained a dynamic local permit to operate in the semi-restricted industrial area.
- The AutoCar has received a "start” signal, which is given after loading or unloading of the unit has been completed (at origin or at destination).

If the area is visited by a unit arriving from public rail network, a human user (the rail yard traffic controller) will be responsible for movement of the visiting unit. Before the visiting unit is allowed to enter the area, the rail yard traffic controller will request a dynamic local permit from the permit management system. Only after a dynamic local permit has been granted, the rail yard traffic controller will set a route for the visiting

unit and open a gate between the semi-restricted area and the public railway network. During the process, the rail yard traffic controller may need to communicate with the railway traffic control responsible for the public railway network.

The human user (rail yard traffic controller) will be given a dynamic local permit for rail yard traffic control in the area if all following conditions are fulfilled:

- The AutoCar is stopped at origin or at destination.
- The validity period of the dynamic local permit given to the AutoCar has ended.

In case of operation based on a dynamic local permit, the following key assumptions were made:

- The AutoCar has a single route which can be travelled both ways without turning any switches.
- Only one AutoCar is in use at a time.
- Visiting units may arrive to a semi-restricted industrial area from public rail network.
- No visiting units will be operating in the area when the AutoCar has power switched on.
- Level crossing safety equipment in the area will operate as isolated units and use track circuit for train detection.
- Level crossing safety equipment will not be installed in areas used for storing rolling stock.
- Level crossing safety equipment will not be installed in an area used for shunting operations not reaching the level crossing, unless the level crossing safety equipment has an elimination function operated by a human user during shunting operations.

6.2.3 Automatic rail yard traffic control in a semi-restricted industrial area

The third operational concept described in the study is based on automated rail yard traffic control system (Figure 23). The AutoCar sends a request to automatic rail yard traffic control system to reserve and set a route from origin to destination via zero or more route points.

After receiving a request to set a route, the automated rail yard traffic control system performs the following actions:

- Automated rail yard traffic control system checks the vacancy of the rail sections along the route and at the destination (using track circuits).
- Automated rail yard traffic control system checks that the status of level crossings along the route is ‘ready’ (not ‘fault’ or ‘unknown’).
- Automated rail yard traffic control system determines the statuses of the switches corresponding to individual movements between route points.
- Automated rail yard traffic control system checks that the human user has not requested a dynamic local permit, and there are no valid dynamic local permits in force.
- Automated rail yard traffic control system blocks granting of dynamic local permits for the area.
- Automated rail yard traffic control system ensures separation of the area from public railway network (in the example closes and locks gate P1).
- Automated rail yard traffic control system sends confirmation of a route from origin to destination via zero or more route points to the AutoCar.

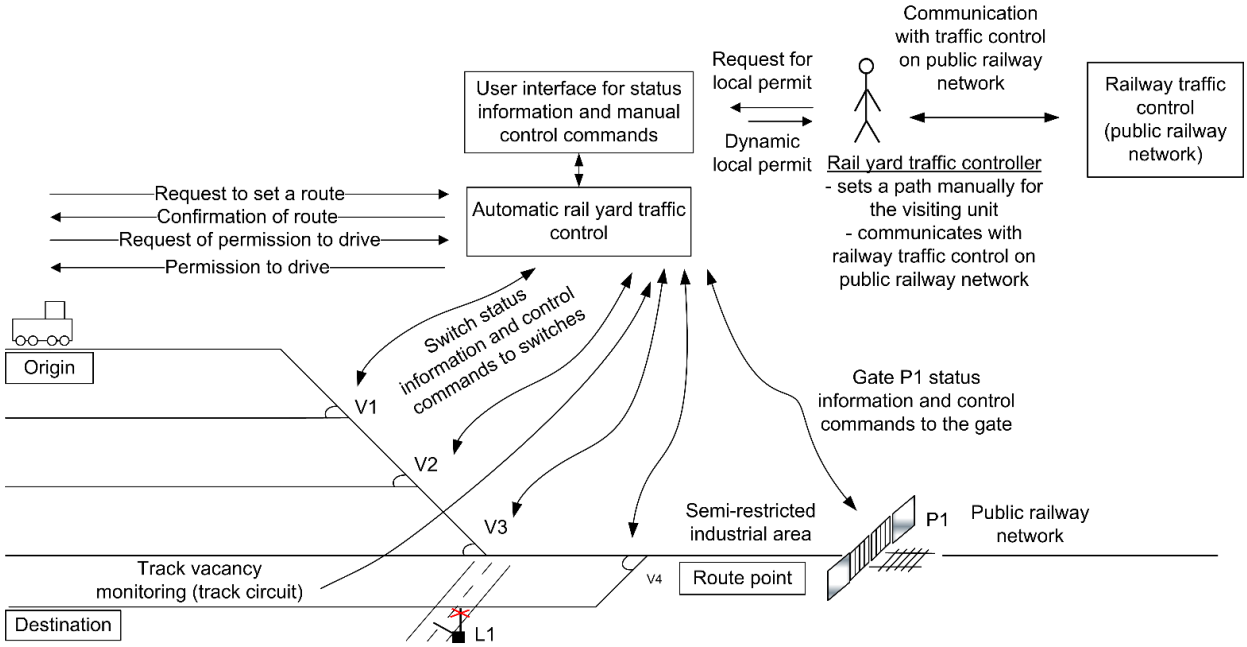


Figure 23. Rail yard traffic control system sets a train path for the AutoCarin an industrial area.

After receiving a confirmation of the route, the AutoCar will request a permission to drive from the origin to the first route point or from a route point to the next route point or to the destination. The automated rail yard traffic control system will send a permission to the AutoCar, if all following conditions are met (checked by the automatic rail yard traffic control system):

- The requested route section belongs to a route which has been confirmed for the AutoCar.
- All level crossings on the route section to be travelled have status ‘ready’ (not ‘fault’ or ‘unknown’).
- Track sections belonging to the route section are vacant (checked with track circuits).
- Control commands have been sent to the switches on the requested route section, and the switches have moved to positions allowing the route section to be travelled.

Before the AutoCar can start movement, three conditions must be met:

- The AutoCar has received a confirmation of a route from origin to destination.
- The AutoCar has received a permit to move between two points included in the route.
- The AutoCar has received a ‘start’ signal, which is given after loading or unloading of the unit has been completed (at origin or at destination).

The operational concept involving automated rail yard traffic control system includes the following key assumptions:

- The AutoCar may use several routes in a semi-restricted industrial area.
- Setting a single route or different routes for the AutoCar may require turning switches on the rail yard.
- Visiting units may arrive to the area from public rail network.
- Only one AutoCar or visiting train may move in the area at the same time.
- Visiting trains may arrive to a semi-restricted industrial area from public rail network.
- Level crossing safety equipment in the area will operate as isolated units and use track circuit for train detection.
- Level crossing safety equipment will not be installed in areas used for storing rolling stock.
- Level crossing safety equipment will not be installed in an area used for shunting operations not reaching the level crossing, unless the level crossing safety equipment has an elimination function operated by a human user during shunting operations.

The operational concept involving automated rail yard traffic control system includes special properties related to level crossing equipment.

- Local operation of the warning or boom system is independent of the automatic track yard traffic control system (triggering and disconnection of the alarm using the track current circuit, basic situation)

- Monitoring the status of level crossing equipment (fault status | normal status) and utilizing the status information to ensure access:
  - The yard traffic control does not confirm the passage through the track section with a level crossing in a faulty state
  - The yard traffic control does not give departure permission for the part of the access road, which includes a level crossing that is in a defective state

- Automatic track yard traffic control moves the level crossing to alarm mode with a control command and at the same time delays the departure permit given to AutoCar, if the route covered by the departure permit includes a level crossing and the distance between the start point of the departure permit (starting point or intermediate point) and the level crossing is too short. s_1/v_1 should be more than 20 s to be realized (Figures 24 and 25).

  - s_1 = The distance between the starting point of the departure permit and the level crossing
  - v_1 = The speed limit in the track yard area

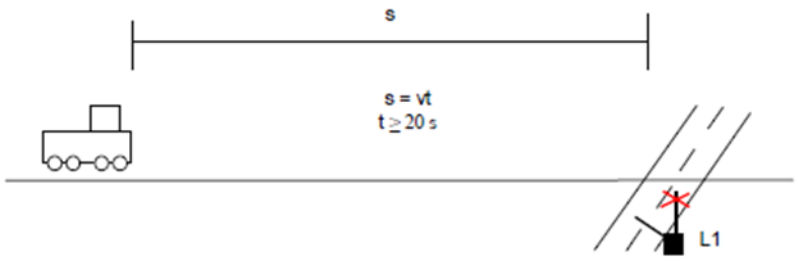


Figure 24. Principle to calculate the safety distance to level crossing.

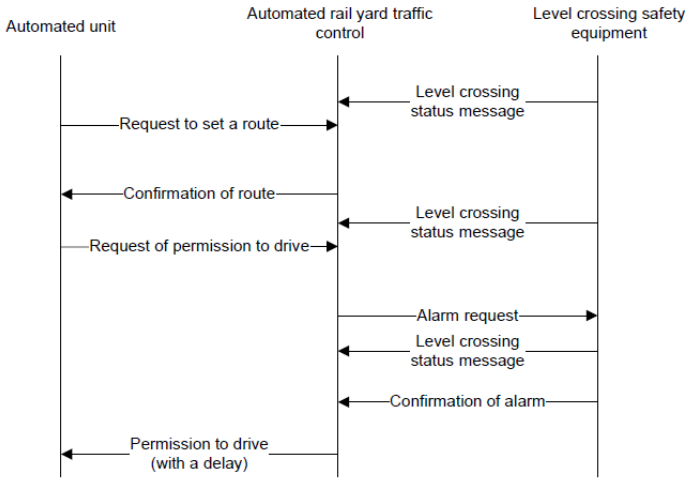


Figure 25. Procedure for getting the permission to drive.

6.3 Level crossing safety concepts for autonomous train operations

In case of autonomous train operations, it is possible to apply the existing principles and knowledge on evaluating and improving safety at level crossings. The traffic rules and regulations applicable to the road user are also substantially similar in case of an autonomous train or a manually operated train.

6.3.1 Regulatory basis in Finland

In Finland, the behavior of the road user at a level crossing is regulated by article 10 of the Road Traffic Act (Anon, 2018). The road user has an obligation to give way to a train or any other equipment moving on railway tracks. The road user approaching a level crossing must exercise special caution and monitor whether a train or any other equipment moving on railway tracks is approaching, regardless of the safety equipment installed at the level crossing. The speed of the vehicle must allow stopping the vehicle before railway tracks. The road user may not take actions to pass the level crossing if a train or other equipment moving on railway tracks is approaching or is passing the level crossing, warning lights installed at the level crossing require the road user to stop, audible warning is active, or the booms or gates of the level crossing are down or moving. In such case, the road user must stop at a safe distance from the railway tracks. The road user must pass the level crossing without unnecessary delay.

In Finland, the Road Traffic Act (Anon, 2018) is applicable on any public roads and streets, private roads, any areas intended for traffic purposes accessible for the public and private areas commonly used for traffic purposes by the public. The definition of a public road covered by the Road Traffic Act has formed in legal practice over the years (Nieminen 2020). For example, the yard of a petrol station has been concluded to be in the scope of the Road Traffic Act (Anon, 1967) while a military area accessible only via a guarded gate was considered not to be covered (Anon, 1987). Industrial areas not covered by the Road Traffic Act (Anon, 2018) typically have their own safety rules, and entry to the area may also be restricted.

6.3.2 Principles for safety concept at level crossings for autonomous train operations

When evaluating the impact of an autonomous train operations on safety at level crossings in general, the evaluation should have a meaningful baseline. Autonomous operation can be compared with manually operated trains or use of transport modes other than rail transport. The safety of different level crossings can be evaluated with a model developed by VTT (Peltola et al, 2012; Metsäranta et al, 2021). The model is applicable to both public roads and private areas.

It can be argued that hazards related to level crossing exist regardless of manual or automated operation of the train. It may also be possible to argue that the safety of level crossings and related risks to the road user will remain on the same level unless the frequency of trains, train speed or visibility of the train changes.

It can be difficult to predict the actions or intentions of a road user approaching a level crossing (will the road user stop or drive under). Once the obstacle on the tracks is secured, it is no longer necessarily possible to stop the train moving on the tracks before the level crossing. Anticipating a fast-accelerating or turning object (e.g., an electric scooter) is difficult.

Stopping an autonomous train when a vehicle or person is detected at a level crossing is not necessarily a problem-free option due to the following reasons:

- The braking distance of a device moving on tracks can be long if there is a lot of mass, the brakes are weak or the friction between the wheel and the track is limited. Stopping before a collision may not be possible.
- When a train moving on tracks makes an emergency brake, the result can be a so-called notch wheel.

- Drivers of vehicles and people moving in the area may learn an incorrect and potentially dangerous operating pattern when they observe an autonomous train giving way at level crossings. According to the Road Traffic Act (Anon, 2018), the driver of a vehicle or a pedestrian is always obliged to give way at a level crossing.

It can be concluded that the following safety principles for level crossings apply for both manual and autonomous train operations.

- Crossing the tracks is only allowed at certain points (level crossings), not anywhere in the open field. At the same time, the movement of vehicles and people is guided to use level crossings, for example with curbstones or fences.
- The level crossings are equipped with a boom system (and in addition also with a warning light and sound).
- Crossing the level crossing is physically prevented when a train moving on the tracks approaches the level crossing and the level crossing sounds an alarm. This is how the metal plates used at level crossings work, for example in Russia. The plates rise from the road surface, which prevent a car from driving into the level crossing, but do not prevent driving away from the level crossing.
- The speed of a train moving on the tracks is limited to a low level in a heavily trafficked terminal area or at a level crossing. The road user or the person moving in the area has more time to observe and react. The consequences of a collision between a vehicle and a train are also less serious.
- Traffic other than by car or a larger vehicle is prohibited in the factory or terminal area where an autonomous train operates (for example, in terminal areas where you can cross the tracks from any point).

References

Anon, (1967). KKO:1967-II-55 https://finlex.fi/fi/oikeus/foki/tapaus/54313

Anon, (1987). KKO 1987:60 https://finlex.fi/fi/oikeus/foki/tapaus/101860

Anon, (2008). *Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive*. ERA/GUI/01-2008/SAF Version: 1.1. European Railway Agency. https://www.era.europa.eu/system/files/2022-11/Guide%20for%20the%20application%20of_%20the%20Common%20Safety%20Methods%20on%20risk%20assessment%20%28EN%29.pdf

EN 50126-1:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

EN 50128:2011 Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems

EN 50129:2018 Railway applications - Communication, signaling and processing systems - Safety related electronic systems for signaling

EN 50159:2010/A1:2020 Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems

SFS 6002:2015 + A1:2018 Safety at electrical work

Anon, (2018). *Tieliikennelaki* [Road Traffic Act] 10.8.2018/729 https://www.finlex.fi/fi/laki/ajantasa/2018/20180729

Anon, (2021). *Junaliikenteen ja vaihtotyön turvallisuussäännöt (Jt)* [Safety regulations for train traffic and shift work (Ts)], Finnish Transport Infrastructure Agency Instructions 3/2021. Finnish Transport Infrastructure Agency. https://ava.vaylapilvi.fi/ava/Julkaisut/Vaylavirasto/vo_2021-03_jt_web.pdf

Anon, (2022). Autonomous train project 2022, Proxion Oy, 31.05.2022, https://www.youtube.com/watch?v=2wCMr14XD-s

Vincoli, J. W. 2006. *Basic Guide to System Safety.* Hoboken, NJ: John Wiley & Sons, Inc.

Tiusanen, R. (2014). *An approach for the assessment of safety risks in automated mobile work-machine systems: Dissertation*. [Dissertation, Tampere University of Technology (TUT)]. VTT Technical Research Centre of Finland. https://publications.vtt.fi/pdf/science/2014/S69.pdf

Nieminen, J. (2020) Onko tien määritelmä todella muuttunut? – Outoja maastopysäköintisakkoja jakavat firmathan joutuisivat palauttamaan aiheettomat maksut. [Has the definition of road really changed? - Companies handing out strange off-road parking fines would have to return unjustified payments.] Tekniikan Maailma, 4.12.2020. https://tekniikanmaailma.fi/pysakointi-maasto/

Peltola, H., Seise, A., Leden, L. & Virkkunen, M. (2012). *Rautateiden tasoristeysten turvallisuuden arviointi: Tarva LC.* Liikenneviraston julkaisut 1241. [Assessment of the safety of railway level crossings: Tarva LC. Publications of the Finnish Transport Infrastructure Agency 1241.]

Metsäranta, H., Haapala, S., Sauni, M. & Mankki, A. (2021). *Perusradanpidon investointien vaikutusarvioinnin kehittäminen, Esiselvitys.* [Development of the impact assessment of base track maintenance investments, Preliminary study.] Finnish Transport Infrastructure Agency. https://www.doria.fi/bitstream/handle/10024/180788/vj_2021-22_978-952-317-858-8.pdf?sequence=1&isAllowed=y

Appendices

Appendix 1 Risk analysis worksheets

Appendix 2 Summary of the proposed safety measures

Risk analysis worksheets

Appendix 1 Risk analysis worksheets

Hazard, threat, problem	Description of the hazardous situations	Causes	Consequences	Existing safety measures or risk control options	Risk before	Proposals for additional safety measures for the autonomous train, infra at the site, other actors...	Risk after
AutoCar runs over a pedestrian or a cyclist on the rails							
Run over hazard	A person is walking on the rails, A person is walking across the rails in the marked crosswalks or in a random location A person comes from behind a structure or behind a vehicle The person does not notice that the AutoCar is coming.	The AutoCar's safety system does not notice the person Failure in the AutoCar control system, AutoCar doesn't stop Failure in the communication system Carelessness, the person doesn't obey the traffic rules	The person dies or is seriously injured	The speed of AutoCar is very low, max. 20 km/h. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents.		AutoCar's safety system must be capable of detecting a pedestrian or cyclist on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar must have audiple and visual warning signals when it is moving. Walking on the rails must be prohibited. There must be marked walkways and warnings of automatic train. Making the tracks more visible and directing light traffic (pedestrians and cyclists) to certain routes. Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.	
Run over hazard	The cyclist is moving across the rails in the marked crosswalks or in a random location The cyclist comes from behind a structure or behind a vehicle The cyclist does not notice that the AutoCar is coming	The AutoCar's safety system does not notice the cyclist. Failure in the AutoCar control system, AutoCar doesn't stop Failure in the communication system Carelessness, the cyclist doesn't obey the traffic rules.	The person dies or is seriously injured	The speed of AutoCar is very low, max. 20 km/h. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents.		AutoCar's safety system must be capable of detecting a pedestrian or cyclist on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar must have audiple and visual warning signals when it is moving. Walking on the rails must be prohibited. There must be marked walkways and warnings of automatic train. Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.	
AutoCar runs over a pedestrian or a cyclist in a level crossing							

Run over hazard	A person is walking or cycling across the rails The person does not notice that the AutoCar is coming.	There is no warning or safety system in the level crossing. Failure in the level crossing safety system. The AutoCar's safety system does not notice the person. Failure in the AutoCar control system, AutoCar doesn't stop. Failure in the communication system Carelessness, the person doesn't obey the traffic rules.	The person dies or is seriously injured	The speed of AutoCar is very low, max. 20 km/h. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents.		AutoCar's safety system must be capable of detecting a pedestrian or cyclist on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar must have audiple and visual warning signals when it is moving. Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area. There must be warnings of automatic train. Level crossings should have safety devices preventing access to the rails when the automatic train is moving through the crossing. See the the concepts written by Risto Öörni for ensuring safe passage for the AutoCar or a train coming from the public rails in the industrial area.
AutoCar crushes a person in the loading or unloading place						
Crushing hazard	AutoCar crushes a person (against a structure) in a loading / unloading station The person is standing on the rails or near the rails or comes from behind behind a structure or behind a vehicle The person does not notice that the AutoCar is coming.	The AutoCar's safety system does not notice the person Failure in the AutoCar control system, AutoCar doesn't stop Failure in the communication system AutoCar doesn't stop in a right place or it moves unexpectedly A person has access to the hazard zones Carelessness, the person doesn't obey the safe working instructions	The person dies or is seriously injured	The speed of AutoCar is very low (max. ?? km/h) when coming to or moving from the loading or unloading place. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents. AutoCar's positioning is based on DGNSS, inertia and reference points.		AutoCar's safety system must be capable of detecting a person on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar's positioning to a right place must be ensured. Unexpected moving at the loading or unloading place must be prevented. AutoCar must have audiple and visual warning signals when it is moving. There must be warnings of automatic train. Hazardous points at the loading or unloading places must be safeguarded and access to hazardous areas must be prevented. In the design of loading and unloading docks, the risks of crushing must be taken into account. Possible crushing hazards should be taken into account in vehicle parking arrangements. Persons working or visiting the area must follow the safety rules and instructions in the industry area.
AutoCar crushes a person at the charging station						

Crushing hazard	AutoCar crushes a person (against a structure) in a charging station The person is standing on the rails or near the rails or comes from behind behind a structure or behind a vehicle The person does not notice that the AutoCar is coming.	The AutoCar's safety system does not notice the person Failure in the AutoCar control system, AutoCar doesn't stop Failure in the communication system AutoCar doesn't stop in a right place or it moves unexpectedly A person has access to the hazard zones Carelessness, the person doesn't obey the safe working instructions	The person dies or is seriously injured	The speed of AutoCar is very low (max. ?? km/h) when coming to or moving from the loading or unloading place. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents. AutoCar's positioning is based on DGNSS, inertia and reference points.		AutoCar's safety system must be capable of detecting a person on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar's positioning to a right place must be ensured. Unexpected moving at the charging station must be prevented. AutoCar must have audiple and visual warning signals when it is moving. There must be warnings of automatic train. Hazardous points at the charging station must be safeguarded and access to hazardous areas must be prevented. Persons working or visiting the area must follow the safety rules and instructions in the industry area.
AutoCar collides a car, forklift truck, lorry, another vehicle or its trailer in the level crossing						
Collision and crushing hazard	A vehicle is moving across the rails. A vehicle or its trailer is stopped in the level crossing. The driver does not notice that the AutoCar is coming to the level crossing.	There is no warning or safety system in the level crossing Failure in the level crossing safety system The AutoCar's safety system does not notice the vehicle Failure in the AutoCar control system Failure in the AutoCar's communication system Failure in the vechicle, the vehicle stops unexpectedly in the level crossing. Driver's error or carelessness, the driver doesn't obey the traffic rules Bright sunlight affects the driver	People die or are seriously injured in the vehicle The vehicle is damaged AutoCar can derail and crash	The speed of AutoCar is very low, max. 20 km/h. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents. AutoCar's positioning is based on DGNSS, inertia and reference points. Access to the industrial area is restricted. Truck drivers and work machine drivers are professionals. There are traffic rules and instructions for vehicle drivers in the industry area.		AutoCar's safety system must be capable of detecting an obstacle on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar must have audiple and visual warning signals when it is moving. Level crossings should have safety devices preventing access to the rails when the automatic train is moving through the crossing. The rail traffic control system must ensure safe passage through the level crossings for the AutoCar. See the the concepts written by Risto Öörni for ensuring safe passage for the AutoCar or a train coming from the public rails in the industrial area. Vehicle drivers must follow the traffic rules and instructions in the industry area. There must be warnings of automatic train.
AutoCar collides a vehicle or its trailer on the rails (not in a level crossing)						

Collision and crushing hazard	A vehicle or its trailer is parked on the rails A vehicle or its trailer is stopped on the rails The driver does not notice that the AutoCar is coming	The AutoCar's safety system does not notice the vehicle Failure in the AutoCar control system Failure in the AutoCar's communication system. Failure in the vehicle, the vehicle stops unexpectedly on the rails. Carelessness, the driver doesn't obey the traffic rules	People die or are seriously injured in the vehicle The vehicle is damaged AutoCar can derail and crash	The speed of AutoCar is very low, max. 20 km/h. Train onboard sensors (radar, thermal and visual cameras) observes environment and reacts when needed. Sensor fusion with related software are planned to take care of decision making to avoid accidents. AutoCar's positioning is based on DGNSS, inertia and reference points. There are traffic rules and instructions for vehicle drivers in the industry area. Access to the industrial area is restricted. Truck drivers and work machine drivers are professionals.		AutoCar's safety system must be capable of detecting an obstacle on the rails and near the rails from such a distance that it is able to stop under all circumstances to prevent an accident. Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving. AutoCar must have audiple and visual warning signals when it is moving. Parking on the rails must be prohibited, including short-term parking during loading or unloading. There must be marked vehicle routes and warnings of automatic train. Directing vehicle traffic and light traffic to safe routes. Vehicle drivers must follow the traffic rules and instructions in the industry area.
A vehicle collides the AutoCar at a loading or unloading station						
Crushing hazard	AutoCar is stopped on the station The driver is loading or unloading the AutoCar The driver can not stop the vehicle The driver can not control the vehicle correctly	A fault in the vehicle's brakes Slippery driveway Failure in vehicle control system, the vehicle doesn't stop or it moves unexpectedly.	The vehicle driver is injured The vehicle and the AutoCar are damaged. AutoCar can derail and crash	There are traffic rules and instructions for vehicle drivers in the industry area. Truck drivers and work machine drivers are professionals.		There must be marked vehicle routes and warnings of automatic train. Area maintenance must ensure that access roads and loading/unloading areas are safe to drive, especially in winter conditions. Vehicle drivers must follow the traffic rules and instructions in the industry area.
A vehicle collides the AutoCar in a level crossing						
Crushing hazard	AutoCar is moving in the level crossing The driver can not stop the vehicle	A fault in the vehicle's brakes Slippery driveway Failure in vehicle control system, the vehicle doesn't stop or it moves unexpectedly	The vehicle driver is injured The vehicle and the AutoCar are damaged. AutoCar can derail and crash	Truck drivers and work machine drivers are professionals.		There must be marked vehicle routes and warnings of automatic train. Area maintenance must ensure that access roads and level crossing areas are safe to drive, especially in winter conditions. Vehicle drivers must follow the traffic rules and instructions in the industry area.
A train collides the AutoCar						
Collision hazard	A train moves to the same rails where the AutoCar is and collides the AutoCar	The train moves to a wrong track, AutoCar is on the wrong track Failure in the train traffic control system, Failure in the communication system Human error of the train traffic controller or the train driver, carelessness	The train driver and other persons in the train are injured The train and the AutoCar are damaged. AutoCar and / or the train can derail and crash			See the the concepts written by Risto Öörni for ensuring safe passage for the AutoCar or a train coming from the public rails in the industrial area.

Crushing hazard	A train collides AutoCar at a trailway switch	AutoCar is in wrong position at the trailway switch (too near the other rails). Failure in AutoCar postioning.		AutoCar's positioning is based on DGNSS, inertia and reference points.		AutoCar's positioning to a right place must be ensured at the railway switches. Failure in the AutoCar's control system or in the communication system must stop the train and prevent the train from moving.
AutoCar collides a train						
Collision hazard	AutoCar moves to the same rails where the train is and collides the train	The train is on the wrong track AutoCar is on the wrong track The railway switch is turned into a wrong 'position' Failure in the train traffic control system Failure in the communication system Human error of the train traffic controller	The train driver and other persons in the train are injured The train and the AutoCar are damaged. AutoCar and / or the train can derail and crash			The train traffic control in the area must prevent the hazardous situations. Failure in the AutoCar's control system or in the communication system must stop the AutoCar and prevent the AutoCar from moving. See the the concepts written by Risto Öörni for ensuring safe passage for the AutoCar or a train coming from the public rails in the industrial area.
Crushing hazard	AutoCar collides a train at a railway switch	A train / wagon is stopped in wrong position at the trailway switch (partly above or too near). Human error of the train driver	The train driver and other persons in the train are injured The train and the AutoCar are damaged. AutoCar and / or the train can derail and crash			The train traffic control in the area must prevent the hazardous situations. Positioning of a train to a right place must be ensured at the railway switches. Failure in the AutoCar's control system or in the communication system must stop the AutoCar and prevent the AutoCar from moving. See the the concepts written by Risto Öörni for ensuring safe passage for the AutoCar or a train coming from the public rails in the industrial area.
The AutoCar collides an unexpected (heavy) obstacle on the rails						
Impact hazard	There is a heavy obstacle on the rails	A vehicle is parked on the rails, a heavy object has dropped from a forklift or from a truck on the rails, a heavy object is left on rails	Damage to the AutoCar and rails and the object, AutoCar can derail and crash			The AutoCar's safety system should be capable to detect an obstacle on the rails from such a distance that it is able to stop the AutoCar to avoid a collision. The workers must follow safety instructions for loading and unloading and instructions. The workers should inform if they see anything out of the ordinary on the track Persons working or visiting the area must follow the safety rules and instructions in the industry area. Area maintenance must ensure that access roads, level crossing areas and loading/unloading areas are safe to drive, especially in winter conditions.
Rerailment hazard due to the material on the tracks						
Impact hazard	There can be ice, a lot of snow, sand, debris, or some extra material on the tracks. The AutoCar drives over the material and the train wheels can come off the rails and train can derail and crash.	Heavy snowfall, ice formation on the track, sand or debris falling from a truck load, etc.	AutoCar can derail and crash Damage to the AutoCar and rails and other vehicles or structures nearby			Area maintenance must ensure that tracks are safe to drive, especially in winter conditions.
Fire hazards caused by the AutoCar						

Fire hazard	AutoCar lights up while moving, the battery catches fire	Electric short circuit, failure in the battery	Persons are injured or exposed to hazardous gases. Damage to the AutoCar			AutoCar (locomotive unit) must be equipped with an automatic extinguishing system or have a sufficient amount of battery fire extinguishing equipment
Fire hazard	The AutoCar catches fire while charging	Electric short circuit, failure in the charging system, failure in the battery	Persons are injured or exposed to hazardous gases. Damage to the AutoCar and the charging station			AutoCar (locomotive unit) must be equipped with an automatic extinguishing system or have a sufficient amount of battery fire extinguishing equipment. The charging station must have a sufficient amount of battery fire extinguishing equipment.
Mechanical hazards caused by the AutoCar						
Crushing hazard	A heavy cargo falls from the wagon at a loading or unloading station, at a level crossing or near the walkways or vehicle routes.	The cargo is not properly secured. AutoCar makes an unexpected movement.	The person dies or is seriously injured	There are safety instructions for loading and unloading and ensuring the cargo. Workers in the area and work machine drivers are professionals.		There must be marked walkways and warnings of automatic train. Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.
Crushing hazard	An object falls from the wagon at a loading or unloading station, at a level crossing or near the walkways or vehicle routes.	Some objects are left on the wagon or on the locomotive e.g. after a maintenance work. Something breaks and is thrown near the AutoCar.	The person is seriously injured	There are safety instructions for maintenance work. Workers in the area and work machine drivers are professionals.		Persons working in the area must follow the safety rules and instructions and they should inform if they see anything out of the ordinary related to the AutoCar.
Electrical hazards caused by the AutoCar						
Electric shock	A maintenance person gets an electric shock	Electric short circuit, failure in the electrical circuits, Human error in maintenance	The person dies or is seriously injured due to the electric shock			The AutoCar must fullfill electrical safety requirements
Electrical fire hazard	Electric batteries or electric circuits in AutoCar catches fire	Electric short circuit, failure in the electrical circuits, Human error in maintenance	The person dies or is seriously injured. An electrical fire can produce toxic gases, battery chemicals can explode			Electric fire hazard must be consided in the design of AutoCar system and its safety measures. AutoCar could be equipped with an automatic fire extinquiser system.

Summary of the proposed safety measures

Summary of the proposed safety measures in AutoCar preliminary risk analysis

To prevent overrunning accidents or minimize the risk of overrun
To prevent crushing accidents or minimize the risk of crushing at the stations
To prevent crushing accidents or minimize the risk of falling cargo
To prevent crushing accident or minimize the risk of falling objects from the AutoCar

- The speed of the AutoCar must be slow, max. 20 km/h.
- The speed of the AutoCar must be slow near the stations.
- AutoCar's safety system must be capable of detecting a pedestrian or cyclist on the tracks and near the tracks from such a distance that it is able to stop under all circumstances. Performance and functional safety (SIL / PL) requirements for the AutoCar control system must be defined.
- AutoCar's safety system must be capable of detecting a person near the tracks from such a distance that it is able to stop under all circumstances at the stations to prevent an accident.
- Failure in the AutoCar's safety system, its control system or in the communication system must stop the train and prevent the train from moving.
- Unexpected moving of the AutoCar must be prevented at the stations. Functional safety (SIL / PL) requirements for the safety related parts of the AutoCar control system must be defined.
- AutoCar's reliable positioning to a right place must be ensured.

- Hazardous points at the stations station must be safeguarded and access to hazardous areas near the tracks must be prevented.
- In the design of loading and unloading docks, the risks of crushing must be considered.
- Possible crushing hazards should be considered in vehicle parking arrangements
- AutoCar must have audible and visual warning signals when it is moving.
- Making the track more visible and directing light traffic (pedestrians and cyclists) to certain routes
- There must be marked walkways and warnings of automatic train.
- Level crossings should have safety devices preventing access to the tracks when the automatic train is moving through the crossing. Functional safety (SIL / PL) requirements for the level crossing safety systems must be defined.
- Walking on the tracks must be prohibited and there must be marked walkways and warnings of the automatic train.

- Persons working or visiting the area must follow the safety rules and instructions for pedestrians and cyclists in the industry area.
- The workers must follow safety instructions for loading and unloading and instructions for ensuring the cargo.
- The workers must follow safety instructions for loading and unloading and instructions.
- Persons working or visiting the station area must follow the safety rules and instructions.
- The workers should inform if they see anything out of the ordinary related to the AutoCar or its cargo.

To prevent electrical hazards

- The AutoCar electrics and the charging station must fulfill electrical safety requirements.
- Maintenance persons must follow the safety rules and instructions (SFS 6002:2015 + A1:2018 Safety at electrical work).
- AutoCar could be equipped with an automatic fire extinguisher system.

To prevent collisions with vehicles in level crossings
To prevent collisions with vehicles on tracks in other places other than level crossings

- The rail traffic control system must ensure safe passage through the level crossings for the AutoCar. See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2 in the report).
- Level crossings should have safety devices preventing access to the tracks when the automatic train is moving through the crossing.
- AutoCar's safety system must be capable of detecting an obstacle on the tracks and near the tracks from such a distance that it is able to stop under all circumstances to prevent an accident.
- Failure in the AutoCar's safety system or in the communication system must stop the train and prevent the train from moving.
- AutoCar must have audible and visual warning signals when it is moving.
- There must be warnings of automatic train.
- Directing vehicle traffic and light traffic to safe routes.
- Vehicle drivers must follow the traffic rules and safety instructions in the industry area.

To prevent accidents where a vehicle collides the AutoCar

- Vehicle drivers must follow the traffic rules and instructions in the industry area.
- There must be marked vehicle routes and warnings of automatic train.
- Area maintenance must ensure that access roads, level crossing areas and loading/unloading areas are safe to drive, especially in winter conditions.

To prevent accidents where a train collides the AutoCar

- The train traffic control in the area must prevent the hazardous situations. See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2 in the report).
- Positioning of a train to a right place must be ensured at the railway switches.
- Failure in the AutoCar's control system or in the communication system must stop the AutoCar and prevent the AutoCar from moving.

To prevent accidents where the AutoCar collides a train

- The train traffic control in the area must prevent the hazardous situations. See the concepts for ensuring safe passage for the AutoCar or a train coming from the public tracks in the industrial area (See chapter 5.2 in the report).
- AutoCar's positioning to a right place must be ensured at the railway switches.
- Failure in the AutoCar's control system or in the communication system must stop the train and prevent the train from moving.

To prevent collisions with an object on the track

- The AutoCar's safety system should be capable to detect an obstacle on the rails from such a distance that it is able to stop the AutoCar to avoid a collision.
- The workers must follow safety instructions for loading and unloading and instructions.
- The workers should inform if they see anything out of the ordinary on the track
- Persons working or visiting the area must follow the safety rules and instructions in the industry area.
- Area maintenance must ensure that access roads, level crossing areas and loading/unloading areas are safe to drive, especially in winter conditions.

To prevent derailment hazard due to the material on the tracks

- Area maintenance must ensure that tracks are safe to drive, especially in winter conditions.