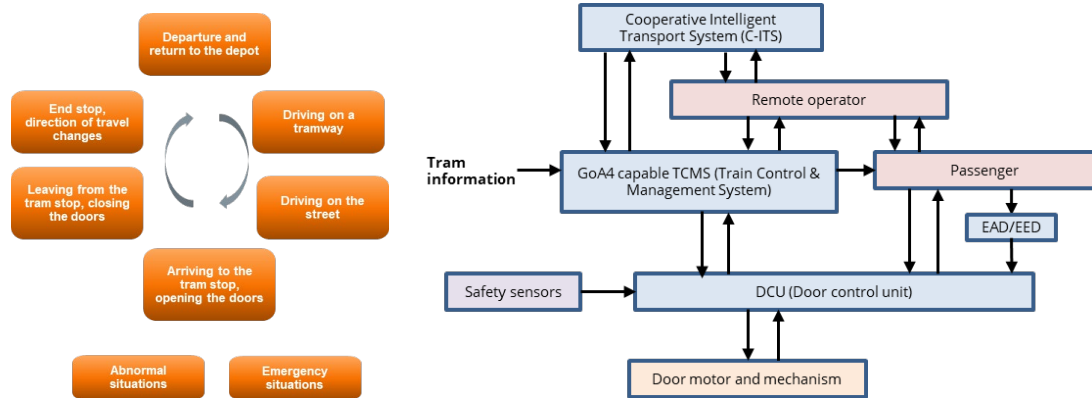


RESEARCH REPORT

VTT-R-00499-23



Safety analyses on the use of tram doors in GoA1 and GoA4 autonomy levels

Authors: Risto Tiusanen, Eetu Heikkilä, Tero Välisalo, Timo Malm

Confidentiality: VTT Public

Version: 25.9.2023



Report's title Safety analyses on the use of tram doors in GoA1 and GoA4 autonomy levels	
Customer, contact person, address	Order reference
Project name SmartRail2	Project number/Short name 124135 / SmartRail2
Author(s) Risto Tiusanen, Eetu Heikkilä, Tero Välisalo, Timo Malm	Pages 20
Keywords Tram, autonomy, safety analysis, STPA, GoA level	Report identification code VTT-R-00499-23
<p>Summary</p> <p>Development towards higher grade of automation (GoA) levels has been a global trend in trains and metros, but so far not in trams due to their complex and highly dynamic operating environment. However, currently rail operators are also showing increasing interest on higher automation levels in tram systems to increase their efficiency and safety. Higher GoA levels in a tram system introduces changes in operating principles, new roles for personnel, and new types of safety risks in daily operations. In this report, we present two studies where risk analysis methods were applied in the conceptual level to identify new autonomy related safety risks in tram operations. The goal of this study was to identify and analyse the effects of increasing level of tram autonomy (from GoA1 to GoA4) on the use of automated tram door and its functionalities. The objectives were to identify the different operating situations of the automatic tram door system, analyse the related safety and availability risks, and define the necessary safety measures.</p> <p>The results of the PHA and STPA analyses show that parts of the door systems are already capable for GoA4 tram operations. There are safety systems ensuring that the doors do not open when the tram is in motion, and to detect obstacles between the doors. Solutions to ensure accessibility and safe entry and exit for all passengers must be developed for GoA4 operation considering especially passengers who move slowly, have reduced mobility, use wheelchair or are visually impaired. Managing of abnormal situations and emergencies needs to be carefully considered in GoA4 operation. For example, to ensure that the tram can be evacuated safely if needed, and that management of technical and human disturbances with the door systems could be managed remotely.</p> <p>The door system, however, is only one aspect of the tram operation and other parts are subject to significant changes. Thus, on the path towards automated tram operations, comprehensive safety analyses of all parts of the system and operations are still needed. Systemic methods, such as STPA, can be applied to support these analyses. The results of the analyses can be used to support development of the door systems by focusing the development actions into the areas where the major changes and improvement needs are expected.</p>	
Confidentiality	VTT Public
Tampere 25.9.2023	
Written by	Reviewed by
Risto Tiusanen Senior Scientist	Raine Hautala Principal Scientist
VTT's contact address Visiokatu 4, PL 1300, 33101 TAMPERE	
Distribution (customer and VTT)	
Business Finland: (PDF) Tamware Oy: (PDF) Skoda Transtech Oy: (PDF) VTT: Achieve (Print copy + PDF); Raine Hautala, Risto Tiusanen (PDF)	
<p><i>The use of the name of "VTT" in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i></p>	

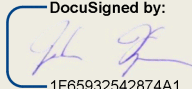


Approval

VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD

Date: 29 syyskuuta 2023

Signature:

DocuSigned by:

1F65932542874A1...

Name: Johannes Hyrynen

Title: Lead, Low carbon and smart machines



Contents

1. Introduction	4
2. Goal and objectives	5
3. The tram door system.....	5
4. Methods and their implementation.....	7
4.1 Preliminary Hazard Analysis (PHA) method.....	7
4.2 System Theoretical Process Analysis (STPA) method	8
5. Results.....	9
5.1 PHA results	9
5.1.1 Use of tram doors in GoA1 level daily operations.....	9
5.1.2 Ensuring the correct functioning of the doors	10
5.1.3 Ensuring the safe functioning of the doors during normal operation	10
5.1.4 Hazards and foreseeable problems during tram operation.....	11
5.1.5 Special situations during tram operation.....	11
5.2 STPA results	11
5.2.1 Step 1: Losses, hazards, and safety constraints	12
5.2.2 Step 2: Control structures	13
5.2.3 Steps 3 and 4: Identification of unsafe control actions and loss scenarios.....	14
6. Discussion	17
6.1 Safety aspects in tram door usage in GoA1 versus GoA4	17
6.2 New challenges in tram door usage in GoA4	17
6.3 Experiences of the analysis methods in this context.....	18
7. Conclusions	19
References	19

1. Introduction

Development towards higher grade of automation (GoA) has been a global trend in trains and metros. Trams operating in street level among other traffic are operated by human drivers. There will be several intermediate stages in the roadmap towards automated tram operations, such as automatic driving between stops, automatic start and stop, and automatic door operations at a stop. It is also assumed that the automation level of tram doors will increase as the autonomy of tram systems increases. Making depot automation commercially viable could be a first stage of introducing autonomous driving, including the legal and economic conditions that must be fulfilled for the approval and operation of an autonomously driving tram (Flaherty, 2021).

According to the International Association of Public Transport (UITP) (UITP, 2018) and the international standard IEC 62290-1 (2014) there are four Grades of Automation (GoA) for railway systems: GoA1 – GoA4, which are illustrated in Table 1.

Table 1. Grades of automation in railway systems according to UITP (2018).

Grade of Automation	Type of train operation	Setting the train in motion	Stopping the train	Door closure	Operation in an event of disruption
GoA1	ATP with a driver	Driver	Driver	Driver	Driver
GoA2	ATP and ATO with a driver	Automatic	Automatic	Driver	Driver
GoA3	Driverless operation DTO	Automatic	Automatic	Train attendant	Train attendant
GoA4	Unattended operation UTO	Automatic	Automatic	Automatic	Automatic

In the

Table 1 ATP = Automatic Train Protection, ATO = Automatic Train Operation, STO = Semi-automatic train operation and UTO = Unattended Train Operation.

Several metro and monorail lines capable of operation at the GoA4 level are already in operation worldwide (UITP, 2018). GoA4 refers to driverless train operation, which is in metro systems enabled by the possibility to effectively confine the system from external disturbances by operating in tunnels and by applying platform screen doors at stations (Pyrgidis, 2021; Emery, 2017). GoA4 systems have been developed and evaluated for mainline railways, for example in Hamburg, Germany (Clinnick, 2021).

Trams and other light rail systems that operate at street level in coexistence with other traffic (all kind of vehicles, motorcyclists, people using electric scooters, cyclists, and pedestrians) are still operated by human drivers. However, rail operators are currently showing increasing interest towards the possibilities of automation also in tram systems to increase safety and efficiency (Connolly, 2018).

The shift towards a higher GoA level in tram operations imposes changes in many of the subsystems in rail traffic management systems and tram control systems. Higher automation levels in a tram system introduces new types of safety risks and uncertainties in daily operations among other traffic. It is therefore essential to identify and assess the new safety risks and uncertainties in the early conceptual design phase, so that they can be eliminated, mitigated, or reduced to an acceptable level. Novel approaches and tools are needed to identify new security and availability risks arising from autonomous operation and to evaluate intelligent (anticipatory or preventive) safety related solutions (Heikkilä et al., 2022).

In this report, we present results of two safety analyses on the use of tram doors in GoA1 and GoA4 autonomy levels. This report is related to the work done in VTT in the Business Finland funded

'SmartRail2' research project in its task 3.4 'Effects of Tram autonomy on door system requirements'. The safety analyses were conducted during 2019 to 2021 by a project team, which included experts from Tamware Oy, VTT Technical Research Centre of Finland Ltd. (VTT) and Skoda Transtech Oy.

For more information about 'SmartRail2' research project and the overall 'SmartRail Ecosystem', see web pages: <https://smartrailecosystem.com/>;

<https://smartrailecosystem.com/events/tampere-smart-city-expo-conference/>.

More information about Tampereen Raitiotie Oy's 'Lyyli' Living Lab development environment can be found from the web pages:

<https://www.businessfinland.fi/en/whats-new/cases/2023/tampere-hasa-unique-living-lab-environment-for-urban-transport->

More about Tampereen Ratikka (Figure 1) can be found from their web page:

[Welcome to the Tramway Era! - Tampereen Ratikka](#)



Figure 1. Tampereen Ratikka (Tampere Tramway Ltd.).

2. Goal and objectives

The goal of this study was to identify and analyse the effects of increasing level of tram autonomy (from GoA1 to GoA4) on the use of automated tram door and its functionalities. The objectives were to identify the different operating situations of the automatic tram door system, analyse the related safety and availability risks, and define the necessary safety measures.

3. The tram door system

In the safety analyses, the tram's door system was examined on a functional level without going into technical details or the specific features of a certain manufacturer's door type. Within the framework of the research project, there was an opportunity to get to know Tamware Oy's door system and Tampereen raitiotie Oy's door systems used in the new trams. These were used when defining the functions of the doors for the safety analyses. The doors used in Tampereen Ratikka can be seen in Figure 2. The photos in Figure 2 are taken from the prototype tram car in Tampere Tramway Ltd's facilities.



Figure 2. The prototype of a single unit of a Tampere tram.

Functional level block diagrams of the tram door control system were created for the safety analyses in collaboration with Tamware Oy's experts. Examples of GoA1 and GoA4 level diagrams are presented in Figure 3 and in Figure 4.

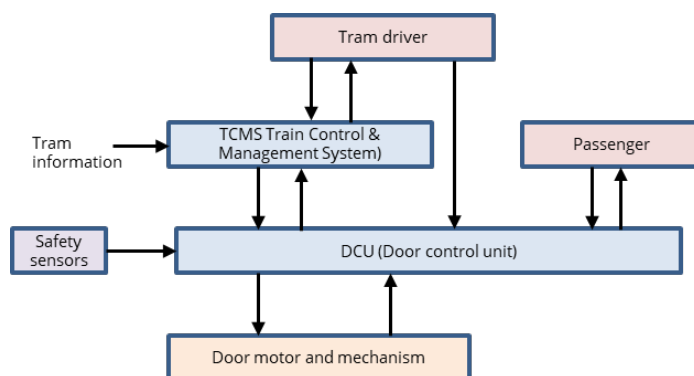


Figure 3. A functional level block diagram of the tram door control system in GoA1 level

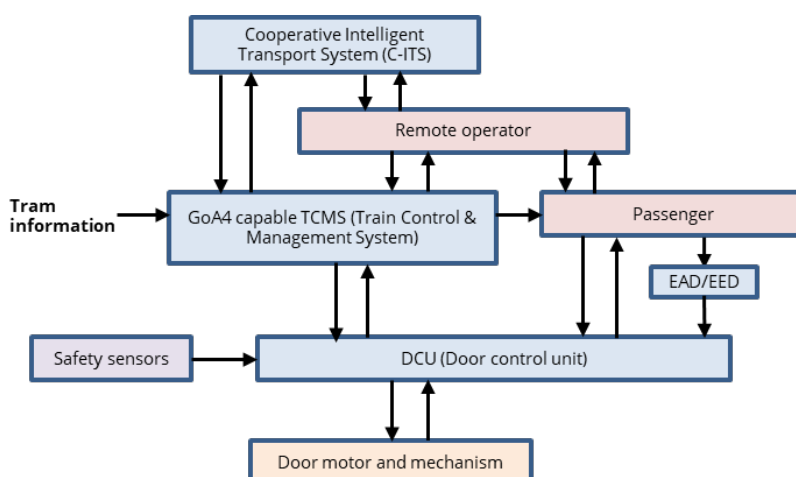


Figure 4. A functional level block diagram of the tram door control system in GoA4 level.

4. Methods and their implementation

4.1 Preliminary Hazard Analysis (PHA) method

Preliminary hazard analysis (PHA) is a semi-quantitative analysis that is performed to identify all potential hazards and accidental events that may lead to an accident, to rank the identified accidental events according to their severity, and to identify required safety measures and follow-up actions (Rausand, 2005).

According to Rausand (2005) the typical steps in PHA are: PHA prerequisites; Hazard identification; Course and consequence estimation; and Risk ranking and follow-up actions. The PHA methodology is described in detail e.g., in Rausand (2005) and in Vincoli (2006).

In this case hazards, hazardous situations, problem situations and uncertainties related to the use of tram doors were identified in various levels of autonomy (from GoA1 to GoA4). The causes and consequences were defined but the risk estimation was not done in this case.

Hazards and their consequences were examined in terms of both safety and tram operating process.

- Loss of life or injury to people
- Disturbance of the tram operation

The following aspects were considered in the analysis:

- Opening and closing a door. When it is done and under what conditions it can happen.
- Observation and monitoring of situations in the door areas, observation of the situation and traffic at the tram stop.
- Observation of passengers and effects on tram operations, e.g., visually impaired passengers, passengers having prams, passengers using wheelchairs, and passengers with reduced mobility.
- Management of emergency situations and use of doors.
- Traffic problems, congestion, situations caused by passengers, difficult conditions.
- Disturbances and malfunctions of the tram control system or infrastructure systems.
- Traffic accidents, emergency situations.

It was evaluated how the use of the doors changes as the autonomy increases, compared to the use situations of manual operation. Current preparedness was recorded and evaluated. Needs for additional analyses or additional safety measures were proposed as results of the evaluation.

The analysis considered also GoA3 level autonomy, where the tram operates autonomously, but still has a representative of the operator onboard in the tram. However, the GoA3 level was assessed to unlikely in tram operation in the future. The autonomy will go directly from GoA level 2 to level 4.

PHA of the tram door system (in GoA1-GoA4 levels) was conducted in close collaboration with Tamware Oy's experts in spring 2021. The effects of various levels of autonomy on the use and operation of tram doors in different operating situations was discussed at a workshop in March 2021 together with experts from Tamware Oy and Skoda Transtech Oy.

VTT prepared a preliminary analysis as the basis for the joint analysis sessions. The analysis was documented in EXCEL worksheets (Figure 5).

ID	Description of the door use and operation in different GoA levels	Possible hazards and problems	Causes	Consequences	Current safety measures	Proposals for further actions or needs for more detailed analyses	Comments

Figure 5. An example of the PHA worksheet structure.

4.2 System Theoretical Process Analysis (STPA) method

Analysis of the control and functions of the tram door system was done using System Theoretical Process Analysis (STPA). STPA is a recent hazard analysis method based on STAMP (Systems-Theoretic Accident Model and Processes). STAMP is an accident causality model based on systems theory, considering safety as a control problem instead of focusing on failures or deviations. STPA describes the system as a hierarchical control structure consisting of feedback loops, intending to incorporate various causal factors, including software aspects, as well as human and organizational factors. STPA provides a systematic procedure to identify flaws within the safety control structure (Leveson, 2012).

The STPA process has been described in the freely available STPA Handbook, which has seen several updates and revisions over the years (Leveson & Thomas, 2018). The Handbook also provides definitions for the key concepts and terminology used in STPA.

Leveson and Thomas (2018) define the method in four steps as follows (Figure 6):

- **Step 1** defines the scope and limitations of the analysis including definitions of losses, hazards, and safety constraints.
- In **Step 2**, the system is modelled as a hierarchical control structure, which is a system model composed of feedback control loops. This is a graphical representation featuring controllers and controlled processes represented as rectangles, and the interactions between them (control and feedback) represented as arrows. The hierarchy is illustrated by the vertical axis, i.e., the highest control authority is at the top of the diagram.
- In **Step 3**, the control structure is systematically analyzed to find unsafe control actions (UCAs) that, in a particular context and worst-case environment, will lead to a hazard.
- Finally, **Step 4** concludes with the identification of loss scenarios, which describe the causal factors that can lead to UCAs and hazards.

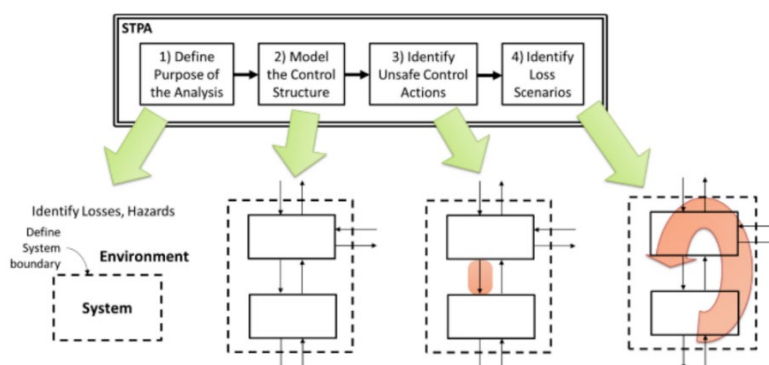


Figure 6. Four steps of STPA method (Leveson & Thomas, 2018).

STPA was first done for the GoA1 implementation describing the current state of the door control system in trams. Tamware Oy provided VTT with information on a typical control system architecture of a tram door system, its functionalities, signals, and interfaces to other systems e.g., TCMS. VTT drew up a diagram of the door system control structure in accordance with STPA as the basis for the identification and analysis of unsafe control actions. Identification of unsafe control actions and creation of loss



scenarios were conducted in autumn 2021. The GoA1 level STPA results were reviewed in the project team by the end of 2021.

Tamware Oy organized a workshop on November 30, 2021, in collaboration with Skoda Transtech Oy and VTT, which discussed the operation concepts of the tram system and the possible hierarchy of control systems at the GoA4 level.

Based on the workshop on November 30, 2021, VTT prepared an outline of the control structure for the operation of the autonomous tram system and the interactions between the main system elements for the GoA4 level STPA analysis. The operation of the autonomous tram concept was examined using STPA, from the overall management of public transport (C-ITS) to the management of the tram system, to the control of an individual tram and all the way to its door system. The impact of autonomy on door operation in different usage situations was evaluated.

5. Results

5.1 PHA results

Safety analysis of tram door system was first conducted by using the Preliminary Risk Analysis (PHA) method. The aim of the analysis was to identify hazardous situations or foreseeable problems of the tram door system at various levels of autonomy. All the PHA results: hazards, hazardous situations, causes and consequences and proposals for additional safety measures were reported in detail in Finnish to Tamware Oy. Summary of the results were presented to the SmartRail2 project steering committee, and the main findings were also summarised in a presentation in Automation Days in Helsinki, March 28-29, 2023 (Tiusanen et al., 2023).

5.1.1 Use of tram doors in GoA1 level daily operations

The use cases of the tram doors were defined as the starting point of the risk analysis. A rough structuring of the main phases of daily tram operations was prepared for the risk analysis (Figure 7).

When trams are operated in GoA1 level, the tram driver drives the tram following the traffic rules and closes the doors at the tram stops. The doors are opened automatically at the tram stops. In GoA 2 level, the driving is automated, the doors are opened automatically at the tram stops but the tram driver closes the doors at the tram stops. In the GoA4 level the tram operates unmanned, and the doors open and close automatically.

Hazardous situations related to the use of the door system were identified in the following situations of tram daily operation:

- Before an operating shift (at the depot)
- Operating events
 - Starting off, driving on the track, driving on the street, condition monitoring while driving
 - Stopping at a stop, opening the doors, closing the doors, starting off from the stop
 - Operation at the end of the tram line, changing driving direction
 - Control room operations
- After an operating shift (at the depot)
 - Switching off the door system, exiting the tram
- Special situations
 - Emergency door opening
 - Mechanical or electronic decommissioning of the door system
 - Considerable damage to the door system



Figure 7. The main phases of tram daily operations and the use of doors.

Tamware Oy defined the tram door operating modes for the analysis. Different options for opening the tram doors are:

- Option 1: Automatic operation. Train Control and Management System (TCMS) + door controller (DCU) opens the doors according to the specified conditions. Location information about being at the stop is currently not available.
- Option 2: Driver operation. The driver presses the button, after which the DCU (after a request via TCMS) opens the doors.
- Option 3: Passenger use. The doors are released for passenger use first by the driver. The passenger then presses the button intended for them, after which the DCU opens the doors. Passengers can also press the unlock button before the driver's release command, in which case the unlocking takes place immediately after receiving the release command.

5.1.2 Ensuring the correct functioning of the doors

At GoA1 and GoA2 levels, the driver performs a 'roadworthiness' check for the tram at the depot before the operating shift. At the GoA3 level, 'roadworthiness' is checked either by the supervisor or the depot staff. At the GoA4 level, the roadworthiness check will be done either by the depot staff or it will be done automatically. A fully automatic 'roadworthiness' inspection would be challenging.

As part of the 'roadworthiness' check the tram doors are calibrated at the depot. This means that the doors are opened and close to from one end position to another. In the calibration the operation of the safety devices is evaluated. Calibration (i.e., determination of the maximum opening) is done for each door - there may be minor differences in the opening of the doors after calibration. An approved calibration is valid until the next calibration. If the calibration is forgotten at the depot, it can be done automatically at the first tram stop. Moving to the GoA4 level operation does not affect the calibration process.

5.1.3 Ensuring the safe functioning of the doors during normal operation

When the tram is moving on the route, a general requirement is that all doors must be mechanically closed and locked, so that the safety interlocking circuit (so-called Green Loop) is connected. In practice this means that a door can not open due to a single technical failure, system malfunction or manual action while the tram is moving. In the event of a door system failure, the door can be taken out of use either electrically or mechanically (the safety interlocking circuit remains connected despite the door being taken out of use).



The correct closing of the door, its movement in the doorway and problem situations are monitored in all GoA levels with several safety sensors. In current tram systems at GoA1 and GoA2 levels monitoring circuits include pulse sensors, current detectors, limit switches, tactile edges, and photocells. Failure in a safety related components can initiate an emergency braking function.

5.1.4 Hazards and foreseeable problems during tram operation

As mentioned earlier all the PHA results: hazards, hazardous situations, causes and consequences and proposals for additional safety measures were documented in EXCEL worksheets and reported in detail in Finnish to 'Tamware Oy. Among others the following hazards, hazardous situations and problems that may arise during the operation of the tram in different level of autonomy were identified and discussed:

- The doors are opened in the wrong place, e.g., outside the tram stop area or from the wrong side of the tram car in the street.
- The door or doors do not close properly, or the safety system trips for some reason.
- The door does not open due to an obstacle (due to e.g., an extra object, ice or packed snow in the doorway, snowbank in the tram stop).
- The strap or string of the bag or backpack gets caught between the doors.
- A slow-moving passenger cannot reach a safe place before the tram starts moving.
- A visually impaired passenger has problems getting on the tram car.
- A visually impaired passenger has problems using the emergency opening handle in an emergency.
- The electricity supply is interrupted, and the tram is stopped in the middle of the street traffic, e.g., due to a damage to the contact wires.

5.1.5 Special situations during tram operation

In case of a traffic accident (e.g., collision with another vehicle) a tram door can be damaged. The driver or a supervisor in a tram car can interrupt the operation unless the wagon's sensors / diagnostics detect the situation at GoA1, GoA2 and GoA3 levels. If a single door is damaged, the other doors are still available for exiting the tram car. At GoA4 level the door system may not notice if the door has been hit. In the worst case, the tram continues moving normally after a bump, unless the passengers intervene with the emergency buttons. The door safety system could be developed so that it can detect an impact in a collision situation.

In case of a considerable damage to the door system when for example a door glass gets broken or a whole door leaf comes off the driver or a supervisor in the tram car can detect the situation and can stop the tram at GoA1, GoA2 and GoA3 levels. The door glasses do not have an integrated break detection. If a whole door leaf comes off that will most probably be detected by the safety interlocking circuit. At GoA4 level damage to the door system may not be automatically detected by the door control system. The control room can intervene in the situation remotely if the situation is detected. Detection could be done if one of the passengers has raised an alarm with the general alarm button.

5.2 STPA results

Alongside PHA, VTT conducted a safety analysis of the tram door system applying the STPA method. STPA aims to identify scenarios leading to dangerous situations, "unsafe control actions", and based on them, in this case, define the necessary measures to ensure safety of an automatic tram door system in all foreseeable use cases and operating situations.

The objectives of the STPA study were to:

- Apply the new STPA safety analysis method to the door system.
- Support and supplement the previously performed PHA analysis.



- Identify the new safety aspects related to the increasing the level of automation.
- Compare findings from the current GoA1 operation and the GoA4 operation concept.

STPA analysis was first done for a typical GoA1 level door control system. To identify the effects of increasing level of automation on the tram door systems the STPA analysis was continued with a GoA4 level tram control concept. The results are presented here following the four STPA study steps.

5.2.1 Step 1: Losses, hazards, and safety constraints

Losses are defined as any losses unacceptable to stakeholders. The losses can be related to safety of humans, but also other types of losses, such as operational aspects. To support traceability, the losses are labelled (L-1, L-2, L-n). In Step 1 of both GoA1 and GoA4 STPA analyses, the following two losses were considered.

L-1: Loss of life or injury to people

L-2: Disturbance of the tram operation

In STPA, hazard is a system state that will lead to a loss with a particular set of worst-case environmental conditions. Hazards identified in system-level were also similar in both GoA1 and GoA4 levels. The hazards are labelled as well, and they are linked to the losses. The hazards considered in these studies are the following:

H-1: Person is crushed or trapped between closing doors. [L-1][L-2]

H-2: Doors are open in a situation when they should be closed. [L-1][L-2]

H-2.1: Doors open while the tram is in motion. [L-1]

H-2.2: The tram departs with the doors open. [L-1][L-2]

H-2.3: Doors open when the tram is stopped, but it is not safe to open the doors [L-1]

H-2.4: The door or door glass is not in place when the tram is in motion. [L-1][L-2]

H-3: Doors do not open as requested at a tram stop. [L-2]

H-4: Doors do not close as requested at a tram stop. [L-2]

H-5: Doors do not open in an emergency. [L-1]

After the hazards have been identified the safety constraints were defined. Safety constraints specify system conditions or behaviours that need to be satisfied to prevent hazards (and prevent losses) (Leveson & Thomas, 2018). Once the system-level hazards are identified, it is quite straightforward to identify safety constraints that must be enforced: simply invert the conditions.

SC-1: Doors shall not close when there is a person between the closing doors. [H-1]

SC-1.1: If doors close when there is a person between the closing doors, this must be detected, and safety measures must be taken to prevent crushing hazards. [H-1]

SC-1.2: If doors close when there is a person or an object (e.g., a bag) trapped between the closing doors, this must be detected, and safety measures must be taken to prevent trapping hazards. [H-1]

SC-2: Doors shall not open in a situation when they must be closed. [H-2]

SC-2.1: If doors open while the tram is in motion, this must be detected, and safety measures must be taken to prevent hazards. [H-2.1]

SC-2.2: If the tram departs with a door open, this must be detected, and safety measures must be taken to prevent hazards. [H-2.2]

SC-2.3: If doors open when the tram is stopped, but it is not safe to open the doors, this must be detected, and safety measures must be taken to prevent hazards. [H-2.3]

SC-2.4: If a door or door glass is not in place when the tram is in motion, this must be detected, and safety measures must be taken to prevent hazards. [H-2.4]



SC-3: If doors do not open as requested at a tram stop this must be detected and safety measures must be taken to prevent hazards. [H-3]

SC-4: If doors do not close as requested at a tram stop, this must be detected, and safety measures must be taken to prevent hazards. [H-4]

SC-5: The doors must be able to be opened in an emergency. [H-5]

According to Leveson & Thomas (2018) each safety constraint can be traceable to one or more hazards, and each hazard is traceable to one or more losses. In general, the traceability need not be one-to-one; a single safety constraint might be used to prevent more than one hazard, multiple safety constraints may be related to a single hazard, and each hazard could lead to one or more losses. The safety constraints do not specify a particular safety solutions or implementations of safety systems to prevent hazards. Safety constraints can also define how the system must minimize losses in case the hazards do occur. (Leveson & Thomas, 2018)

5.2.2 Step 2: Control structures

In STPA Step 2, the system model for GoA1 level tram door implementation was built according to information and documents received from Tamware Oy including written technical specifications and descriptions of control signals to and from, and within, the door system. The general technical requirements for train and tram door control systems are specified in the standard EN 14752:2019 Railway applications - Bodyside entrance systems for rolling stock (EN 14752:2019 + A1:2021).

In Figure 8, a control structure of a GoA1 system used in STPA is presented. There are multiple options for how a GoA1 system functionality can be implemented, and this represents one configuration for the STPA study. In the door control system described in Figure 8, the tram driver enables the doors at a selected side of the tram before arriving to a stop. This means that when the tram comes to a stop, the doors can be opened either by the driver or by a passenger using the door button. The doors also close automatically after a pre-set time in case there are no obstacles detected by safety sensors in the doorway. There are safety sensors which detect collision of the door with object or person between the doors. Persons with reduced mobility (PRM) can request door opening by pressing the PRM button on the door, in which case the driver must close the doors after confirming that the passenger has moved to a safe distance.

Safety interlocking system (Green loop) prevents the tram from moving if any of the doors is not closed correctly. This ensures that the tram cannot depart without closing the doors first. In case of malfunctions, the driver has the possibility to turn off the automatic door controls and directly operate the doors or, if needed, isolate individual doors so that they are put out of use. Depending on the situation, this can be done electronically or by a physical switch at the door. In emergency situations where the tram needs to be evacuated, the driver opens the doors. Additionally, the passengers can use physical handles of the emergency egress devices (EED) located by the doors.

The doors are operated by a Door Control Unit (DCU), which provides the opening and closing commands to the door actuators and gathers relevant sensor data. The information of door enabling status, open and close requests, as well as information of whether the tram is in motion, is provided to the DCU by the Train Control & Management System (TCMS). TCMS is a central system in rail vehicles, integrating information from several sources and controlling many of the train subsystems (Härri, et al., 2019).

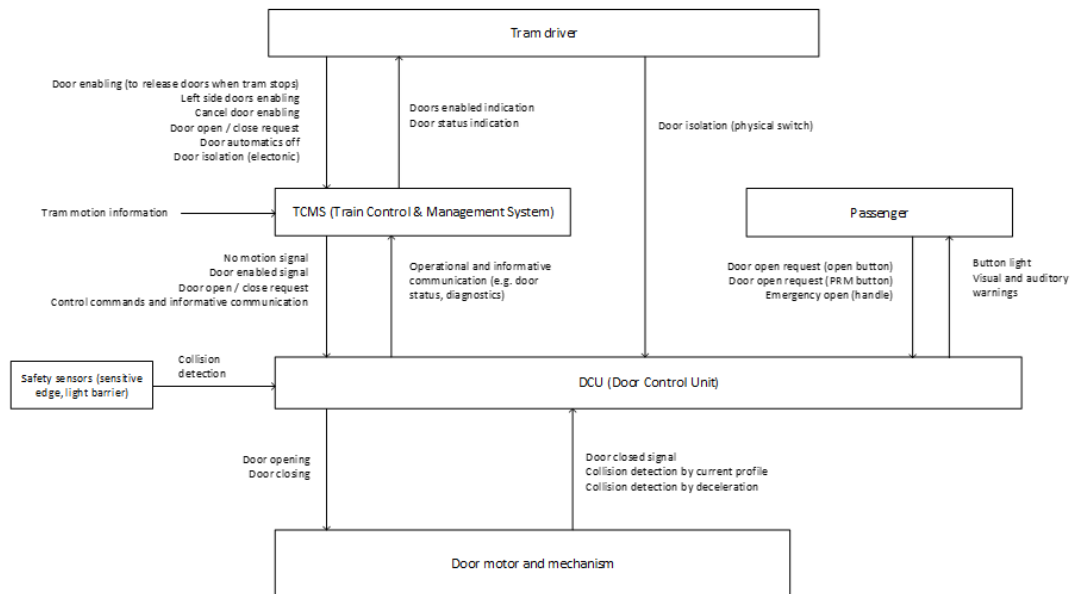


Figure 8. STPA control structure of a tram door controls for GoA1 level analysis (Heikkilä et al., 2022).

In Figure 9, a control structure of a GoA4 system concept is presented. As GoA4 trams do not yet exist, this system model is provisional and based on assumptions of experts from Skoda Transtech Oy and Tamware Oy involved in the workshop on November 30, 2021. In the GoA4 level model, it should be noted that only the systems related to the operation of the door systems are incorporated in the model. In addition to the depicted system elements, GoA4 operation will introduce several changes in other systems, for example related signalling, which was outside the scope of the analysis.

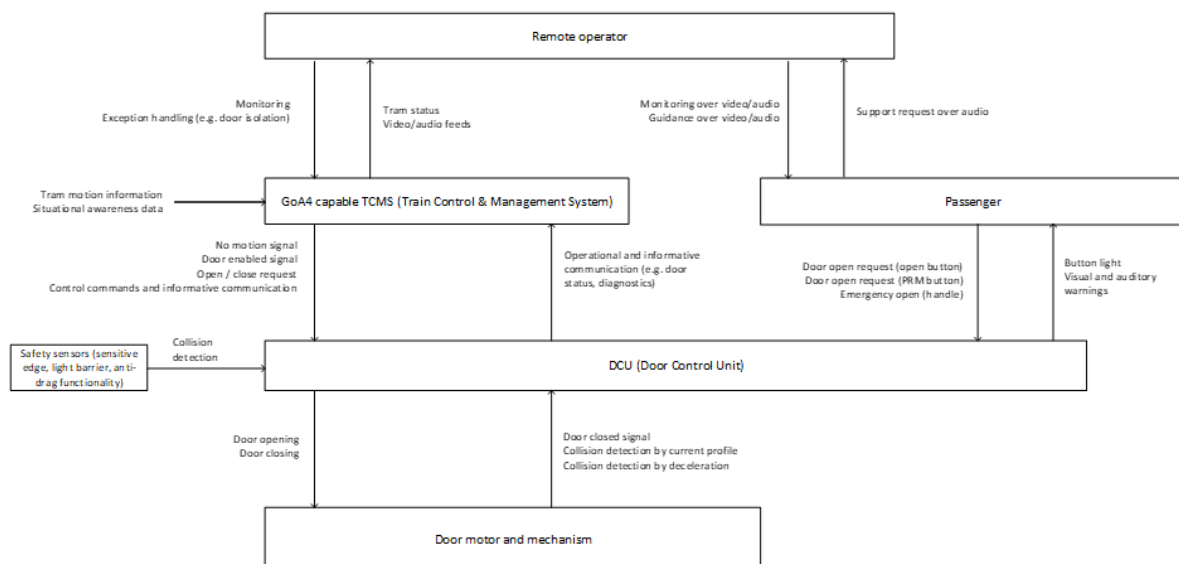


Figure 9. STPA control structure of a tram door controls for GoA4 level analysis (Heikkilä et al., 2022).

5.2.3 Steps 3 and 4: Identification of unsafe control actions and loss scenarios

Safety constraints specified in Step 1 describes the system conditions or functionalities that need to be satisfied to prevent hazards (and prevent losses). The actual analysis work in STPA is done in Steps 3 and 4 in which the aim is to systematically identify and analyse of scenarios that can violate these safety constraints, leading to system-level hazards and losses.



The analysis started by analysing the existing Control Actions (CA) in GoA1 level (See Figure 8) and planned control actions in GoA4 level (See Figure 9) to identify how and in what conditions the control actions could turn into unsafe control actions and cause a hazardous situation.

According to Leveson & Thomas (2018) an Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard. There are four ways a control action can be unsafe (Leveson & Thomas, 2018):

1. Not providing the control action leads to a hazard.
2. Providing the control action leads to a hazard.
3. Providing a potentially safe control action but too early, too late, or in the wrong order
4. The control action lasts too long or is stopped too soon (for continuous control actions, not discrete ones).

Examples of identified unsafe control actions related to five control actions in GoA1 level operation are shown in Figure 10.

CA	Control action	Providing causes hazard	Not providing causes hazard	Providing too soon / too late / in wrong order causes hazard	Stopping too soon / applying too long causes hazard
CA-1	Tram driver provides door enabling command to TCMS	UCA-1.1 Tram driver provides the door enabling command but the tram fails to stop at the stop area [H-2]		UCA-1.2 Tram driver provides door enabling early, causing the doors to open outside the stop [H-2]	
CA-2	Tram driver provides left side door enabling to TCMS	UCA 2.1 Tram driver provides left side door enabling when arriving at stop where left side doors should stay closed [H-2]			
CA-3	Tram driver cancels door enabling by providing central close command to TCMS		UCA 3.1 Tram driver does not cancel door opening when the next stop is unusable [H-2] UCA-3.2 Tram driver does not cancel door opening when the tram needs to stop before the stop area [H-2]	UCA-3.3 Tram driver executes cancelling too late and the doors open as requested by the passengers. [H-2]	
CA-4	Tram driver provides emergency force open command to TCMS	UCA 4.1 Tram driver provides emergency force open command accidentally in a situation where it is not needed [H-2]	UCA-4.2 Tram driver does not provide emergency force open command in emergency situation [H-5]		
CA-5	Tram driver provides door automatics off command to TCMS	UCA-5.1 Tram driver sets door automatics off in a situation where automation could be used [H-2][H-3][H-4]			

Figure 10. Examples of identified unsafe control actions in GoA1 level STPA.

In Step 4 all the identified UCA's were analysed, and the loss scenarios were described. The scenarios describe tram operating conditions (e.g., traffic situation, weather conditions, tram driver actions, passenger behaviour) and chains of events, because of which it could be possible for the UCA in question to be realized and cause a hazardous situation. The following types of loss scenarios were specified for the identified unsafe control actions:

- Loss scenarios related to commands given by tram driver.
- Loss scenarios related to signals from TCMS.
- Loss scenarios related to actions of passengers.
- Loss scenarios related to EAD/EED.
- Loss scenarios related signals from DCU.
- Loss scenarios related to door isolation.
- Loss scenarios related to sensor systems.

Figure 11 presents examples of loss scenarios created in GoA1 level STPA in relation to control actions and unsafe control actions presented in Figure 10.



Scenario description	Related C
Tram driver provides the door enabling command but the tram fails to stop at the stop area, causing the doors to open in a dangerous area. The tram can stop at wrong area due to: - Brake failure. - Erroneous braking by driver. - Unexpected need to stop before the stop area, e.g. obstacle on tracks.	CA-1
Tram driver provides left side door enabling when arriving at stop where left side doors should stay closed. This allows passengers to exit on the upcoming tracks or to stop area that is not in use. This can be caused by: - Tram driver provides the enabling by pushing the button accidentally. - Tram driver provides the enabling erroneously when arriving at a stop where there is no left side platform. - Tram driver provides the enabling when arriving at a stop where the left side platform is obstructed/not in use.	CA-2
Tram driver does not cancel door enabling when the next stop is unusable. - The driver forgets that the doors are enabled. - The driver needs to react to a surprising situation, making it impossible to cancel enabling.	CA-3
The driver cancels door enabling too late, allowing the doors to open in a dangerous area.	CA-3
Tram driver provides emergency force open command accidentally in a situation where it is not needed, causing the doors to open in a dangerous area.	CA-4
Tram driver sets door automatics off in a situation where automation could be used. - The driver does not understand the automatic/manual operation correctly and thus deactivates automatics unnecessarily.	CA-5

Figure 11. Examples of loss scenarios created in GoA1 level STPA.

An example of STPA results is presented in Table 2. It summarizes the results from one 'Loss Scenario' description backwards to the 'System Loss' defined in the beginning of the analysis. This example might clarify the aim of the analysis and reasoning for all the steps.

Table 2. An example of GoA1 level STPA results.

STPA step	Output of the step	Description of the output
4	Loss scenario [LC-2]	Tram driver provides left side door enabling when arriving at stop where left side doors should stay closed. This allows passengers to step out into the driveway, step out on the tracks or to tram stop area that is not in use. [UCA-2][CA-2] [SC-2.3][H-2.3][L-1] This can be caused by: <ul style="list-style-type: none"> Tram driver provides the enabling by pushing the button accidentally. Tram driver provides the enabling erroneously when arriving at a stop where there is no left side platform. Tram driver provides the enabling when arriving at a stop where the left side platform is obstructed/not in use.
3	Unsafe control action [UCA-2]	Tram driver provides left side door enabling when arriving to a tram stop where the left side doors should stay closed [CA-2][SC-2.3][H-2.3][L-1]
2	Control action [CA-2]	Tram driver provides left side door enabling to TCMS.
1	Sub safety constraint [SC-2.3]	If doors open when the tram is stopped, but it is not safe to open the doors, this must be detected, and safety measures must be taken to prevent hazards. [SC-2][H-2.3][L-1]
1	Safety constraint [SC-2]	Doors shall not open in a situation when they must be closed. [H-2][L-1]
1	Sub hazard [H-2.3]	Doors open when the tram is stopped, but it is not safe to open the doors [L-1]
1	Hazard [H-2]	Doors are open in a situation when they should be closed. [L-1][L-2]
1	System Loss [L-1]	Loss of life or injury to people



6. Discussion

In cities trams share the same infrastructure with other traffic which makes higher autonomy much more difficult than metros and city trains that have an independent network. Many of the new autonomy related safety risks in trams arise from the complexity of sharing the same street infrastructure with cars, cyclists and pedestrians, and unexpected behaviour of the tram passengers. Increasing the level of automation in tram operations is a challenging task as the trams operate in an open environment with many uncertain elements.

6.1 Safety aspects in tram door usage in GoA1 versus GoA4

The safety functionality which ensures that the tram cannot move with doors open is already very robust in the GoA1 system. Similarly, the sensors that ensure that no persons or objects are trapped between doors are already in place. In the case of GoA4, additional safety sensors should be added to ensure that even very thin objects (e.g., belt or dog's leash) trapped between the doors can not cause any accidents (anti-drag functionality). This kind of technology is already available and can be applied at different GoA levels. At GoA4, the remote operator should be able to monitor the door system status and resolve malfunctions in the door system, for example by disabling a malfunctioning door over a remote connection.

One significant difference between the GoA 1 and GoA4 levels is related to the role of the driver, who is in the case of GoA4 system replaced by a remote operator monitoring and managing the operation. At GoA1, the driver is in the cabin, and is responsible for observing that the doors are enabled only when it is safe to do so. The driver also observes the closing of the doors and can intervene if needed. The driver can also observe the near surroundings of the door for other disturbances, such as any loose objects on the platform. At GoA4, such continuous observation is not available, and sufficient situational awareness needs to be achieved by technical systems. In metro systems platform screen doors help to confine the train and to effectively ensure there are no obstacles beside the doors. In trams, however, platform screen doors seem unlikely to be implemented at tram stops. Thus, higher level of monitoring of the surroundings of the doors will be required. This may be a part of the situational awareness data collected by the tram systems and processed by the TCMS, but observation of the environment can be envisioned as a part of the door system in the future as well.

At all levels of tram autonomy, the DCU controls the actuators that are responsible for opening and closing the doors. For the DCU, no major changes are expected in GoA4 operation, if the commands it receives are correct. Especially the positioning data managed by TCMS is of utmost importance: as there are no personnel on board to confirm the location of the tram at the platform, the positioning accuracy needs to be sufficient for aligning the tram and all its doors with the platform. To achieve this, various positioning methods, such as satellite navigation as well as balises or other types of beacons can be applied. It should be considered whether further sensors are needed for individual doors to ensure their placement at the platform.

As the level of autonomy increases there will be needs for major changes in Train Control & Management Systems (TCMS). The TCMS system monitors and controls several systems within the tram, including the DCU. In GoA1 operation, the TCMS processes the commands given by the driver, providing the necessary information to the door control unit to determine when the doors can be opened. In GoA4, this capability of deciding whether the doors can be opened needs to be incorporated in the TCMS.

6.2 New challenges in tram door usage in GoA4

Based on the analysis results, challenging situations in GoA4 level tram operation can arise with passengers who move slowly, have reduced mobility, use wheelchair or are visually impaired. Solutions to ensure accessibility and safe entry and exit for all passengers must be developed. From the perspective of the passenger, the changes in door operation are not necessarily evident in normal operation when

beyond the obvious



changing from GoA1 level to GoA4 level. For example, the buttons used to request door opening function similarly in both cases. Currently, in GoA1 level operation passenger can use a PRM 'People with Reduced Mobility' button. By using the button, the passenger indicates to the tram driver that a certain door and door area need special attention. In case the door opening is requested by the PRM button in GoA4 operation, the door system (or the TCMS) needs to determine when the door can be safely closed, or the closing needs to be delegated to the remote operator. The need for various access devices, such as lifts or ramps, also needs to be considered, as their operation also needs to be safely automated.

It was clearly noticed in this study that it is impossible to develop sensing capabilities for all situations related to the use of tram doors during daily tram operations. In GoA4 level operation possibility to response to exceptional situations could be given to the passengers. A general alarm button, which a passenger could press to connect to the tram's remote control and whose user would not have to be afraid of any sanctions (compared to the emergency brake handle), is one option. Passengers could contact a person who can manage the situation and organize help on the spot if necessary and information on how to act. Control room support for passenger, as is used in elevators, could even be a mandatory feature in GoA4 level tram systems. The most extreme example is evacuation in an emergency. For this purpose, a reliable communication link is needed between the remote operator and the tram in GoA4 applications, so that the remote operator can do emergency opening of the tram doors and give instructions to the passengers. However, in an accident, the communication connection may also be lost due to the accident and additional measures may need to be considered.

The time spent at the tram stop is critical factor in tram operations. To speed up the exit of passengers from the tram at levels at GoA1 to GoA3 levels, the driver/supervisor could give permission to open the doors before the speed has dropped below the opening speed limit. The door can be opened as quickly as possible at the passenger's request. The photocell in the doors can also be deactivated to speed up the stop event. At GoA4 level, to speed up the exit, passengers could be directed to the less crowded doors with visual and audible information. The number of people at the door area could be scanned by e.g., using advanced surveillance camera technology. On the other hand, the safety measures required for autonomous operation (e.g., photocells being constantly on at the door openings) may slow down the closing or opening of the doors if there are of passengers in the door area.

6.3 Experiences of the analysis methods in this context

Our experiences and results of the STPA studies seems to be in line with the results Leveson and Thomas (2018) have stated. STPA can be used in several different phases of a system engineering process, starting in the earliest concept development stage as experienced in this study regarding GoA4 concept. STPA can be used to generate high-level safety requirements early in the concept development phase, refine them in the system requirements development phase. The system requirements and constraints can then assist in the design of the system architecture and more detailed system design and development.

The results and our experience using the PHA and STPA methods in this study reinforces our belief that STPA complements and in a way continues the safety analysis made applying PHA. In the PHA, hazards and dangerous situations are identified at a general level without going into more detail about operating procedures, system usage situations or control actions. In STPA then specifies control actions, identifies unsafe control actions (UCAs) that must be prevented. As Leveson and Thomas (2018) express, STPA identifies UCAs that must be prevented, and the UCAs are then used to derive functional requirements and make design decisions to prevent or mitigate the UCAs. After potential unsafe behavior is identified, then the specific design features can be created, and safeguards added (if the design does not already exist) or the adequacy of existing design decisions and safeguards can be determined (if the design already exists). STPA also promotes traceability throughout the development process so decisions and designs can be changed with minimum requirements for redoing previous analyses.

7. Conclusions

The results of the PHA and STPA analyses show that many parts of the door systems are already capable for GoA4 tram operations. There are safety systems ensuring that the doors do not open when the tram is in motion, and to detect obstacles between the doors.

Solutions to ensure accessibility and safe entry and exit for all passengers must be developed for GoA4 operation considering especially passengers who move slowly, have reduced mobility, use wheelchair or are visually impaired.

Managing of abnormal situations and emergencies needs to be carefully considered in GoA4 operation. For example, to ensure that the tram can be evacuated safely if needed, and that management of technical and human disturbances with the door systems could be managed remotely. The results show the importance of accurate positioning information in GoA4 operation to ensure that the doors are only opened at correct locations. As the near surroundings of the doors are no more observed by the driver, situational awareness around this area needs to be improved.

The door system, however, is only one aspect of the tram operation and other parts are subject to a significant change. Thus, on the path towards automated tram operations, comprehensive safety analyses of all parts of the system and operations are still needed. Systemic methods, such as STPA, can be applied to support these analyses.

The results of the analyses can be used to support development of the door systems by focusing the development actions into the areas where the major changes and improvement needs are expected.

References

- Clinnick, R. 2021. DB and Siemens demonstrate automated S-Bahn train in Hamburg. International Railway Journal. Available: <https://www.railjournal.com/signalling/db-and-siemens-demonstrate-automated-s-bahn-train-in-hamburg/>
- Connolly, K. 2018. Germany launches world's first autonomous tram in Potsdam. The Guardian, World. Available: <https://www.theguardian.com/world/2018/sep/23/potsdam-inside-the-worlds-first-autonomous-tram>
- Emery, D. 2017. Towards Automatic Train Operation for long distance services: State-of-the art and challenges. 17th Swiss Transport Research Conference, 17-19 May 2017, Ascona, Switzerland.
- EN 14752:2019 + A1:2021 Railway applications. Bodyside entrance systems for rolling stock.
- Flaherty, N. 2021. Fully automated depot has self-driving trams. Technology News, August 27, 2021. Available: <https://www.eenewseurope.com/en/fully-automated-depot-has-self-driving-trams/>
- Heikkilä, E., Malm, T., Välisalo, T., Tiusanen, R., Hämäläinen, M. & Järvinen, M. (2022) Systemic safety analysis of a tram door system considering increasing level of automation. Poster in the Transport Research Arena (TRA) Conference in Lisbon 14.-17.11. 2022.
- Härri, J., Arriola, A., Aljama, P., Lopez, I., Fuhr, U. & Straub, M. (2019). Wireless technologies for the next-generation train control and monitoring system. IEEE 5G World Forum, 5GWF 2019 - Conference Proceedings, 179–184.
- IEC 62290-1:2014 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts.



- Kate Connolly, K. 2018. Germany launches the world's first autonomous tram in Potsdam. The Guardian, World. Available: <https://www.theguardian.com/world/2018/sep/23/potsdam-inside-the-worlds-first-autonomous-tram>
- Leveson, N., 2012, Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, USA.
- Leveson, N. & Thomas, J., 2018, STPA Handbook. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- Pyrgidis, C. N. 2021. Railway Transportation Systems: Design, Construction and Operation. CRC Press.
- Rausand, M. 2005 Preliminary Hazard Analysis. System Reliability Theory (Second ed), Wiley, 2004 – 1 / 36. Available: <https://kntu.ac.ir/DorsaPax/userfiles/file/Mechanical/OstadFile/kazerooni2/PreliminaryHazardAnalysis.pdf>
- UITP (2018). World Report on Metro Automation. UITP Statistic Brief. Available: https://cms.uitp.org/wp/wp-content/uploads/2020/06/Statistics-Brief-Metro-automation_final_web03.pdf
- Tiusanen, R., Heikkilä, E. Malm, T. & Välisalo, T. 2023. Towards automated tram systems – risk analysis case studies. Available: <https://www.automaatioseura.fi/automationdays2023/accepted-abstracts/>
- Vincoli, J. W. (2006). Basic Guide to System Safety. Hoboken, NJ: John Wiley & Sons, Inc.

Certificate Of Completion

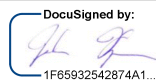
Envelope Id: 66F3206382874A74BCF346D3AC042649	Status: Completed
Subject: Complete with DocuSign: VTT-R-00499-23.pdf	
Source Envelope:	
Document Pages: 21	Signatures: 1
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Christina Vähävaara
Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	Vuorimiehentie 3, Espoo, .. . P.O Box1000,FI-02044 Christina.Vahavaara@vtt.fi IP Address: 130.188.40.68

Record Tracking

Status: Original	Holder: Christina Vähävaara	Location: DocuSign
25 September 2023 12:47	Christina.Vahavaara@vtt.fi	

Signer Events

Johannes Hyrynen
johannes.hyrynen@vtt.fi
Lead, Low carbon and smart machines
Teknologian tutkimuskeskus VTT Oy
Security Level: Email, Account Authentication
(None), Authentication

Signature

Signature Adoption: Uploaded Signature Image
Using IP Address: 85.76.36.215
Signed using mobile

Timestamp

Sent: 25 September 2023 | 12:50
Viewed: 29 September 2023 | 09:59
Signed: 29 September 2023 | 10:01

Authentication Details

SMS Auth:
Transaction: 963667ed-7448-4a82-a159-0d7cc964297d
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 29 September 2023 | 09:59
Phone: +358 40 8336364

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	25 September 2023 12:50
Certified Delivered	Security Checked	29 September 2023 09:59
Signing Complete	Security Checked	29 September 2023 10:01
Completed	Security Checked	29 September 2023 10:01
Payment Events	Status	Timestamps