TECHNICAL GUIDE

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

AUTOMATED ROAD TRANSPORT SYSTEMS

Technical guide related to « GAME » demonstration for ARTS

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

Version 1 of August 31, 2022

1. **Purpose - Scope - Intended recipients**

This technical guide is an initial supplement to the STRMTG GAME Implementation Guide which explains a demonstration methodology for the "GAME" principle (Globally at least equivalent) provided for by Decree no. 2021-873 of June 29, 2021 implementing Ordinance No. 2021-443 of April 14, 2021 on the type of criminal liability applicable to the operation of an automated road transport vehicle and its conditions of use (French Automated Road Transport System Decree - ARTS Decree). This technical guide clarifies some aspects to guide the GAME approach described in the GAME Implementation Guide.

Like the Implementation Guide, this guide applies to automated road transport systems (ARTS), defined by Article R. 3151 -1 of the French Transport Code (added by Article 6 of the ARTS Decree) as *"technical automated road transport systems, deployed on predefined routes or traffic areas, and supplemented by operating and maintenance rules, for the purpose of providing a public collective or individual road transport service or private road transport service, excluding transport systems subject to Decree No. 2017-440 of March 30, 2017 concerning guided public transport safety"*.

It is intended for all professionals in the automated road transport sector, including public transport authorities, project owners, operators, engineering firms, approved qualified organizations (OQA), designers of automated road transport technical systems, and equipment manufacturers.

The provisions of this guide are intended to clarify the applicable safety regulations for certain aspects of the safety demonstration. Developed in consultation with the profession, they provide a framework to facilitate the work of professionals. It is not regulatory in nature, but observance of its provisions can be seen as an indication of compliance with the regulatory requirements relating to the GAME principle and/or the suitability of the approach adopted.

The provisions of this guide are limited to the safety of vehicle occupants and third parties with regard to the operation of the system, and to the operating phases for which the dynamic control of the vehicle is not ensured by a human driver, on roads open to public traffic (i.e. roads where there is nothing to prevent use by the public).
It is specified that under these conditions, this guide covers the safety of operating and maintenance personnel with respect to operation of the system,
- for occupants, when they are on board the system's vehicles,
- and third parties, when they are present on the route.

In addition, this guide also covers the safety of third parties when they interact with the equipment and facilities specifically installed for the system, outside the system's operating phases.

This guide does not address:
- issues related to cybersecurity;
- issues related to public safety (suspicious packages, acts of vandalism, etc.);
- issues related to regulatory obligations concerning accessibility of the transport system for people with disabilities;
- issues related to health and safety conditions for operating and maintenance staff;
- intervention and rescue procedures defined by emergency services;
- issues related to public access buildings such as stations, except for their interfaces with the transport system;
- issues related to external fire control (DECI);
- the consideration of potential risks generated by project works when they do not impact on an existing automated road transport system;

- system performance issues.

This guide does not cover all aspects of the GAME demonstration. The information it contains is specifically intended to be implemented as part of the detailed “Type 3” risk analysis presented in the GAME implementation guide.

This initial guide is intended to be supplemented in an incremental manner as work on the safety demonstration of ARTS is enriched, particularly concerning aspects related to safety objectives and risk evaluation, which will be used to decide on its acceptability.

Revision history

Version number	Author	Date	Description
1	Pierre Jouve	8/31/2022	Created by the GAME working group (ARTS)

WRITTEN BY	EDITED BY	APPROVED BY
Pierre Jouve Head of the Automated Public Transport Department	**Alexandre Dusserre** Head of the Metros and Rail Systems Department	**Daniel PFEIFFER** Director
Signature numérique de Pierre JOUVE pierre.jouve Date : 2022.11.09 15:21:04 +01'00'		Le Directeur du Service Technique des Remontées Mécaniques et des Transports Guidés Daniel PFEIFFER Daniel PFEIFFER daniel.pfeiffer 2022.11.10 15:43:15 +01'00'

Technical Service in Charge of Safety for Ropeways and Guided Transport (STRMTG)
1461 rue de la piscine
38400 St Martin d'Hères
tel.: +33 (0)4 76 63 78 78
email: strmtg@developpement-durable.gouv.fr
www.strmtg.developpement-durable.gouv.fr

1 Introduction

Decree no. 2021-873 of June 29, 2021, implementing Ordinance no. 2021-443 of April 14, 2021, on the type of criminal liability applicable in the event of the operation of an automated transport vehicle and its conditions of use, sets out the safety requirements applicable to Automated Road Transport Systems (ARTS) and in particular the “Globally at least equivalent” (GAME) principle. This decree is referred to in the rest of this document as the "ARTS Decree".

In addition to the GAME Implementation Guide, which presents the different approaches to demonstrating safety within the framework of the GAME principle, this guide aims to provide input and principles for performing a detailed risk analysis within the framework of an ARTS.

As a reminder, this detailed risk analysis is one of the possible demonstration approaches within the GAME approach. This “Type 3” approach covers the cases of systems integrating innovative equipment or functions and for which there are neither regulatory or technical standards applicable to the complete system, nor an acceptable reference system.
Therefore, this approach is based on a comprehensive analysis of the hazards and the management of each identified hazard, either according to a non-ARTS standard/reference document demonstrated to be acceptable (Type 3a), or according to an explicit analysis resulting from quantitative and qualitative measures (Type 3b).

This document further describes this detailed analysis and provides input information to initiate the analysis process.

The information detailed here is the result of joint reflection of all the participants of the STRMTG GAME working group involving professionals from across the industry. However, this guide does not claim to be exhaustive in terms of the information it provides and is intended to be enriched as feedback is received from the various cases of implementation.

This document should therefore be considered as an initial guide to:
- *Specify the framework of the Type 3 “Detailed risk analysis” approach;*
- *List the main input information to be considered in the various analyses.*

Please note that the person overseeing the analysis is responsible for supplementing or adapting these various lists of input information according to the specificities and context of the system being analyzed.

Moreover, some information from these lists does not need to be taken into account, but must be justified by the person overseeing the analysis according to the specificities and context of the system being analyzed.

2 Definitions

The following definitions are taken from Articles R. 311-1, R. 311-1-1 and R. 3151-1 of the French Transport Code:

“Dynamic control”: execution of all operational and tactical functions in real time necessary to operate the vehicle. This includes controlling the lateral and longitudinal movement of the vehicle, monitoring the road environment, reactions to road traffic events and preparing and signaling maneuvers.

“Operational domain”: the operational conditions of use of an automated road transport technical system associated with specific routes or traffic areas consistent with the system technical design domain.

“System technical design domain”: the operating conditions under which an automated road transport technical system is specifically designed to operate.

“Remote intervention”: action performed by the authorized person referred to in Article L. 3151-3, located outside the vehicle, in the context of an automated road transport system, for the purpose of:
a) Activate, deactivate the system, give instructions to perform, modify, or interrupt a maneuver, or acknowledge maneuvers proposed by the system;
b) instruct the system’s navigation system to select or modify a route schedule or user stops.

“Minimal risk maneuver”: a maneuver to stop the vehicle in a situation of minimal risk for its occupants and other road users, performed automatically by the automated driving system, following a hazard not foreseen in its conditions of use, a serious failure or, in the case of remote intervention, a failure to acknowledge the maneuver requested by the system.

“Emergency maneuver”: a maneuver automatically performed by the automated driving system in the event of an imminent risk of collision, with the goal of avoiding or mitigating it.

“Substantial modification”: any change to an existing automated road transport system or part of a system, where the change alters the safety assessment.

“Qualified organization”: an organization approved to conduct safety assessment of the design, implementation and operation of automated road transport systems.

“Predefined route or traffic area”: all the road sections or areas with defined geographical limits in which one or more automated road transport system vehicles travel or stop;
Note: in the rest of the document, “route” is used instead of "route or predefined traffic area".

“Automated Driving System”: system combining hardware and software enabling the sustained dynamic control of a vehicle.

“Automated road transport technical system”: a set of highly or fully automated vehicles, as defined in Article R. 311-1, Sections 8.2 and 8.3 of the French Highway Code, and technical installations used for remote intervention or safety;
Note: in the rest of the document, “technical system” is used instead of “automated road transport technical system”.

“Automated road transport system”: automated road transport technical system deployed on predefined routes or traffic areas, and supplemented by operating and maintenance rules, for the purpose of providing a public collective or individual road transport service or private road transport service, excluding transport systems subject to Decree No. 2017-440 of March 30, 2017 concerning guided public transport.

“Highly Automated Vehicle”: a vehicle equipped with an automated driving system with dynamic control of a vehicle within a particular operational design domain, capable of responding to any traffic hazards or failures, without requesting to regain control during a maneuver performed within its operational. This vehicle may be integrated into an automated road transport technical system as defined in 1o of Article R. 3151-1 of the Transport Code.

“Fully automated vehicle”: a vehicle equipped with an automated driving system with dynamic control of a vehicle capable of responding to any traffic hazards or failures, without requesting takeover of control during a maneuver within the system technical design domain of the automated road transport system in which the vehicle operates, as defined in 1° and 4° of Article R. 3151-1 of the Transport Code.

In addition, the following useful terms are based on definitions from existing publications or developed within the specific framework of this guide, in consultation with the profession *(when the definition comes from an existing reference document, the source is provided in italics):*

“Accident”: an unexpected event or series of events resulting in damage, which may threaten the safety of persons.

"Traffic accident": a collision between a vehicle and another vehicle or a moving or fixed obstacle.

"FMECA (Failure Mode, Effects and Criticality Analysis)": A systematic method of assessing an entity or process to identify its possible failure modes and rank their criticality, and identify their effects on the performance of the entity or process, as well as on the surrounding environment and personnel.

"Causal analysis": analysis of the reasons how and why a particular hazard can come into existence *(EN 50129:2018)*.

"Risk analysis": systematic use of all available information to identify hazards and to estimate the risk *(EU Regulation 402/2013)*.

"Safety concept": specification of the functional safety requirements, with the associated information, their allocation to the various elements of the architecture, and the description of the interactions required to achieve the safety objectives.

"Criticality": characterization of the level of risk.

"Hazard": a condition that could lead to an accident *(EU Regulation 402/2013).*

"Fault/failure": abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (IEC 61508-4:2010).

"Damage": physical injury, damage to personal health, or damage to property.

"Malfunction": wrong response of the system in two possible cases:
- in the event of a failure,
- when operating conditions occur that are not properly managed due to functional limitations (functional deficiencies).

"Equipment": single apparatus or set of devices or apparatuses, or the set of main devices of an installation, or all devices necessary to perform a specific task *(EN 50129:2018)*.

"Risk estimation": the process used to arrive at a measure of the level of risk analyzed and includes the following steps: analysis and estimation of risks, estimation of frequency.

"Risk evaluation": a procedure based on the risk analysis to determine whether an acceptable level of risk has been achieved *(EU Regulation 402/2013)*.

"Event": change in the external environment or malfunction of the system in question (e.g., ego vehicle), at a given time, which can be characterized, and which must be taken into account for a decision.

"Hazardous Event": An unwanted event that can cause a dangerous situation and an accident under certain conditions.

"Avoidability": the ability to avoid an accident through the timely reactions of those involved, possibly with the help of measures outside the vehicle.
Note 1: Persons involved may include the remote operator, potential drivers of third party vehicles, persons in the vicinity of the vehicle, and in some cases, the occupants.
Note 2: The parameter "Av" is an estimation of this avoidability.

"Safety requirements": the safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) and maintenance necessary in order to meet legal or company safety targets; *(EU Regulation 402/2013)*.

"Exposure": the state of being in a given operational situation that may be dangerous if it coincides with the hazardous event.
Note: The "E" parameter represents the average time of exposure to a given operational situation as a proportion of the total operational time.

"Severity": an estimate of the level of damage resulting from an accident.

"Infrastructure": the set of equipment that makes up the road and digital infrastructure.

"Road infrastructure": a combination of infrastructure comprising:

- The road surface;
- Road equipment and facilities, including horizontal (markings, etc.) and vertical signs (traffic lights, standard signs, variable message signs, etc.), safety elements (guardrails, cones, triangles, etc.), information media (street furniture, gantry signs, etc.) and shared passenger stations;
- Equipment and facilities specific to the automated road transport system, including off-board sensors, dedicated markings, specific fixed or retractable barriers and dedicated passenger stations.

Note 1: road infrastructure can be characterized by generic descriptors used to define infrastructure categories (e.g., number of lanes, types of traffic lights, density of street furniture, functionalities of roadside units). These descriptors can then be specified or supplemented by descriptors specific to the infrastructure on which the system is deployed (e.g., location of traffic lights, precise geometrical configuration of a given intersection).

Note 2: The method of describing road infrastructure (i.e. the lists of relevant descriptors) is not developed in this initial version of the technical guide and will be developed in a later supplement.

"Digital infrastructure": all the communication and connectivity equipment required for the ARTS, i.e. roadside units, 3G/4G/5G communication networks, C-ITS, connecting the various smart components of the system or ecosystem and the equipment dedicated to supervision.

"Safety measures": a set of actions either reducing the frequency of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk; *(EU Regulation 402/2013)*.

"Automated driving mode": mode in which the automated driving system is responsible for the dynamic control of the vehicle.

"Risk level": the result of a risk evaluation that quantifies the likelihood of occurrence and severity of the impact.

"Passenger": category of user inside a vehicle in the system who cannot be involved in any dynamic control of the vehicle.

"Risk": the combination of the frequency of damage and its severity.

"Residual risk": risk remaining after prevention or protection measures have been taken.

"Safety Of The Intended Functionality" (SOTIF): the absence of unreasonable risk due to hazards resulting from functional deficiencies of the intended functionality, or by reasonably foreseeable misuse by persons.

"System": a group of interconnected elements (hardware, software or human) considered to form a whole in a defined context and organized in such a way as to achieve a given objective, under certain conditions.

"Subsystem": part of a system, which is itself a system *(EN 50126-1:2017)*.

"Hazardous situation": a situation in which persons are (or could have been) exposed to one or more hazards.

“User” (of the system): general term referring to the role of the human in relation to autonomous driving.

“Road user”: anyone who uses the road (including sidewalks and other adjacent spaces) *(EN ISO TR 4804: 2020)*.
Note: System users are a category of road users. In contrast, other road users are third parties.

3 Abbreviations

FMECA: Failure Mode Effects and Criticality Analysis
AOM: Public transport authority (*Autorité Organisatrice de la Mobilité*)
PHA: Preliminary Hazard Analysis
PRA: Preliminary Risk Analysis
ASIL: Automotive Safety Integrity Level (*ISO 26262-1: 2018)*
DCST: Technical system design file (*Dossier de Conception du Système Technique*)
DPS: Preliminary safety file (*Dossier Préliminaire de Sécurité*)
DS: Safety file (*Dossier de Sécurité*)
E: Exposure classification
Av: Avoidability classification
HE: Hazardous Event
ERP: Public access building (*Etablissement recevant du public*)
RRF: Risk Reduction Factor
S: Severity class
GAME: Globally at least equivalent (*Globalement au moins équivalent*)
HMI: Human-Machine Interface
MRM: Minimal Risk Maneuver
RRM: Risk Reduction Measure
OGS: Overall safety objective (*Objectif Global de Sécurité*)
OQA: Approved qualified organization (*Organisme qualifié agréé*)
OSS: Specific safety objective (*Objectif Spécifique de Sécurité*)
PCC: Central command center (*Poste de Commande Centralisé*)
HS: Hazardous Situation
SMS: Safety Management System
SIL: Safety Integrity Level (*EN 61508-4: 2011)*
SOTIF: Safety Of The Intended Functionality
ARTS: Automated Road Transport System
TFFR: Tolerable Functional Failure Rate
TFR: Tolerable Fail Rate
TDG: Transport of Dangerous Goods

4 Regulatory context

This guide applies to systems or parts of automated road transport systems covered by Article R. 3152-2 of the French Transport Code created by Article 6 of ARTS Decree No. 2021-873 of June 29, 2021.

The ARTS Decree introduces the obligation for automated road transport systems to comply with the "GAME" principle (Globally at least equivalent principle) with regard to their safety level.
This requirement formalized by Article R. 3152-2 of the Transport Code created by Article 6 of the ARTS Decree:
“Art. R. 3152-2. – I. - For the purposes of Article L. 3151-1, any automated road transport system or any part of an existing transport system shall be designed, commissioned and, where appropriate, modified in

such a way that the overall level of safety with regard to users, operating staff and third parties is at least equivalent to the existing level of safety or to that resulting from the implementation of systems or sub-systems providing comparable services or functions, taking into account the current practices, field experience concerning them, and reasonably foreseeable traffic conditions on the route or traffic area in question."

The same Article R. 3152-2 addresses the case where a comparative analysis cannot be conducted with an existing system:
"When it is established that there is no comparable system for assessing the safety of the system in question or of one of its subsystems, the level of safety may be established on the basis of a specific safety study for the system or subsystem concerned, conducted in accordance with good engineering practice."

In general, this document supplements the STRMTG's GAME Implementation Guide and has the same scope and limits. It is designed to clarify the detailed risk analysis approach (Type 3).
This applies to cases where there is no applicable regulatory or technical standard or reference system for an ARTS and a detailed risk analysis needs to be carried out for the system.
Please note that:

- This approach can also be chosen voluntarily instead of the difference-based approach (Type 2);
- The safety demonstration for a system can be based on a combination of the different approaches described in the GAME Implementation Guide.

Therefore, as with the GAME Implementation Guide:

- For the purposes of this document, the term “system” is used generically. It can therefore refer to a complete automated road transport system, a technical system, a subsystem, a component or equipment.
- The demonstration information explained in this guide only refers to the safety of the vehicle occupants (including the operating personnel when they are passengers of the system) and third parties with regard to system operation.

5 Presentation of the detailed risk analysis

5.1 General

The purpose of this document is to provide guidance for performing a detailed risk analysis (Type 3) for a technical system or ARTS system, in implementation of the GAME principle.

There are several objectives:

- Ensure that the methods implemented are consistent, in particular by specifying milestones in order to encourage dialog between stakeholders;
- Initiate reflection by providing input information for the analyses;
- Limit the risk of oversights;
- Develop a common framework for capitalizing on stakeholder field experience.

This document does not claim to be exhaustive:

- Some demonstration areas will need to be further detailed in future versions of this document or in supplementary documents;
- The information provided will need to be enriched as and when feedback on field experience is received from the actors involved in the various cases of implementation.

It is always up to the entity responsible for the analysis to supplement the various aspects of this guide as necessary in order to carry out an analysis that covers the specificities of the system being analyzed.

Similarly, there is always the possibility of justifying why an aspect of this document is not taken into account due to it being inapplicable because of the specificities of the system being analyzed.

5.2 Scope of the detailed analysis

An ARTS can be made up of various elements:

- Highly and/or fully automated vehicles;
- Technical installations specific to the system, enabling remote intervention or contributing to safety, deployed on the route;
- Technical installations enabling remote intervention or contributing to safety, dedicated to supervision, deployed outside the route;
- Operating and maintenance rules (organizational aspect supported by the SMS in operation);
- A route and its installations.

It also interfaces with various elements that contribute to its operation:

- Shared communication and location equipment outside the system;
- The roadway on which the system’s vehicles can travel;
- Pre-existing generic technical facilities shared with road users;
- External services (law enforcement, emergency services, road services, weather forecasting and information services, traffic information services, etc.);
- Applicable traffic regulations on the route;
- Etc.

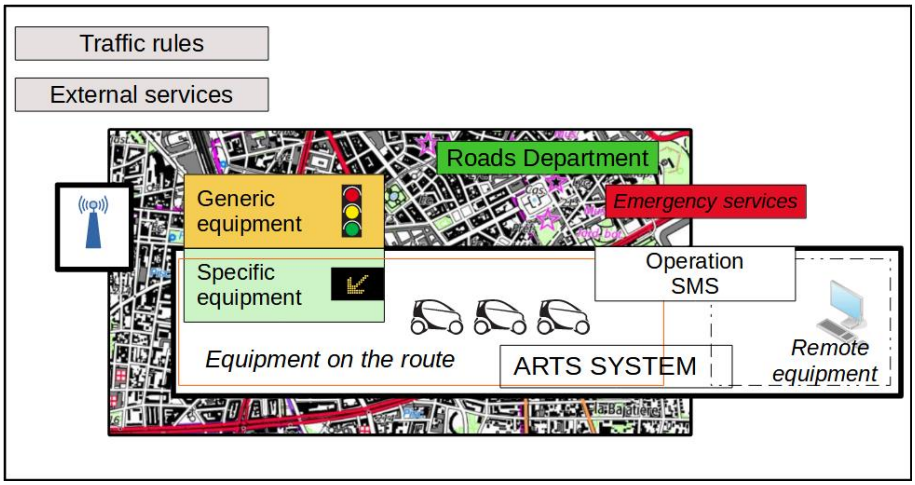

Figure 1 - Organic breakdown of an ARTS

Within these constituent or interfacing elements, the scope of the safety demonstration must include all elements that contribute to the safety of the ARTS.

Among these elements, the following need to be identified:

- Elements that are part of the system and directly integrated into the demonstration. For example, the requirements for a traffic light specific to the system under analysis must be directly identified and resolved as part of the safety demonstration;
- Elements that are not part of the system but that contribute to its safety, for which the safety demonstration may specify exported requirements, which must be verified by the project owner. For example, requirements related to a pre-existing traffic light that is not specific to the system under analysis must be specified as exported requirements and resolved in a second step under the responsibility of the transport authority at the deployment stage.

As specified in the GAME Implementation Guide, the safety demonstration must be conducted for the entire automated road transport system in question, i.e. a technical system deployed on a given route and subject to operating and maintenance rules. Therefore, in the case where only a subsystem or a piece of

equipment is subject to a detailed analysis, the final safety demonstration will ultimately have to cover the entire automated road transport system.

5.3 Framework of the detailed analysis

The process, covering the DCST and DPS / DS phases, consists in analyzing the risks for the entire system, and defining a set of requirements concerning all the elements involved in the system, i.e. the technical system, its architecture, the route and its installations, the operating conditions, the traffic conditions, the operating and maintenance rules, etc.

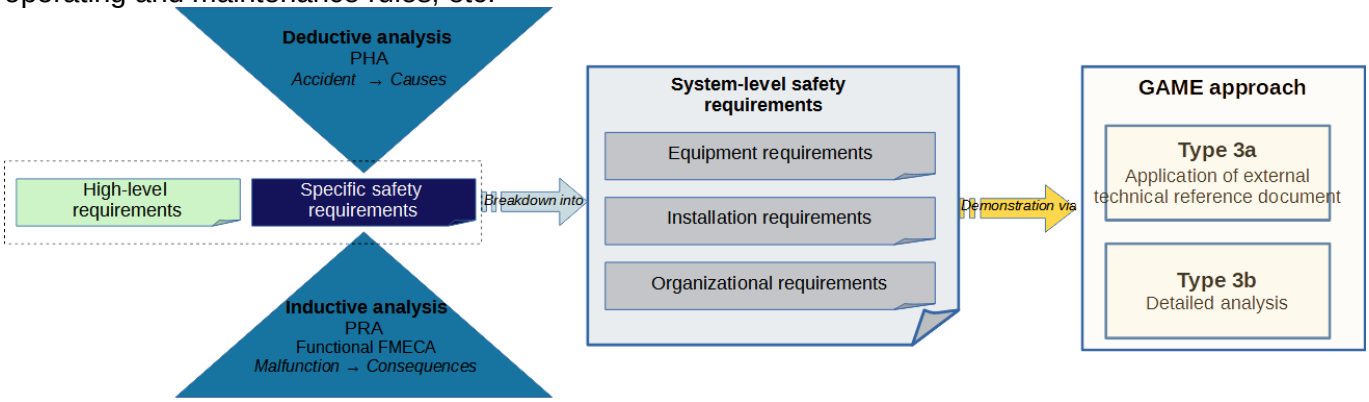

Figure 1 - Type 3 detailed analysis

There are 2 types of requirements:

- <u>High level requirements:</u>

The high-level requirements presented in Section 7 are generic essential requirements applicable outside of any accident or hazardous situation. Unless otherwise justified, they must be met by the system in all circumstances.

- <u>Specific requirements:</u>

The specific requirements are defined for the project by way of 2 additional analyses described in Sections 8 and 9:

- A deductive analysis designed to identify combinations of potential causes of an accident. This analysis starts from the hazards to determine the potential causes (Preliminary Hazard Analysis, PHA);
- An inductive analysis to systematically analyze the impacts of potential system malfunctions. This analysis starts from the functions of the system to analyze all potential impacts in the event that they malfunction (Preliminary Risk Analysis (PRA) or Functional FMECA).

These two cross-analyses are complementary and must be conducted so that they build on each other: any risk identified in one of the analyses must also be analyzed in the other. These analyses are first performed at the DCST stage, and then potentially supplemented at the DPS and DS stages depending on the results of the safety analysis of the route.

The rest of this document provides information to support these various analyses.

The system safety requirements are then successively applied to the subsystems, equipment and components of the system, or exported to the route installations, or to the operating and maintenance rules formalized in the operational safety management system (SMS).

For each identified risk, the requirements for this process may involve the application of a standard outside the ARTS field for which it has been demonstrated that it covers the risk in question and its context (Type 3a demonstration of the GAME Implementation Guide), or the implementation of specific measures after having demonstrated that combining them would reduce the residual risk to an acceptable level (Type 3b demonstration of the GAME Implementation Guide).

For all demonstration work, each activity related to safety must be recorded and documented, (identification of risks, safety measures, results of estimations, etc.). This requirement can be met by keeping a log of hazardous situations.

Analysis of key scenarios

In addition, a specific analysis will be carried out of key scenarios for the operational domain. This guide will be supplemented by requirements applicable to the definition of key scenarios and the specific safety analysis to be applied to them.

5.4 Information for the explicit analysis (Type 3b)

If no technical standard outside the ARTS domain has been deemed acceptable (Type 3a), a detailed analysis must be conducted in order to identify the proper qualitative and/or quantitative measures applicable for each identified risk (Type 3b).

This analysis can be broken down into 2 main phases:

- Definition of an overall safety objective (qualitative and/or quantitative);
- Successive allocation of the safety objective to different levels.

Quantitative safety objectives

An overall safety objective (OGS) is defined when there is sufficient data from field experience, consistent with the system's operational domain. This, for example, can be an overall safety objective defined for traffic accidents involving injuries, by “number of events per km” or “number of events per hour”.

Specific safety objectives (OSS) dividing the overall objective into the different subcategories of accidents are defined if the data is sufficiently precise and meaningful. For example, a specific safety objective defined for injuries from “head-on collisions with another road vehicle” by “number of events per km” or “number of events per hour”.

Further information about these objectives will be added in future versions of this guide in the light of the various work on the subject.

Allocation of safety objectives

In the case of detailed analysis (type 3b), the qualitative or quantitative objectives must be allocated to each function of the system in relation to the safety objectives established from the deductive approach and to the functional FMECA carried out through the inductive approach.

This requires determining the independence of functions and analyzing the combinations of failures that can lead to each system-level accident.

This functional allocation is the prerequisite to allocating safety objectives to each piece of equipment and component of the system.

These various allocation steps are not presently described in this technical guide. Please refer to relevant publications (e.g., EN 50126-2)

Type 3b analysis if a quantitative safety objective is defined

The following table presents the steps for the specific analysis approach (Type 3b) specifically where a quantitative safety objective can be defined.

	Activity	Observations and comments	Reference
1	Establish an Overall safety objective (OGS) for categories of accidents (e.g., collision). As necessary, develop OSSs (Specific safety objectives) for each type of accident in the category (e.g., collision with different third parties, or collision without third parties).	The risk acceptance criterion can be defined in terms of the maximum acceptable rate of occurrence (OGS). For each type of accident, identify the corresponding OSS.	This will be covered in a later version of this guide
2	Identify hazardous situations via a PHA (Preliminary Hazard Analysis).	Identification of hazardous situations (HS) for a given accident scenario. Identification of the HS affected by the OSS.	See Section 8
	Calculate a TFR objective for HS that incorporates the accident-prone context	Consideration of the plausibility of an accident based on the actual context at the time of occurrence of the hazardous situation (accident conditions). The TFR represents the fail rate, i.e. the rate of failures and functional deficiencies.	Not covered in this guide
3	PRA (Preliminary Risk Analysis)	Identification of the causes of HS. The PRA facilitates the identification of ARTS system failures by linking them to HS.	See Section 9
4	Allocate the TFR objectives (related to HS) to the functions of the ARTS system. The TFR is broken down into the functional failures = TFFR. These failures constitute the HE (hazardous events)	This breakdown into TFFR can either be equally spread across the functions of the ARTS system affected by the accident or a breakdown taking into account the complexity and/or the field experience from the functions of the ARTS in question. The purpose of this step is to verify that TFR < Σi TFFR(i).	Not covered in this guide
5	Translate and convert TFFR frequencies into consistent SILs or ASILs.	Based on the TFFR objectives and depending on the relevant standard, associate the SIL and/or ASIL level consistent with the TFFR to each function of the ARTS system.	Not covered in this guide
6	Translate the TFR into objectives for functional deficiencies	-	Not covered in this guide

Table 1 - Steps in the specific analysis process (Type 3b) - quantitative case

6 Risk estimation principles

6.1 General

The analysis concerns all events that can lead to system-level accidents.
The scope to be taken into account in the analysis covers all events that may take place during system operation, and that may have impacts on the safety of vehicle occupants and third parties.
It is therefore not limited to traffic accidents but includes, for example, events, failures and functional deficiencies related to fire or passenger transfers (see Table 8 of this document).

The definition of an accident covers events resulting in damage or injuries that may compromise the safety of people.
An event that does not compromise safety is not considered an accident for the purposes of this guide.

An accident can be seen as the combination of a pre-accident hazardous situation and one or more accident conditions, without which the accident cannot take place.
For example, a collision at an intersection may be caused by the hazardous situation involving “failure to obey a traffic control device”, which is not enough on its own. The collision will occur if a third party vehicle crosses the intersection at that time.

The hazardous situation itself may be the consequence of a hazardous event, itself caused by different events or combinations of events.
Using the same example, the hazardous situation involving “failure to observe a traffic control device” may be caused by a system failure or poor perception due to an obscured view/sign.

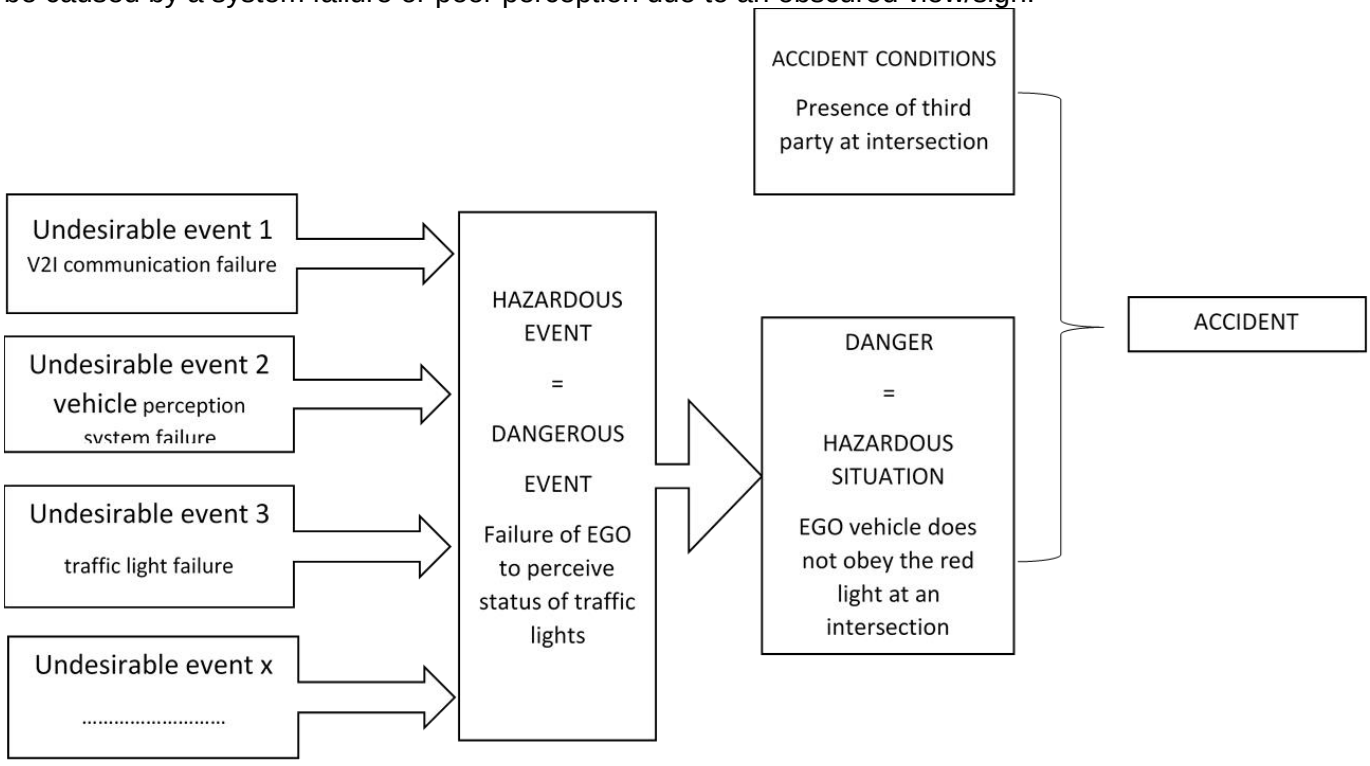

Figure 3 - Accident sequence

Risk is the combination of the frequency of damage and severity. Accident severity and frequency metrics are detailed later in this section.

A risk posed by an event is estimated by taking into account the frequency of the event, the likelihood of its conditions materializing into a real accident, and the severity resulting from the potential consequences of the accident.
In general, the risk estimation should be conducted using a conservative approach that analyzes the reasonably foreseeable worst-case scenario. When the same event can give rise to different scenarios, the scenario with the highest level of risk should be used.

The number of vehicles in the system is not taken into account in the risk estimation. The risk is estimated for a vehicle of the system by considering that a user is in a single vehicle at a given time, and by considering the situations that the vehicle could encounter on its route.

The number of instances of each physical infrastructure configuration in the system is not considered in the risk estimation. For example, the risk is estimated for each intersection on the route by considering that a user is present at only one point on the route at a given time.

The ARTS detailed risk analysis phase therefore requires the ability to scale the severity and frequency.

6.2 Severity estimation

Severity is the level of damage resulting from an accident.

Severity must be estimated by considering the case where the accident occurs, taking into account the reasonably foreseeable worst-case scenario and the conditions established for the scenario (for example for a collision: type of third parties involved, nature of the impact, type of vehicle, speeds, presence of installations or protective devices, etc.)

The severity estimation must be recorded and documented.

The severity metric is derived from the severity classification used in ISO 26262:2018.
Severity level S0 corresponds to damage only (no injuries) and is given in the table for the sake of completeness. Because the GAME demonstration only concerns the safety of people, a reasonably foreseeable worst-case scenario resulting only in damage will not be analyzed.

Severity classification	Description
S0	No injuries
S1	Light to moderate injuries
S2	Severe to life-threatening injuries (survival probable)
S3	Life-threatening to fatal injuries (survival uncertain) (*)

Table 2 - Severity Classifications

(*) Classification S3 with a large number of equivalent fatalities in particular cases
Within level G3, a marker (*) is provided to mark events associated with configurations that could give rise to an accident scenario in the case of road-rail interaction zones or a domino effect accident scenario in some specific cases, whose potential consequences would be catastrophic because of the number of people potentially involved: large number of passengers with widespread risk of fatal injuries or accident impacts potentially involving a large number of road users, which would lead to a large number of equivalent fatalities (likely more than 10. Reference should be made in particular to Annex C of EN 50126-1).

The severity classification and the safety objective associated with the scenarios marked (*) are those of level S3, but each of these events associated with these traffic configurations, require a specific analysis, which may lead to additional safety measures beyond the vehicle.

These additional safety measures may concern:

- Operating conditions specific to the situation;
- Road equipment and installations specific to the situation;
- Organizational measures specific to the situation.

The following table lists the configurations that require this type of additional specific analysis. This list is not exhaustive and it is up to the project owner to identify the risk situations concerned by the marker (*).

Table 3- List of situations concerned by the marker (*)

ACCIDENT	ID[1]	Subtype	Conditions	Vehicle category / class [3]				Reason for the marking (*)
				cat M1 (8p max)	cat M2/M3 classes A/B 9-22p	cat M2/M3 classes 1/2/3 >22p	NAVURB (French urban shuttle) 9-16p	
Collision	1.2	Collision with a solid obstacle (containers, animals, falling trees, etc.)	if traveling in a tunnel [2] > 300 m long (200m if TDG) with ego vehicle speed > 30 km/h	N/A	N/A	YES	N/A	collision causing a vehicle fire in the tunnel (extended damage only for heat potential classes 1/2/3)
			if there is a risk of falling from a height (traveling on a structure, over a ravine, etc.) with ego vehicle speed > 30 km/h	N/A	N/A	YES	N/A	collision, run-off and rollover with numerous victims following a fall from height
	1.3	Collision with another road vehicle	if traveling in a tunnel [2] > 300 m long (200m if TDG) with possible speed differential between ego vehicle and third party > 30 km/h on impact	N/A	N/A	YES	N/A	collision with another vehicle causing a vehicle fire in the tunnel (impacts on the traveling vehicle itself and if collision with a truck, extensive consequences following a truck fire)
			if traveling with a risk of falling from a height (traveling on a structure, over a ravine, etc.) with possible speed differential between ego vehicle and third party > 30 km/h on impact	N/A	N/A	YES	N/A	collision with a third party with numerous victims in the ego vehicle following a fall from height
	1.4	Collision with a guided transport system vehicle at a double track intersection (e.g., tramway line and tramway crossing)	if ego vehicle speed > 15 km/h on impact	YES	YES	YES	YES	collision with numerous victims in the ego vehicle and in the tram following the derailment of the tramway causing collision with the crossing tramway
		Collision with a rail transport system vehicle (heavy rail) at a level crossing		N/A	N/A	YES	N/A	collision with railway system with many victims in the ego vehicle
Fire, smoke, explosion	5.1	Fire/smoke in the vehicle	Fire originating from a vehicle: if traveling in a tunnel [2] > 300 m long (200 m if TDG)	N/A	N/A	YES	N/A	1 - fire originating in the vehicle (prevention measures): risks for tunnel users only if the heat capacity of the vehicle is high (classes 1/2/3 or unstable on-board energy in the vehicle) 2 - fire initiated by a truck with the ego-vehicle in second position (evacuation of the ego-vehicle): risks for tunnel users only if the heat capacity of the vehicle is high (classes 1/2/3)

[1] The situation identification ID field refers to the number in Table 8.

(2) For the purposes of this table, all covered roadways are considered tunnels, regardless of their construction method: excavated or immersed structures, covered trenches, non-airtight covers, partial covers with an opening to the outside of less than 1 m^2 per traffic lane and per linear meter
"Tunnel length" = the distance between the two tunnel openings or between a tunnel opening and the retaining wall of an adjacent underground station or between the retaining wall of two consecutive underground stations (Art 1, Ministerial Order of 22/11/2005).
(3) Vehicle categories are given in reference to Article R. 3111-1 of the French Highway Code.

6.3 Estimation of accident frequency

As part of the detailed risk analysis described here, the aim of the estimation is to assess the probability of each accident, seen as the combination of a pre-accident hazardous situation and one or several accident conditions forming the scenario.

A conservative approach should be adopted in estimating the frequency of each accident, by choosing the reasonably foreseeable worst-case scenario.

The accident frequency (F) incorporates the probability of the hazardous situation and the probability of the accident conditions (RRF), as shown in the figure below.

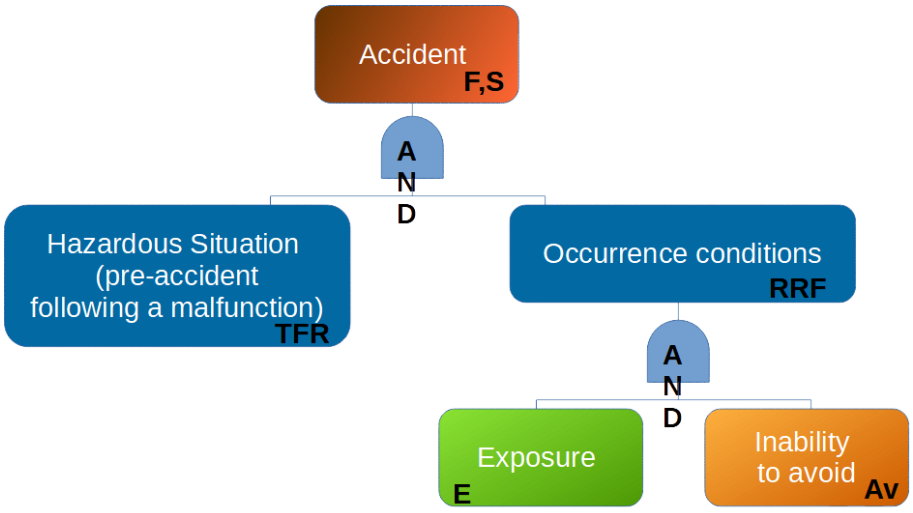

Figure 4 - Risk estimation factors

The probability of the traffic conditions occurring is represented by the risk reduction factor (RRF). This is the combination of the exposure (E) to the context necessary for the accident to occur (operational driving situation), and the inability of the persons involved to avoid the accident (Av).

The risk reduction factor (RRF) is the product of exposure (E) and avoidability (Av).

The frequency of an accident thus makes it possible to scale the estimation of risk with regard to the random events required for the accident to occur:

- The estimation of risk associated with an accident scenario involving the random failure of a piece of equipment can therefore include the equipment’s likelihood of failure (TFR).
  For example, reducing the hourly probability of failure of a critical circuit board embedded in a smart traffic signal reduces the risk associated with crash scenarios involving signal failure;
- Estimating the risk associated with an accident scenario involving a specific behavior of a third party could therefore include a parameter conveying the “common” or “exceptional” nature of the behavior in view of the data from observations (E).
  For example, the likelihood of the driver of a passing third party vehicle losing control of the vehicle can be estimated to be lower than the likelihood of a speed violation.

The levels of the various factors involved in the frequency of occurrence should be estimated on the basis of data from road vehicle traffic under comparable conditions, or data from comparable situations, with preference for the most conservative estimate.

The estimates used in estimating the frequency of occurrence must be recorded and documented.

Consideration of exposure to the operational situation (E)

The exposure metric is derived from the classification used in ISO 26262:2018.

Exposure classification (E)	Description	Quantification in the RRF (1)
E1	Very low probability or Less than once a year for most vehicles	0.001
E2	Low probability <1% of operating time or A few times a year for most vehicles	0.01
E3	Medium probability Between 1 and 10 % of operating time or Once a month or more for most vehicles	0.1
E4	High probability > 10% of operating time or On average almost every trip	1

Table 4 - Exposure Classifications

(1) The RRF quantification values given here are standard values linked to exposure classification thresholds. More precise quantification values can be used if significant data is available from field experience (e.g., an instance of E4 exposure could be quantified at 0.33 to calculate the RRF, based on the analysis of data from field experience)

The exposure (E) reflects the probability that the operational situation required for the accident to occur exists when the hazardous situation occurs. It makes it possible to assess the concurrence between a hazardous situation and an operational situation, the combination of which can cause an accident.

Depending on the context of the situation under analysis, exposure (E) can be estimated in terms of the length of exposure to the operational situation (proportion of time the system vehicle is exposed to the situation) or in terms of the frequency of exposure to the situation (number of times the system vehicle is exposed to the situation). The most appropriate approach to the situation under analysis should be used.

The notion of exposure applies only in cases where the concurrence of several independent events makes sense (i.e. the concurrence between the moment when the hazardous situation occurs and exposure to the operational situation).
Therefore, in cases where the hazardous situation is not limited in time, the exposure classification chosen must be E4 (exposure value = 1). In this case, it must be considered that at some point the hazardous situation and the operational situation will occur simultaneously.
This can be the case for the following hazardous situations:

- Functional deficiencies;
- Cases where the exposure to the operational situation actually generates the hazardous situation (for example, the exposure must be 1 when analyzing a "fog collision" accident in the case of a vehicle that is not suitable for operation in fog because in this case the "fog" condition is both the hazardous situation and the operational situation required for the accident to occur), etc.

Situational exposure values are key elements of risk estimation and the values selected must cover the actual traffic conditions encountered on the route, whether it is the generic route at the DCST stage or the actual route at the DPS/DS stage.

The exposure values must therefore be recorded and documented in order to verify that the exposure values selected at the technical system stage (DCST phase) are sufficient at the route safety analysis stage (DPS/DS phases).

Consideration of avoidability (Av)

Avoidability (Av) is the capacity of the people involved in a scenario to avoid an accident, due to their timely reaction to the situation, i.e. suitable and timely action.
The people involved in an ARTS accident scenario may include the remote operator, potential drivers of third party vehicles, persons in the vicinity of the vehicle, and in some cases, the occupants.
Ways of avoiding the accident may include avoidance or stopping.

Avoidability should be estimated conservatively by conveying the realistic ability of those involved to avoid the accident, particularly in view of their abilities and circumstances.

The criteria for estimating avoidability depend on the scenario under analysis and reflect the ability of those involved to implement a response. For example, the following should be taken into account:

- The speed of occurrence of the event;
- The visibility of the event (lines of sight and distances, obscured view, signs/signals, etc.);
- The predictability of the event (standard or unlikely event, whether it is foreseeable);
- The possibility of avoidance (is there a realistic way to avoid the scenario) ;
- The characteristics of the people involved (professional or not, trained or not, physical abilities, age, level of alertness, level of availability, etc.).

For each scenario, the avoidability classification must be consistent with the actual traffic conditions encountered on the route, whether it is the generic route at the DCST stage or the actual route at the DPS/DS stage.

The avoidability metric is derived from the classification used in ISO 26262:2018.

Avoidability classification (Av)	Description	Quantification in the RRF
Av0	Avoidable in general	0
Av1	Simply avoidable Avoidable more than 99 times out of 100 on average	0.01
Av2	Normally avoidable Avoidable more than 90 to 99 times out of 100 on average	0.1
Av3	Difficult to avoid Avoidable less than 90 times out of 100 on average	1

Table 5 - Avoidability Classifications

While the concept of avoidability is derived from the concept of controllability defined by ISO 26262:2018, it is important to highlight the main difference. This relates to the fact that there is no driver in an ARTS

vehicle, or even in third-party vehicles in the case of interactions between vehicles in a fleet of automated vehicles for instance.
Since the vehicle driver is the essential vector of controllability, their removal from the scenario will have a significant impact on the ability of those involved to avoid an accident.

7 High level requirements

High-level requirements are essential generic requirements that must be met by the ARTS as a whole.
These requirements apply outside the context of any accident or hazardous situation, and are complementary to the specific safety requirements derived from the deductive and inductive analyses covered in Sections 8 and 9.

- These requirements must be taken into account when specifying the expected behavior of the system, during deductive and inductive analyses,
- and be broken down into a list of detailed requirements, adapted to the system and its context (route, operating conditions, traffic conditions, etc.). Compliance with each of these requirements must be demonstrated based on evidence from specific analyses and the various demonstration activities (safety analyses, scenario approach).

The high-level requirements presented here are intended to be generic and independent of the technologies implemented in the system, or the ARTS routes. At every stage of the project, they are broken down into specific requirements which may be technical or organizational in nature and may give rise to constraints on the route or operating conditions.

The table below lists the high-level requirements for an automated road transport system. Compliance with these requirements does not preclude compliance with any other requirements applicable to the system or its equipment, such as those under EU Regulation 2019/2144 on type-approval requirements for motor vehicles.

The following rules of use should be taken into account:
- The list is not exhaustive and can be added to in the course of a specific project.
- Conversely, although the listed requirements are intended to be generic, some of them may not be applicable to a specific project, in which case a substantiated record of their exclusion should be kept.
- The high-level requirements listed here are system-level requirements. However, some of them may already be met by the certification requirements for the vehicle used in the system. The choice was made to cover a broader scope than may be strictly necessary.
- In general, it has been verified that these high-level requirements do not contradict regulations applicable to vehicles without autonomous driving systems.
- High-level requirement 11 concerning “compliance with applicable traffic regulations” is broken down into sub-requirements which are only intended to illustrate the content of the requirement with more concrete information. Each of these sub-requirements refers to a set of articles under the French Highway Code. It is important to note that the list of these sub-requirements, given for illustration purposes, is not exhaustive. It is also important to note that the list of Highway Code articles specified as a source is not exhaustive. Compliance with the Highway Code which defines the applicable traffic regulations is an essential requirement and must be followed by vehicles across the entire system. The project owner is responsible for complying with this requirement.

<u>Guide for reading the table below</u>
- The requirements are classified by major topic and area;
- The title is intended to be general and is broken down into one or more requirements depending on the case;
- The source is provided for information purposes to put the requirement in context. The sources may come from regulations in draft form pending publication as legislation;

- The title “EU ADS Regulation” refers to Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles;
- Details are provided in the last column to guide readers.

Table 6.1 - List of High-Level Requirements - General Requirements

Area	No.	Title	No.	Sub-requirements	Source	Details
	GENERAL REQUIREMENTS					
Conditions of use	1	The system shall not allow vehicles to operate in automated driving mode if the system is outside its operational domain	1.1	The system shall recognize if the vehicle leaves its operational domain	Transport Code Art. R. 3152-2 II	There are 2 cases: 1 - the vehicle leaves the ODD or there is a failure resulting in inability to drive safely --> mandatory stop via an MRM. 2 - deterioration of traffic conditions or failure that does not result in an inability to drive but the need to switch to fall-back mode (reduced speed). This fall-back mode has been assessed, and is therefore not an exit from the ODD. The driving tasks are still carried out safely under fall-back conditions. Stopping via an MRM is not mandatory. The requirement applies to case 1 only. The operational domain is formalized by various traffic conditions such as location, weather conditions, light conditions, road conditions, the number of passengers and their transport conditions, etc. The system is considered to leave its operational domain "for" (because of) a particular vehicle. In this case, automated driving mode shall only be deactivated for this vehicle. Automated driving mode is deactivated in a sequence that starts with an MRM. See EU ADS Regulation Annex II Article 3.1.5. "When the ADS reaches the ODD boundaries, it shall perform a MRM to reach a MRC and shall warn the on board operator (if applicable)/remote operator accordingly (if applicable)"
			1.2	the system shall only allow activation of the automated driving mode when it is within its operational domain	French Transport Code Art. R. 3152-2 II	
			1.3	When the system leaves its operational domain, vehicles affected by the loss of safe operating conditions shall deactivate the automated driving mode after performing an MRM.		
			1.4	The system shall inform the operator of any exit from its operational domain, in all operating modes	French Transport Code Art. R. 3152-2 II	

Area	No.	Title	No.	Sub-requirements	Source	Details
	GENERAL REQUIREMENTS					
Conditions of use	2	The technical system shall not allow vehicles to operate in automated driving mode if the system is outside its system technical design domain	2.1	The technical system shall recognize if the vehicle leaves its system technical design domain	French Transport Code Art. R. 3152-2 III	Exit from the system technical design domain shall be detected primarily by technical measures. If it is demonstrated that this requirement is technically impossible, the requirement of Art R. 3152-2 III shall be covered by the requirement of Art R. 3152-2 II regarding detection of an exit from the operational domain.
			2.2	The technical system shall inform the operator of any exit from its system technical design domain, in all operating modes	French Transport Code Art. R. 3152-2 III	
	3	The system shall be able to anticipate foreseeable exits from the conditions of use	3.1	The technical system shall be able to anticipate foreseeable exits from its system technical design domain		Any exit from the operational domain shall be anticipated and properly managed when it is foreseeable. See EU ADS Regulation Annex II Article 3.1.3. "The ADS shall be able to anticipate exits from the ODD."
			3.2	The system shall be able to anticipate foreseeable exits from its operational domain		
System integrity	4	The system shall ensure that any vehicle in automated driving mode complies with applicable traffic regulations, everywhere at all times.	4.1	The system shall detect failures that potentially impact safety.	French Transport Code Art. R. 3152-2 II and III	
			4.2	The system shall inform the operator of any failures that potentially impact safety.		
			4.3	The system shall not allow vehicles to operate in automated driving mode in the event of a failure affecting safety for these vehicles.		The failure may involve equipment of the technical system located outside the vehicle.
			4.4	The system shall not allow vehicles to operate in automated driving mode in the event of an alteration to the technical system equipment affecting safety for these vehicles.		For example, in the event of a collision with a sensor of the technical system which would change its configuration

Area	No.	Title	No.	Sub-requirements	Source	Details
	GENERAL REQUIREMENTS					
System responses	5	The system shall be designed to avoid accidents that may result from reasonably foreseeable situations within its operational domain.			French Transport Code Art. R. 3152-2 II	Compliance with this requirement is demonstrated by the safety analyses identifying the reasonably foreseeable risks in the operational domain and the definition of measures to make them acceptable.
	6	The technical system shall be designed to avoid accidents that may result from reasonably foreseeable situations within its system technical design domain.			French Transport Code Art. R. 3152-2 III	
	7	System responses (actions including minimal risk maneuvers, emergency maneuvers, maneuvers eligible for remote intervention, etc.) shall not generate unacceptable additional risks.			French Transport Code Art. R. 3152-2 III	The system takes appropriate action for each situation to minimize the overall risk
	8	When the system detects that the conditions for its safe operation are no longer met due to an equipment failure or exit from its operational domain, the system shall ensure that the vehicles concerned perform an MRM.				There are 2 cases: 1 - the vehicle leaves the ODD or there is a failure resulting in inability to drive safely --> mandatory stop via an MRM. 2 - deterioration of traffic conditions or failure that does not result in an inability to drive but the need to switch to fall-back mode (reduced speed). This fall-back mode has been assessed, and is therefore not an exit from the ODD. Driving tasks are still carried out safely under fall-back conditions. Stopping via an MRM is not mandatory. The requirement applies to case 1 only.

Area	No.	Title	No.	Sub-requirements	Source	Details
	GENERAL REQUIREMENTS					
System responses	9	A vehicle can only deactivate automated driving mode when it is stopped.			EU ADS regulation Annex II Article 4.1.2.2	Ability of the system to command the vehicle to stop and exit automated driving mode, even in the event of a failure. Note: this only concerns failures because functional deficiencies impacting the safety of the system are considered as exits from the ODD requiring MRMs. EU ADS Annex II Article 4.1.2.2 "The ADS shall execute a MRM to achieve a MRC in the event of a failure of the ADS and/or other vehicle system that prevents the ADS from performing the DDT."
	10	The vehicle shall retain the ability to stop even in the event of a major failure.			EU ADS regulation Annex I Article 17.6.5 + Annex II Article 4	
Compliance with applicable traffic regulations	11	The system shall ensure that any vehicle in automated driving mode complies with applicable traffic regulations, everywhere at all times.	11.1	Monitor the situation of the vehicle: respect maximum authorized mass, maximum dimensions, etc.	French Highway Code R312-2, R312-10, R312-20, R313-21, etc.	Each sub-requirement refers to a set of articles under the French Highway Code. It is important to note that the list of these requirements, given for illustration purposes, is not exhaustive. It is also important to note that the list of Highway Code articles is not exhaustive. Compliance with the Highway Code which defines the applicable traffic regulations is an essential requirement and must be followed at all times. The project owner is responsible for complying with this requirement. Compliance with the traffic regulations of the country of operation is one of the requirements for vehicle approval, potentially
			11.2	Regularly check the condition of the vehicle: lighting, tires, brakes, etc.	French Highway Code R313-1 to R313-19, R314-1, R315-1, etc.	
			11.3	Switch on vehicle lighting: e.g., high beams, low beams, etc.	French Highway Code R416-4 R416-5 R416-6 R416-7 R416-8 R416-9	

Area	No.	Title	No.	Sub-requirements	Source	Details
			GENERAL REQUIREMENTS			
Compliance with applicable traffic regulations			11.4	Signal to third parties: e.g., when braking in an emergency, when driving at reduced speed, when stopping in a hazardous area, when changing direction, etc.	French Highway Code R313-17-1 R416-18 R416-19 R412-10, etc.	via exported requirements (see EU ADS Regulation Annex II Article 1.3. "The ADS system shall comply with traffic rules of the country of operation"). The List of Final Requirements for the ARTS is intended to apply to the overall system, regardless of which part of the process it covers. For example: some will be covered via ADS APPROVAL (those for which the automated vehicle is self-sufficient). All those for which the automated vehicle is not self-sufficient, must be evaluated on the TECHNICAL SYSTEM and ARTS layers. The evaluator is therefore either the APPROVAL BODY or the ARTS APPROVED QUALIFIED ORGANIZATION (OQA). Any changes to the Highway Code shall be taken into account.
			11.5	Adopt appropriate behavior: comply with safety distances, adapt behavior when third parties are using hazard lights or flashing lights, adapt speed to circumstances and the environment without hindering the normal movement of other vehicles, etc.	French Highway Code R412-12, R412-11-1, R413-17 R413-18 R413-19, etc.	
			11.6	Obey roadside traffic checks: follow orders, provide vehicle documents, etc.	French Highway Code L233-1 R233-1 R233-2 R233-3	
			11.7	Drive only in authorized lanes: follow lane markings, do not drive in restricted lanes, follow directional traffic signs, etc.	French Highway Code R412-7 R412-8 R412-19 R412-22 R412-23 R412-24 R412-26 R411-17 R412-28 R412-26, etc.	
			11.8	Adopt an appropriate lateral position in the traffic lane: in normal driving and at intersections	French Highway Code R412-9 R414-1, etc.	
			11.9	Observe priorities/right-of-way: intersections with right-of-way for traffic entering from the right, with STOP sign, with yield, entry into traffic from parking spots, entry into roundabouts, etc.	French Highway Code R415-5, R415-6 R415-7 R415-9 R415-10 etc.	

Area	No.	Title	No.	Sub-requirements	Source	Details
	GENERAL REQUIREMENTS					
			11.10	Obey traffic lights	French Highway Code R412-30 R412-31	
Compliance with applicable traffic regulations			11.11	Follow rules for crossing railroad tracks	French Highway Code R422-3	
			11.12	Obey the right of way for pedestrians	French Highway Code R415-11	
			11.13	Observe the right of way in special cases: meeting priority vehicles, meeting oncoming traffic if lanes are not wide enough, emergency vehicles in all circumstances, public transport vehicle leaving its stop, processions, etc.	French Highway Code R414-2 R414-3 R415-12 R412-11 R412-15 etc.	
			11.14	Obey speed limits	French Highway Code R413-1 R413-2 R413-5 R413-10 etc.	
			11.15	Obey rules of conduct for specific configurations: intersections, RH turn, LH turn, highway entry/exit lanes, etc.	French Highway Code R415-1 R415-2 R415-3 R415-4 R421-3 R421-4, etc.	
			11.16	Obey rules when overtaking	French Highway Code R414-4 R414-5 R414-6 R414-7 R414-8 R414-10 R414-12 R414-16 etc.	

Area	No.	Title	No.	Sub-requirements	Source	Details
		GENERAL REQUIREMENTS				
			11.17	Stop the vehicle only in suitable locations: on the shoulder or in the right-hand lane, outside of crosswalks, outside of dangerous or inconvenient areas, outside motorways, etc.	French Highway Code R417-1 R417-4 R417-5 R417-9- R417-10 R417-11 R421-7	
			11.18	Stop and alert in the event of a traffic accident involving the vehicle	French Highway Code R231-1	
Compliance with applicable traffic regulations			11.19	Comply with any other applicable rules and regulations	French Highway Code	
Compliance with applicable planning and traffic control device regulations	12	Roadside equipment and installations derived from requirements exported by the system (either specific to the system or specified for the system but of shared use with other users) must comply with locally applicable rules.				E.g.: the geometry of an intersection modified for the deployment of an ARTS must comply with regulations so as not to induce risks for other users; a traffic light for other users added specifically for the ARTS must be installed in such a way that it can be seen by these users.
Access safety	13	The parts of the ARTS system for which access by third parties may present a safety risk shall only be accessible to authorized persons.			FRAV-23-05 Rev2 GRVA Section *4.4.2.*	FRAV-23-05 Rev2 GRVA 4.4.2. "The ADS shall be designed to protect against unauthorized access." FRAV-23-05 Rev2 GRVA Table 1-17 "The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices."

Table 6.2 - List of High-Level Requirements - Requirements for vehicle maneuvers

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR VEHICLE MANEUVERS					
Vehicle behavior	14	The vehicles of the system shall behave in a way that is understandable to other road users			Also see 11.4 and 11.8 of the French Highway Code	- signaling: see French Highway Code (lights, sounds, etc.) - quality of trajectories: anticipated, smooth - smoothness of longitudinal control - positioning in the lane
	15	The vehicles of the system shall behave in a safe manner that maintains appropriate safety distances	-		EU ADS regulation Annex II Article 1.1.2. Also see requirement 11.5 of the French Highway Code	EU ADS regulation Annex II Article 1.1.2. "As part of the DDT, the ADS shall be able to: ... (b) maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle; ;..."
	16	The vehicles of the system shall operate at an appropriate and uniform speed with respect to other users, and their driving environment.			EU ADS regulation Annex II Article 1.1.2. Also see requirement 11.5 of the French Highway Code	EU ADS regulation Annex II Article 1.1.2. "As part of the DDT, the ADS shall be able to: (a) operate at safe speeds and respect speed limitations applicable to the vehicle; ..."
	17	The vehicles of the system must adapt their behavior to the environment, giving priority to the safety of people			EU ADS regulation Annex II Article 1.1.2.	EU ADS regulation Annex II Article 1.1.2. "As part of the DDT, the ADS shall be able to: c) adapt its behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic) in an appropriate safety oriented way; (d) adapt its behaviour in line with safety risks and give the highest priority to the protection of human life;"

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR VEHICLE MANEUVERS					
Management of traffic accidents	18	In the event of a traffic accident involving a vehicle, - the vehicle shall detect the impact dynamically or statically (whether or not it is stopped) - appropriate actions shall be implemented: - the vehicle should brake (e.g., MRM), or remain stopped; - once the vehicle is stopped, automated driving mode shall be deactivated. - the command center shall be alerted - automated driving mode cannot be reactivated until the necessary checks have been carried out - provide access to data (Order 2021-442 of 14 April 2021)			EU ADS regulation Annex II Article 2.1.5.	In the event of a collision at a standstill EU ADS Regulation Annex II Article 2.1.5 "In the event of a traffic accident involving the fully automated vehicle, the ADS shall aim to stop the fully automated vehicle and aim to perform a Minimal risk Manoeuvre to reach the Minimal risk Condition. ADS resuming normal operation shall not be possible until the safe operational state of the fully automated vehicles has been confirmed by self-checks of the ADS or/and the on- board operator (if applicable) or the remote intervention operator (if applicable)."
MRM	19	Any MRM initiated by a vehicle must be signaled to the vehicle's passengers, other road users and the operator.			EU ADS Regulation Annex II Article 5.2	EU ADS Regulation Annex II 5.2 "The ADS shall signal its intention to place the fully automated vehicle in an MRC to occupants of the fully automated vehicle as well as to other road users in accordance with traffic rules (e.g., by activating the hazard warning lights)"
	20	After a minimal risk maneuver, the vehicle shall only resume operation in automated driving mode after checks have been performed to confirm that the conditions that caused the minimal risk maneuver are no longer present.			EU ADS Regulation Annex II Article 5.3	EU ADS Regulation Annex II Article 5.3: "The fully automated vehicle shall only leave the MRC after confirmation by self-checks of the ADS or/and by the on-board operator (if applicable) or remote intervention operator (if applicable) that the cause(s) of the MRM is no longer present."

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR VEHICLE MANEUVERS					
Emergency stop	21	Any emergency maneuvers initiated by a vehicle must signaled to the vehicle's passengers, other road users and the operator.			-	A procedure is required to return to automated driving mode. Specific signaling/ other users Information from the operator
	22	Following an emergency maneuver that results in the vehicle coming to a stop, the vehicle shall signal to other road users and to the command center			-	

Table 6.3 - List of High-Level Requirements - Requirements for Passengers

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR PASSENGERS					
Evacuation	23	The system shall ensure that passengers are able to evacuate the vehicle in the best possible conditions in all foreseeable situations for the route.				Note: when areas of the route/area impair the ability to safely evacuate, an evacuation strategy must be defined and formalized via the SMS The following aspects in particular shall be taken into account: - the occurrence of another danger preventing evacuation (e.g., fire, collision which blocks the openings, etc.) - difficult evacuation due to insufficient size or number of emergency exits or openings - poor information on how to open doors and/or emergency exits - evacuation of persons with reduced mobility, even if alone - panic in the system vehicle making evacuation difficult - evacuation impossible due to posts or obstacles - failure of the communication system with the command center - vehicle location information fails to be properly relayed to the command center following a collision Note that under this requirement, evacuation must be possible via other openings besides the doors (window and hammer available). See regulations on this subject (in particular the French Decree of 2 July 1982 on the public transport of persons, for the transport of

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR PASSENGERS					
Evacuation						passengers in a vehicle with more than nine seats, including the driver). Evacuation conditions shall be adapted depending on whether the vehicle has retained its ability to move.
	24	Each vehicle in the system must allow for passengers to be evacuated by emergency services or operating personnel from outside the vehicle				Enable openings to be opened from the outside by emergency services or operating personnel Manage protection against malicious acts
Passenger stop request	25	Each vehicle in the system must allow for passengers to request that the vehicle be stopped in an emergency.			EU ADS Regulation Annex II Article 6.3	The following aspects in particular shall be taken into account: - access to the emergency stop device - information on the emergency stop device - processing of the stop request - management of the stop phase EU ADS Regulation Annex II 6.3 " "The ADS shall provide vehicle occupants with means to request a minimal risk manoeuvre to stop the fully automated vehicle. In case of emergency: a) for vehicles equipped with automatically operated doors, the unlocking of the doors shall be conducted automatically when it safe to do so, b) a mean shall be given to passengers to exit a vehicle at standstill (opening the doors or via an emergency exit).

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR PASSENGERS					
Passenger communication	26	Each vehicle in the system shall allow for passengers to communicate with the command center			EU ADS Regulation Annex II Article 6.2	The following requirements shall be taken into account: possibility of passenger alert in case of a critical situation (passenger distress, fire on board, etc.) This may be supplemented by a sign and phone number to call in case of emergency, in the event of communication system failure EU ADS Annex II Article 6.2 "If a remote intervention operator is part of the ADS safety concept, the fully automated vehicle shall provide means for vehicle occupants to call a remote intervention operator through an audiovisual interface in the fully automated vehicle. Unambiguous signs shall be used for the audiovisual interface (e.g., ISO 7010 E004)."

Table 6.4 - List of High-Level Requirements - Requirements for remote operator/command center

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR REMOTE OPERATOR/COMMAND CENTER					
Operator controls	27	The system shall give the remote intervention operator personnel the ability to order a vehicle MRM according to suitable predefined procedures.				The procedures for bringing the vehicle to a standstill shall be defined in the ARTS SMS
	28	The system shall give the remote intervention operator personnel the ability to bring all vehicles across the system to a standstill according to suitable predefined procedures.				This includes high-level requirements for situations affecting the entire system: cyber attack, a sudden and large-scale weather event. Bringing vehicles to a standstill includes performing an MRM or other type of stop.
	29	The system shall give the remote intervention operator personnel the ability to open the vehicle's automatic doors under suitable conditions.				See EU ADS Regulation Annex II 6.5 "If a remote intervention operator is part of the ADS safety concept, it shall be possible for the remote intervention operator to open the power operated service door remotely."

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR REMOTE OPERATOR/COMMAND CENTER					
Communication from the command center	30	The system shall give the remote intervention operator personnel the ability to communicate with the system vehicle's passengers.				The following requirements shall be taken into account: ability to give passengers instructions when necessary, including: - if the system leaves its operational domain - if service is interrupted or modified - etc. Also see EU ADS Regulation Annex II Article 6.4 "If a remote intervention operator is part of the ADS safety concept, the fully automated vehicle shall provide vision systems (e.g., cameras in accordance with chapter 6 of ISO16505:2019) of the occupant space inside the vehicle and of the surrounding of the vehicle to allow the remote intervention operator to assess the situation inside and outside of the vehicle."

Table 6.5 - List of High-Level Requirements - Requirements for command center HMI

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR COMMAND CENTER HMI					
HMI	31	The system's HMI must be designed to limit the risks of misuse by the operating personnel.				- rapid assessment of the system or vehicle's situation - relevance of the information, prioritization - field of vision Concerns both the display of information (volume and presentation of the information, prioritization, etc.) and the control procedures (e.g.: principle of double entry or acknowledgment) - only a deliberate action from the operator shall enable a maneuver to be carried out, modified, or interrupted (see definition of remote intervention) - only a deliberate action from the operator shall enable maneuvers recommended by the system to be acknowledged (see definition of remote intervention)
	32	Activation or reactivation of automated driving mode shall require a specific and unambiguous action from the operator.				This includes following an emergency stop or an MRM (return to automated mode) - only a deliberate action from the operator shall enable automated driving mode (see "Automated driving safety validation: proposals from the French Eco-system" Jan 2020 - TR-01)
Information for operator personnel	33	The remote intervention operator personnel shall have the necessary information about the system status.				The system status shall include all relevant information related to the system: automated driving status, speed, door status, etc. - knowledge of the driving mode (see "Automated driving safety validation: proposals from the French Eco-system" Jan 2020 - T03)

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR COMMAND CENTER HMI					
Information for operator personnel	34	The remote intervention operator personnel shall have the means to perceive the vehicle's surroundings with a level of quality (precision, range, latency) that is consistent with their remote intervention duties.			EU ADS Regulation Annex II Article 6.4	EU ADS Regulation Annex II Article 6.4. "If a remote intervention operator is part of the ADS safety concept, the fully automated vehicle shall provide vision systems (e.g., cameras in accordance with chapter 6 of ISO16505:2019) of the occupant space inside the vehicle and of the surrounding of the vehicle to allow the remote intervention operator to assess the situation inside and outside of the vehicle."
	35	The command center shall receive information: - if the vehicle leaves the operational domain (see 1.4) - if the vehicle leaves the system technical design domain (see 2.2) - in the event of a failure that can affect safety (see 4.1) - in the event of a traffic accident involving a vehicle in the system (see 18) - if an MRM is initiated by a vehicle (see 19) - in the event of an emergency stop (see 21) - in the event of a passenger request to stop a vehicle (see 25) - in the event of a communication request by a passenger (see 26)				EU ADS Regulation Annex II Article 3.1.5. "When the ADS reaches the ODD boundaries, it shall perform a MRM to reach a MRC and shall warn the on board operator (if applicable)/remote operator accordingly (if applicable)" An emergency stop is the stopping of the vehicle following an emergency maneuver: see approval regulation (gamma threshold to be defined).
Information for third parties	36	The system shall enable third parties, law enforcement and emergency services to know the automated driving status of the vehicle			FRAV-23-05 Rev2 GRVA Table1-5	- including escort vehicles - FRAV-23-05 Rev2 GRVA Table1-5 "The ADS shall signal its operational status (active/inactive) as needed."

Area	No.	Title	No.	Sub-requirements	Source	Details
	REQUIREMENTS FOR COMMAND CENTER HMI					
Information for third parties	37	Law enforcement in the presence of a vehicle shall be able to communicate with the system command center			Draft order on Urban Automated Shuttles	Draft order on Urban Automated Shuttles: 7.7.9.6 "When necessary, the shuttle shall: 7.7.9.6.2 clearly display the following pictogram on the outside allowing law enforcement or any passenger to communicate with the operator from the outside"

8 Deductive analysis (preliminary hazard analysis)

8.1 Presentation

Deductive analysis uses an approach that starts from the effects and works towards the causes. It is designed to identify combinations of potential causes of an accident. This analysis starts from the hazards to determine the potential causes (Preliminary Hazard Analysis, PHA)

The starting point of deductive analysis is the accident. The analysis uses a in a top-down approach to explore all the causes and combinations of causes that could lead to the accident (causal analysis).
The deductive analysis does not analyze the causes of cyber attack type accidents. Taking these events into account is covered in specific guide.

Each scenario that results in an accident is then analyzed and the severity of its consequences estimated. This analysis takes into account potential factors related to the context (situation, aggravating factors such as the absence of a driver and staff and the collective nature of the collective transport system, etc.).

This analysis is used to define a set of safety, technical and/or organizational requirements which must be consistent with the high-level requirements presented in Section 7.

These requirements may involve the application of a standard outside the ARTS field for which it has been demonstrated that it covers the risk in question and its context (Type 3a demonstration of the GAME Implementation Guide) or the implementation of specific measures after having demonstrated that combining them would reduce the residual risk to an acceptable level (Type 3b demonstration of the GAME Implementation Guide).

- If an external standard is applied (Type 3a demonstration), the safety requirements from the external standard are those to be implemented;
- In the case of a detailed analysis (type 3b demonstration), evaluation of the frequency of each scenario makes it possible to estimate its criticality and define the safety requirements to be implemented.

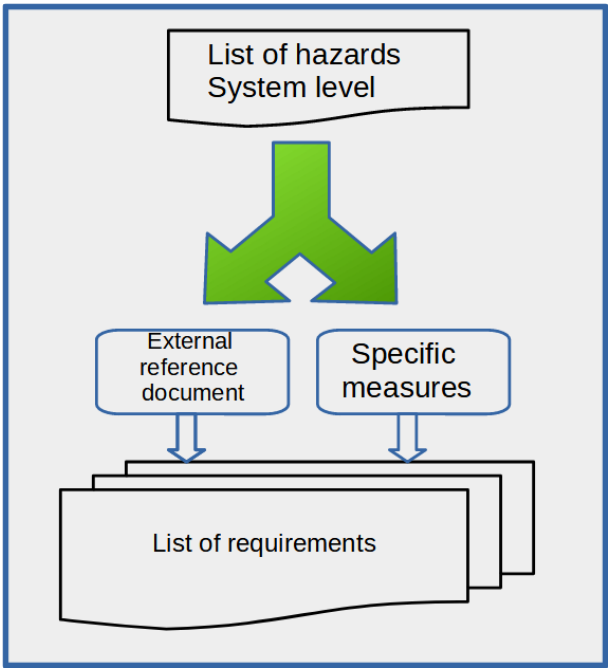

Figure 5 - Diagram of the deductive analysis

Objectives

- The deductive analysis is used to develop scenarios, estimate risks at the system level, and clarify their relevance.

- The deductive analysis is used to estimate each risk and specify the list of requirements to be implemented.

- Deductive analysis is a tool that uses fault trees to describe the causes leading to each accident in order to identify and chart the scenarios where quantitative, overall or specific safety objectives need to be demonstrated.

Project phases

- Deductive analysis is a high-level, system-wide approach that is first implemented at the DCST stage for a generic technical system associated with a known system technical design domain. The requirements that it identifies concern the design and architecture of the technical system, the constraints exported by the technical system to the type of route targeted and its operating conditions. These various elements define the system technical design domain included in the declaration of functionalities and safety provided for by the ARTS Decree (2021-873 of 29 June 2021).

- Then, at the DPS and DS stage, the specifics related to system-level deployment on the actual route are analyzed through the route safety analysis. The deductive analysis must then be completed in view of the traffic conditions on the specific route on which the technical system is deployed, in order to take into account the specific scenarios.

  The approach must ultimately serve to verify that all risks specific to the actual project have been taken into account in the analysis carried out at the generic level and that the safety objectives have been met for the system being deployed.

8.2 Outline

The following tables provide an example of an outline describing the various aspects of the deductive analysis (for illustrative purposes only).

POTENTIAL ARTS-LEVEL ACCIDENT				**IDENTIFICATION OF THE HAZARDOUS SITUATION**						
#	Type	#	Sub-type	Type of infrastructure section	Dynamics (of the actors in the situation)	Additional contextual information	Example(s) of the situation in question	**SUMMARY of the system-level hazardous situation (HS)**		Person(s) exposed
								Ref	Description	
1	Collision	1.1	Collision with a vulnerable road user (cyclist, pedestrian, etc.)	Running section with work zone		Operation of a system vehicle through a risk area that exacerbates the potential impacts of a hazardous event	Collision with a pedestrian crossing the road on a crosswalk as a result of not perceiving them in time (visibility obscured by heavy equipment). The braking distance was also extended due to the roadway being locally distorted by the ongoing work.			
associated with Table 8				associated with Tables 9 and 10						

POTENTIAL CAUSE(S)			**INITIAL RISK EVALUATION**							**TYPE OF GAME APPROACH**	
Potential contributor = Relevant component(s) of the ARTS	Type of potential cause(s)	Description	Severity		Exposure		Avoidability		Risk estimation ***(optional)***	Type	Description
			Classification	Comment(s)	Classification	Comment(s)	Classification	Comment(s)			
SMS	Route specificities, i.e. the specific characteristics of a route/area (or type of route) that would generate or increase the chance of an accident, or that would require a particular system response	Operation of a system vehicle in a work zone									
associated with Table 8											

Table 7.1 - Deductive Analysis Outline

SAFETY REQUIREMENTS		FINAL RISK EVALUATION						
Category	Description	Severity		Exposure		Avoidability		**Risk evaluation**
		Classification	Comment(s)	Classification	Comment(s)	Classification	Comment(s)	***(optional)***
- with respect to line of sight	- specify standard installations compatible with the system's capabilities							
- with respect to the management of work zones	- supervise the organization of work zones in the vicinity of the route							
	- requirements for the roads manager							
	- reduce speed in work zones							
- with respect to the condition of the roadway	- daily check of the route condition before the first trip							
	- specify maximum pavement distortion thresholds							

Table 7.2 - Deductive Analysis Outline

8.3 Input information for the deductive analysis

The following tables provide input information to be included in the deductive analysis:

- Table 8: List of system-level accidents;
- Table 9: List of causal focus points to be considered when determining possible causes of accidents (fault trees);
- Table 10: List of life situations that can be encountered within a system which must be taken into account in the scenarios;
- Table 11: List of the contextual aspects of a system that may influence the hazard response requirements.

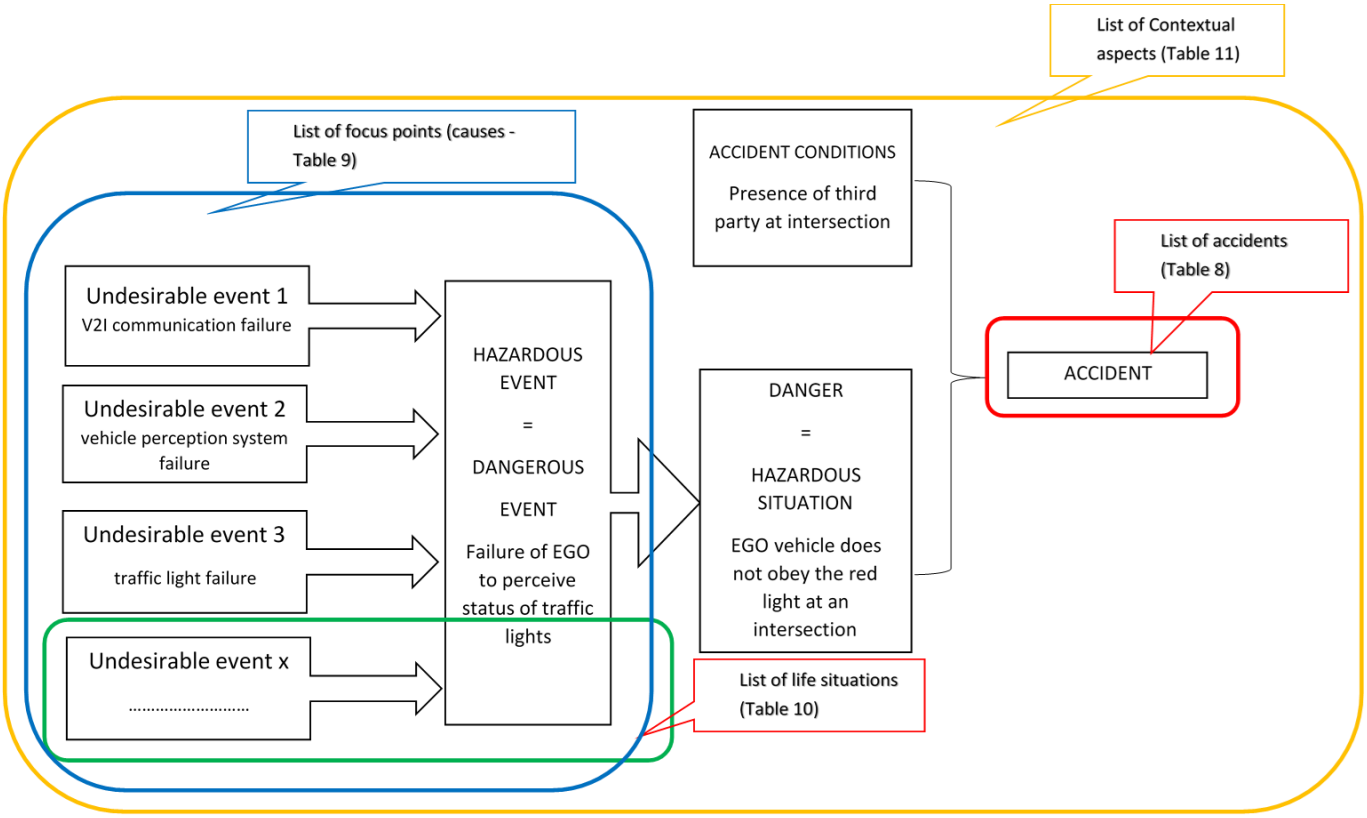

Figure 6 - Organization of the deductive analysis guide tables

The following tables provide generic lists of the various aspects to be taken into account, which are intended to be independent of the technologies implemented in the system, and the types of traffic routes. The purpose of these tables is to achieve greater exhaustiveness in risk analyses and to help in structuring these analyses. However, they must be adapted and supplemented if necessary by the project owners in view of the specificities of each system.

The analysis developed on the basis of these 4 tables should cover the entire operational domain of the ARTS, taking into account:

- All the types of objects that can be expected to interact with the components of the system in view of the operational domain of the ARTS, such as:
  - The system users (e.g., pedestrians, people with reduced mobility, with strollers, with heavy luggage, with personal mobility devices, etc.) present in the system vehicles or stations;

  - Vulnerable road users (e.g., pedestrians, persons with reduced mobility, with strollers, with heavy luggage, with personal mobility devices, with bicycles, cyclists, etc.) present in the traffic environment of the system vehicles;
  - Road users (e.g., different types of road vehicles);
  - Other transport systems (guided or rail transport, etc.);
  - Permanent and non-permanent obstacles / objects on the route;
  - Sight obstructions;

- All the types of events that can be expected to interact with the components of the system in view of the operational domain of the ARTS (in relation to its descriptors):
  - Weather conditions;
  - Light conditions;
  - The condition of infrastructure;
  - Etc.

- All the operating modes of the various system components (e.g., for vehicles: operating phase in manual mode (if applicable), driving phase in automated mode, remote intervention phase (if applicable), etc.)

- All life situations of the system in view of its operational domain (see Table 10)

The following rules must be observed when using the tables:

- The lists are not exhaustive and are meant to be added to in the course of a project.
- Conversely, although the listed requirements are intended to be generic, some of them may not be applicable to a specific project, in which case a substantiated record of their exclusion should be kept.
- One type of accident may be caused by another type of accident in a scenario: for example, a collision may occur as a result of the vehicle running off the road, a fire may occur as a result of a collision, etc. The analysis can then prioritize the management of the initial accident in order to put in place safety measures to prevent it.
- Some of the accidents included in Table 8 may be grouped together if the analysis shows that they are managed in the same way.

Table 8:
List of system-level accidents

TYPE	ID	POTENTIAL ACCIDENTS	ADDITIONAL INFORMATION (if any)	EXAMPLES (not exhaustive)
Collision	1.1	Collision with a vulnerable road user (cyclist, pedestrian, etc.)	In particular, the active "collision of the system vehicle with" and passive "collision of... with the system vehicle" cases must be considered	
	1.2	Side/head-on collision with a solid obstacle (containers, animals, falling trees, etc.)	The following cases shall be taken into account: - collision with fixed and permanent obstacles - collision with non-permanent fixed or mobile obstacles	Collision with permanent fixed obstacles: walls, barriers, etc. Collision with non-permanent fixed obstacles: tree branches, containers, etc. Collision with moving obstacles: animals
	1.3	Collision with another road vehicle	All relevant vehicle categories shall be considered In particular, the active "collision of the system vehicle with" and passive collision "of ... with the system vehicle" cases must be considered. Passive collision includes all configurations where the collision is not caused by the system vehicle but by a third-party vehicle (rear-ending, side collision at an intersection by another vehicle that fails to give right of way, during a maneuver of the other vehicle (e.g., reversing), etc.	
	1.4	Collision with the vehicle of a guided transport system (tramways, etc.) or rail transport system (heavy rail)	In particular, for collisions with a guided transport system, the active "collision of the system vehicle with" and passive "collision of... with the system vehicle" cases must be considered	
	1.5	Collision with another type of vehicle		Collision with non-road vehicles (e.g., heavy equipment)
Falls	2.1	A person falling inside the vehicle		Passenger loss of balance and fall following braking of the automated vehicle Passenger fall due to breakage of a handhold

TYPE	ID	POTENTIAL ACCIDENTS	ADDITIONAL INFORMATION (if any)	EXAMPLES (not exhaustive)
Falls	2.2	Fall of a person from the system vehicle in station	The term "in station" includes the following phases: - approaching and leaving the station, when the vehicle is in motion - at standstill in station, including during passenger transfers from the vehicle	Passenger falling from the vehicle on approach to the station as a result of the doors opening before the stop or on route Passenger falling from the vehicle when leaving the station as a result of restarting with the doors open Passenger falling when leaving or entering the vehicle due to untimely movement of the wheelchair ramp Passenger falling when leaving or entering the vehicle due to untimely closing of the doors Passenger falling when leaving or entering the vehicle due to breakage of a passenger handhold
	2.3	Fall of a person from the system vehicle while on route	The term "on route" includes the following phases: - vehicle in motion - vehicle stopped outside stations	Fall of passengers from the vehicle on route due to untimely opening of the doors Fall of passengers from the vehicle on route due to mechanical failure of a passenger restraint element (e.g., window)
Rollover	3.1	Vehicle rollover	The rollover can result from - vehicle instability - speeding on a curve - etc.	Rollover as a result of the vehicle running off the road Rollover due to excessive speed and hitting an obstacle Rollover as a result of the vehicle running off the road in a work zone Rollover due to excessive and poorly distributed load Rollover as a result of a mechanical failure (braking, etc.) Rollover due to collision with an obstacle on the roadway Rollover due to contact with an uneven road surface
Electric shock/Electrocution	4.1	Electric shock/Electrocution in the vehicle		
	4.2	Electric shock/Electrocution in station		

TYPE	ID	POTENTIAL ACCIDENTS	ADDITIONAL INFORMATION (if any)	EXAMPLES (not exhaustive)
Electric shock/Electrocution	4.3	Electric shock/Electrocution on the route from system equipment		Electric shock at a dedicated electrical cabinet Electric shock at a charging station on the route
Fire/smoke/explosion	5.1	Fire/smoke in the vehicle	In particular, a fire in the system vehicle caused by a fire in the immediate vicinity of the system vehicle shall be taken into account	
	5.2	Fire/smoke at a station		
	5.3	Fire/smoke on the route from system equipment		Fire in an electrical cabinet located on the route and specifically dedicated to the system
	5.4	Explosion in the vehicle		
	5.5	Explosion at a station		
	5.6	Explosion on the route involving system equipment		
Other passenger accidents	6.1	Passengers trapped/pinched by the openings (windows, doors, etc.) of a system component	In particular, cases of passengers being trapped in vehicle openings and platform edge doors shall be taken into account.	
	6.2	Passengers trapped/pinched by a moving part of system component		Passenger trapped in the mobile access ramp Passenger trapped in a turnstile
	6.3	Dragging of persons by the vehicle (in particular dragging of persons when the vehicle leaves the station or due to clothing being caught)		A person is dragged when the vehicle restarts to leave the station A person on the platform is dragged as a result of their clothing being caught

TYPE	ID	POTENTIAL ACCIDENTS	ADDITIONAL INFORMATION (if any)	EXAMPLES (not exhaustive)
Other passenger accidents	6.4	Contact with a harmful part of a system component (injury due to contact with/by protruding, sharp, pointed parts, etc.)		
	6.5	Contact with a hot or cold part of a system component		
	6.6	Contact with a hazardous liquid (toxic, corrosive, etc.) from one of the system components		
	6.7	Contact with a hazardous gas (toxic, etc.) from one of the system components		
Fall/projection or loss of object	7.1	Fall/projection/loss of parts from a system vehicles into the roadway	Note: may collide with a third party or system user on the route (e.g., other vehicle, pedestrian, etc.) or cause them to run off the road	- an obstacle left on the roadway by a system vehicle component causes a third party vehicle to run off the road/to collide with it - a part from a system vehicle hits a vulnerable user
	7.2	Passengers hit by a falling / projected / lost part of a vehicle in its passenger compartment	This case corresponds to the loss of a part/component of the vehicle, or untimely activation of safety equipment (e.g., airbag), etc.	
	7.3	Passengers hit as a result of objects carried in the passenger compartment of a system vehicle falling (e.g., luggage, packages, etc.)		
	7.4	Falling of objects from the system infrastructure (e.g., traffic lights, signs or station lighting, etc.)	Note: may collide with a third party or system user on the route (e.g., other vehicle, pedestrian, etc.) or cause them to run off the road	- a traffic light dedicated to the system falls on the roadway and causes a third party to run off the road/collision - a camera dedicated to the system falls on the roadway and hits a vulnerable user

Table 9:
Informative list of points not to be omitted from risk analyses when identifying possible causes of ARTS-level hazards

ID	Title	Additional information	Comment
1	**Failure to execute / or erroneous execution of a requirement / rule / operating procedure**	operator error maintenance defect failure to check etc.	
2	**No rule or rule unsuited for the intended use**	unsuitable operating procedure etc.	Related to constraint exported to SMS
3	**Characteristic(s) of the route or a system component not compatible or no longer compatible with the intended use**	Deteriorated performance of a sensor as a result of a change in brightness uneven road surface etc.	Related to the route safety analysis (or type of route)
4	**route specificities, i.e. the specific characteristics of a route/area (or type of route) that would generate or increase the chance of an accident, or that would require a particular system response**	presence of sight obstructions presence of an unplanned work site on the route ground markings erased along the route type of building in the vicinity presence of parking spaces in the immediate vicinity etc.	Related to the route safety analysis (or type of route)
5	**Electrical/electronic equipment failure**	sensor failure circuit board failure systematic software failure etc.	The failures considered are part of the causal chain leading to the accident The granularity of the analysis must be at the ARTS system level. The specific dedicated analyses will translate these system-level requirements into component-level requirements.
6	**Functional deficiency (SOTIF)**	Object classification error etc.	System-level analysis, identifying the functional safety analyses

ID	Title	Additional information	Comment
7	**Unsuitable design of interface devices and equipment (displays, markings, visual or audible signals, etc.) with third parties (system users, other road users, law enforcement, emergency services, operating personnel, etc.), leading to misuse**	Remote operator assessment error as a result of unclear or incomplete HMI passenger unable to contact the PCC due to lack of information in the vehicle operator error as a result of not being notified of a system element failure	The HMI is to be considered with respect to system users and third parties, including emergency services and law enforcement.
8	**Stresses from the external environment on the component (e.g., EMF, thermal, vibrations, chemicals, etc.)**	- any "industrial risk" constraints linked to the areas of operation shall be taken into account in the route safety analysis	
9	**Risks posed by the component on its environment (e.g., fuels, chemical catalysts, capacitors, batteries, pressure vessels, tension springs, pressurized fluids, traveling mechanism, objects that can be projected, pumps, materials that emit static electricity, energy in all its forms, switches, pyrotechnic devices, heaters, electrical generators, EMF, etc.)**	- e.g., gas released from batteries following mechanical impact - any "industrial risk" constraints created by the system in relation to the areas of operation shall be taken into account in the route safety analysis etc.	
10	**Imperfect / unsuitable design with respect to foreseeable use, ergonomic principles (e.g., mechanical undersizing, insufficient durability, electrical, slippery material, sharp corners, etc.)**	significant delay in communication between the vehicle and the remote operator causing an operator assessment error etc.	The vehicle approval covers several aspects of the list given in the title.
11	**Risks related to new technologies integrated into the system**		- risk related to an innovative technology integrated into the system (e.g., hydrogen, etc.) - risks related to cyber-attacks are not to be addressed at this level as they are covered by dedicated global requirements
12	**mechanical failure**	flat tire brake overheating following a failure etc.	
13	**fire in the vicinity of the system**	third party vehicle fire in front of the system vehicle fire in a tunnel on the route etc.	
14	**dangerous behavior of system users**	smoking violations destabilization of the system vehicle people voluntarily placing themselves in front of the vehicle etc.	

ID	Title	Additional information	Comment
15	**malicious and intentional user behavior**	- people voluntarily placing themselves in front of the vehicle - people hanging on to the vehicle - flame on the seats	The focus is on behaviors of the system users that are predictable for this type of automated system because they have already been observed on public transport systems

Table 10
Informative list of scenarios and maneuvers not to be omitted from risk analyses when identifying possible causes of system-level accidents

When analyzing hazards identified at the system level, certain situations in which these hazards may occur deserve special consideration and analysis. The following table provides a non-exhaustive list of these special circumstances for information purposes.

ID	situations	example of related accident
1	Interaction between a system vehicle and a law enforcement officer	Collision with a vehicle in an accident zone due to failure to understand a law enforcement officer's orders
2	Interaction between a system vehicle and an emergency vehicle	At an intersection, the vehicle collides with an emergency vehicle not recognized as such
3	Operation of a system vehicle in a work zone	The vehicle leaves the road due to a detour for a work zone
4	Unwanted stop of a system vehicle in a hazardous area (e.g., road intersection, railroad crossing, tunnel, viaduct, etc.)	Vehicle stopped in the middle of a railroad crossing
5	Situation generating panic inside a system vehicle	Passengers trapped as a result of panic due to a sudden release of smoke in the vehicle
6	Situation generating panic on the system's route or in a station inside a system vehicle	Sudden crowd surge due to panic caused by an explosion in the vicinity of the route
7	Fire in the vicinity of the system	Fire in the system vehicle following a fire in a third party vehicle behind which the system vehicle is waiting in the event of traffic congestion Fire in a building in the immediate vicinity of the system vehicle

Table 11
List of contextual elements that can influence the analysis of accidents

When analyzing accidents identified at the system level, the analysis of the impacts of these accidents can be modified by specific contextual aspects.
The following table provides a minimum list of contextual situations to consider. This non-exhaustive list may be adapted to the operational domain of the system.

ID	situations	examples
1	Operation of a system vehicle through a risk area that exacerbates the potential impacts of a hazardous event	- tunnel - viaduct - ravine - etc.
2	Operation of a system vehicle through an area where the configuration makes minimal risk maneuvers difficult	- tunnel - viaduct - narrow lane - etc.
3	Operation of a system vehicle through an area where the configuration makes passenger evacuation hazardous	- tunnel - viaduct - etc.

9 Inductive analysis (preliminary risk analysis)

9.1 Presentation

An inductive analysis systematically analyzes the consequences of potential system malfunctions. This analysis starts from the functions of the system to determine all the potential impacts should they malfunction (Preliminary Risk Analysis or PRA).

Inductive analysis uses an approach that starts from the causes and works towards the effects. Its purpose is to investigate malfunctions (failures and functional deficiencies) and to determine the resulting hazardous situations and scenarios, and all their possible impacts.

The starting point of the inductive analysis is the functional decomposition of the system. The principle of functional decomposition is to identify the so-called “root functions”, the sub-functions connected to them and their own sub-functions. The iterative process of searching for sub-functions continues as long as necessary and leads to a tree diagram where the position of a sub-function in the deductive tree does not predicate its importance for the system.

On the basis of this decomposition, a systematic analysis of the potential malfunctions of each elementary function and their impacts is conducted in order to construct all malfunction scenarios.
The inductive analysis does not include malfunctions due to cyber-attacks as these events are covered in a specific guide.

For each scenario resulting from a malfunction, the severity of its impacts (and its frequency for the Type 3b demonstration) is estimated in order to estimate its severity and to scale the requirements to be implemented to protect against it (functional FMECA).

These requirements may involve the application of a standard outside the ARTS field for which it has been demonstrated that it covers the risk in question and its context (Type 3a demonstration of the GAME Implementation Guide) or the implementation of specific measures after having demonstrated that combining them would reduce the residual risk to an acceptable level (Type 3b demonstration of the GAME Implementation Guide). These measures can be both qualitative and quantitative: function architecture, functional specifications, component reliability, etc.

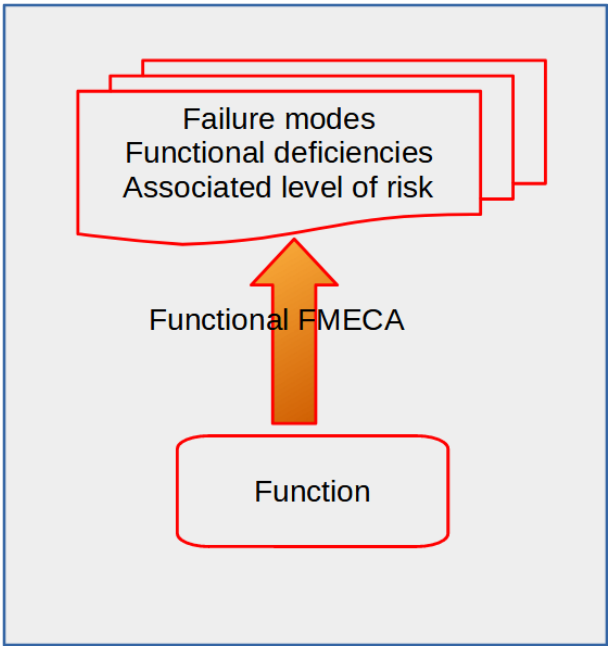

Figure 7 - Inductive analysis

The inductive analysis concerns all components of the system and can be conducted at different levels. The analysis presented here is carried out for the overall system and is used to determine overall requirements initially for the various functions of the system.
These requirements must then be broken down for the various sub-functions, and then the various equipment and components, in view of the architectures supporting the functions.

Objectives

- Identify all failures and functional deficiencies of the system that impact safety
- The inductive analysis is used to estimate and chart each risk resulting from the malfunction approach, in relation to system-level accidents.

Note: The inductive analysis is conducted before the allocation of safety objectives (see Section 5.4).

Project phase

- The inductive analysis is a high-level, system-wide approach that is first implemented at the DCST stage for a generic technical system associated with a known system technical design domain. The requirements that it identifies concern the design and architecture of the technical system, and the constraints exported by the technical system to the type of route targeted and to its operating conditions. These various elements define the system technical design domain included in the declaration of functionalities and safety provided for by the ARTS Decree of 29 June 2021).

- Then, at the DPS and DS stage, the specifics related to system-level deployment on the actual route are analyzed through the route safety analysis.
  The inductive analysis must then be completed in order to take into account the consequences of the malfunctions in the context of scenarios specific to the route.

9.2 Outline

The following tables provide an example of an outline describing the various aspects of the inductive analysis (for illustrative purposes only).

FUNCTION				IDENTIFICATION OF THE HAZARDOUS SITUATION					
Studied function			Failure or functional deficiency mode	SUMMARY of the system-level hazardous situation (HS)		Type of infrastructure section	Dynamics (of the actors in the situation)	Additional contextual information	Example(s) of the situation in question
#	Title	Description		Ref	Description				
3.2.1	Prevent doors from being authorized to open outside transfer or evacuation phases	Authorize the doors to open if all the conditions {C1&C2} are met C1 = immobilized vehicle C2 = listed zone or if emergency command is given	Untimely authorization to open doors			station or listed zone			Authorization to open doors while vehicle is not immobilized in station
						running section			Authorization to open doors while vehicle is not immobilized in station
						running section			Authorization to open doors while vehicle is immobilized but not in an authorized area.
			no authorization to open doors			running section			No authorization to open doors in an authorized area
						running section			No authorization to open doors in an emergency situation

Table 12.1 - Inductive Analysis Outline

POTENTIAL ARTS-LEVEL ACCIDENT						**OTHER POTENTIAL EFFECTS**	
DESCRIPTION	EFFECT = POTENTIAL ARTS-LEVEL ACCIDENT				Person(s) exposed		
	#	Type	#	Sub-type		1st level	potential consequences
passenger falls		Falls	2.2	Fall of a person from the system vehicle in station			
			2.3	Fall of a person from the system vehicle while on route			
passenger falls / passenger disembarking in unsuitable areas		Falls	2.3	Fall of a person from the system vehicle while on route			
						Service not provided	passengers panic
						High Level Requirement no. 23 for evacuation not met	self-evacuation of passengers not possible in emergency situations

INITIAL RISK EVALUATION							**ARTS-LEVEL SAFETY REQUIREMENT(S)**					
Severity		Exposure		Avoidability		**Risk evaluation** ***(optional)***	**TYPE OF GAME APPROACH**			Share of the quantitative Safety Objective allocated to the studied function, for the studied failure or functional deficiency mode		Required integrity level
Classification	Comment(s)	Classification	Comment(s)	Classification	Comment(s)		Type	Reference(s) used	Description	Document substantiating the sub-requirement	Value	

Table 12.2 - Inductive Analysis Outline

9.3 Input information for the inductive analysis

The proposed functional decomposition is structured according to a tree structure with four levels, the first 2 of which are presented in the figure below.

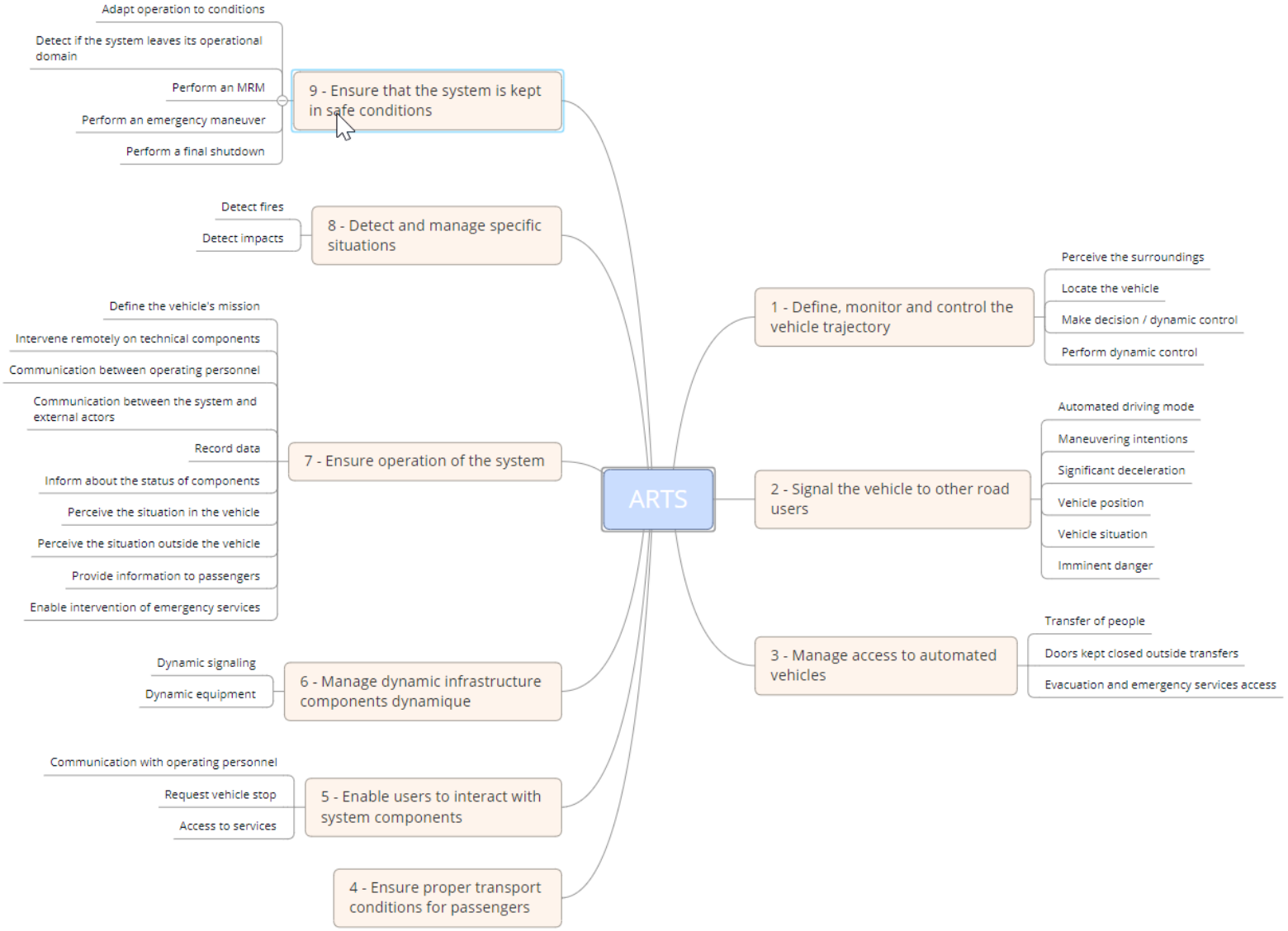

Figure 8 - Functional decomposition tree diagram

The following table provides a generic functional decomposition of an ARTS. This decomposition is intended to be independent of the technologies implemented in the system and the types of routes.

This table must be adapted and supplemented by the project owners in view of the specificities of each system.

The following rules must be observed when using the tables:

- The list of functions is not exhaustive and is meant to be added to in the course of a project.
- Similarly, although the listed functions are intended to be generic, some of them may not be applicable to a specific project, in which case a substantiated record of their exclusion should be kept.
- The functional decomposition follows a purely functional tree structure. The function’s level in no way reflects its importance with regard to safety issues or regulatory obligations.
  A function (whatever its level) can contribute by transmitting the flow (e.g., data, matter, energy, etc.) to several functions of an equivalent or higher level (e.g., function 1.1 “Sense the surroundings” can pass on useful data to functions 1.2; 1.3; 2; 3; etc.)
- The functions listed in the table do not include “technical” functions such as power supply, communication connections, etc. These must be considered at the analysis stage of each function to which they contribute.
- The functions of groups 7.2, 7.7 and 7.8 will be detailed in the supplements to this guide concerning remote interventions.

Table 13
ARTS functional decomposition framework

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
1-Define, monitor and control the vehicle trajectory		1.1-Perceive the surroundings (sense)	Function 1.1 enables the perception of data, for example: the detection of objects (static, dynamic, living beings, etc.), traffic events, conditions (weather, etc.) and infrastructure elements Can be performed by sensors: e.g., cameras, lidars, radars, (onboard/offboard)	1.1.1-Perceive/process objects	Static/mobile obstacles and/or other road users	1.1.1.1-Detect objects	Be able to detect an object on the trajectory or close to it
						1.1.1.2-Characterize objects	Be able to identify an object (bike, motorcycle, truck, animal, obstacle, pedestrian, law enforcement officer, emergency vehicle, etc.)
						1.1.1.3-Predict/interpret the behavior of objects	Anticipate the speed and trajectory of identified objects (before making a decision: I overtake, I stop, etc.) Interpret the gestures and orders of law enforcement officers
				1.1.2-Perceive/process infrastructure	Smart or otherwise (traffic lights, STOP sign, crosswalk, road marking, etc.), can also be provided by geolocation (a priori perception)	1.1.2.1-Detect infrastructure	Be able to detect infrastructure
						1.1.2.2-Characterize infrastructure	Be able to identify a static or dynamic piece of infrastructure (red light, green light, STOP sign, road markings, etc.)
						1.1.2.3-Process the status of infrastructure	Obey dynamic or non-dynamic signs (stop at red light, go at green light, stop at STOP sign, etc.)

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
1-Define, monitor and control the vehicle trajectory				1.1.3-Perceive/process EVs and law enforcement officers	-	1.1.3.1-Detect EVs and law enforcement officers	Detect emergency vehicles (EV), other vehicles with siren and blue flashing lights and law enforcement officers (LEOs)
						1.1.3.2-Characterize EVs and LEOs	Identify the types of EVs, and LEOs
						1.1.3.3-Interpret LEO orders and EV intentions	-
		1.2-Locate the vehicle on the route / area in relation to the defined route	Function 1.2 allows the vehicle to be located on a route/area The route can be defined at different levels: - before the mission (case of an ARTS deployed on a predefined route) - during the mission (case of an itinerary calculated and updated during the mission by the system according to external elements (traffic, command center	1.2.1 Know the mission (defined route)	Know the route to be followed for the transport service allocated to the vehicle, including passenger stations, on-demand stops, possible evacuation locations, etc. for example, in the case of a predefined route, by scanning and updating the map and the mission (time) in the system command center.	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
1-Define, monitor and control the vehicle trajectory			information, etc.) (case of a "robotaxi" ARTS for example) - etc.	1.2.2 - Locate the vehicle	Geolocate the vehicle (coordinates)	1.2.2.1-Load the map	Remotely monitor the position and the movement of the vehicle, and know in advance the environment in which the vehicle will operate. Take action if the position or movement deviates from certain pre-set values. => 1.3
						1.2.2.2-Locate the vehicle on the map	Geolocation can be provided by GPS signals and/or on-board sensors: e.g., IMU/odometry, with or without equipment deployed on the infrastructure.
		1.3-Make decisions about dynamic control (plan)	Based on perception (1.1) and location (1.2), decide on the movements and dynamic control of the vehicle, taking into account the mission, maneuvers and the regulatory constraints.	1.3.1- Decide on the operational actions for the longitudinal and lateral movement of the vehicle.	Decide on the next sequence of "nominal" maneuvers (with its longitudinal and lateral aspects) to be performed in the short term (e.g., turning left and changing lanes, while slowing down to x km/h etc.).	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
1-Define, monitor and control the vehicle trajectory				1.3.2- Decide on the tactical actions for the longitudinal and lateral movement of the vehicle.	Decide on the maneuver in real time (with its longitudinal and lateral aspects) to be performed immediately (e.g., decelerate, brake, and turn left by 10°)	-	-
		1.4-Perform dynamic control (act)	Function 1.4 provides control of lateral (steering) and longitudinal (braking and acceleration) movement, taking into account the energy used for traction/braking.	1.4.1-Perform longitudinal control	Meets service level requirements such as "obey the speed limit", "allow safe distancing".	1.4.1.1- Manage acceleration	- includes actions on traction and brake - includes consideration of gamma + and jerk values
						1.4.1.2-Manage deceleration	- includes actions on traction and brake - includes consideration of gamma - and jerk values
						1.4.1.3-Immobilize	- prolonged stop - ensure immobilization of the vehicle
				1.4.2-Perform lateral control (direction)	Basic function allowing the vehicle to position itself on the lane in the Y-axis (to center itself in the lane, to turn, to change lanes, etc.)	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
2-Signal the vehicle to other road users (sound, visual signals, etc.)	Depending on Function 1, signaling to other road users via audible warnings (horn, bell, etc.), via visual warnings (low beam, high beam, fog lights, turn signal, etc.), or via V2X communication. This function can be performed by the vehicle and/or infrastructure equipment (e.g., station arrival/departure maneuvering intentions)	2.1 - Signal the automated driving mode	-	-	-	-	-
		2.2 - Signal the vehicle's maneuvering intentions	- to other vehicles - to pedestrians - to VRUs - during specific phases (station entry/exit)	-	-	-	-
		2.3 - Signal a significant deceleration of the vehicle	see approval: signaling if gamma > threshold	-	-	-	-
		2.4 - Signal the vehicle's position	- nominal situations - situations with lack of visibility	-	-	-	-
		2.5 - Signal the vehicle's situation	- signaling following an MRM - signaling following an incident (hazard lights)	-	-	-	-
		2.6 - Signal an imminent danger	- in case of imminent danger detected by the ego vehicle (hazard lights, horn, flashing headlights, etc.)	-	-	-	-
	-	3.1-Manage the transfer of	Function 3.1 allows the transfer of people	3.1.1-Ensure limited vehicle/curb spacing	- case of public transport: horizontal and	3.1.1.1 - Respect a limited vertical gap	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
3-Manage access to automated vehicles		people at authorized locations	(boarding/disembarking of passengers/emergency services/service employees, etc.) at authorized locations (station, on-demand stop, etc.)		vertical gap < 50 mm (see accessibility decree of 13 July 2009) - Address the case of on-demand / robotaxi stop Deploy dedicated devices in the station or in the vehicle (mobile steps, kneeling system, etc.)	3.1.1.2 - Respect a limited horizontal gap	-
				3.1.2- Manage the opening and closing of doors to let people in/out	- open doors at authorized locations - prevent doors from opening other than at authorized locations and evacuation cases - etc.	-	-
				3.1.3-Manage entry and exit of PRM	Deploy dedicated devices in the station or in the vehicle (mobile steps, wheelchair ramp, kneeling system, etc.)	-	-
				3.1.4- Monitor the maximum capacity of the vehicle	-	3.1.4 .1 - Monitor the number of standing and/or seated passengers	-
						3.1.4.2 - Monitor the maximum authorized mass	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
3-Manage access to automated vehicles				3.1.5- Monitor vehicle restart conditions with respect to mobile access and boarding devices	- position of doors, elevators, ramps, kneeling system, etc. - no one trapped - no users being dragged	-	-
		3.2-Keep the automated vehicle closed when not transferring people/evacuating	Outside of the authorized locations, Function 3.2 ensures that the doors are kept closed.	3.2.1 - Prevent doors from being authorized to open outside transfer or evacuation phases	-	-	-
				3.2.2 - Monitor door status	monitor door locks and closed position outside of transfer or evacuation phases	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
3-Manage access to automated vehicles		3.3-Enable evacuation and emergency access	In addition to Functions 3.1 and 3.2, Function 3.3 enables passenger evacuation and emergency access.	3.3.1- Provide a means for passengers to evacuate the vehicle	Sufficient and accessible emergency exits. Accessible and suitable opening means. Case of PRM to be taken into account For Cat M2 and M3, the approval requirements set the number of emergency exits (see UNR 107). Case of automatic door opening control in emergency situations.	-	-
				3.3.2 - Provide means for technical personnel and emergency services to access the inside of the vehicle		-	-
				3.3.3 - Inform the remote operator if the emergency exit opening systems are activated for evacuation		-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
4- Ensure proper transport conditions for passengers	These functions ensure passenger comfort (thermal, acoustic, vibratory, support, brightness and visibility, etc.) However, some of these functions may present a safety issue, and must therefore be taken into account in the safety demonstration. For example, lighting inside the vehicle may be necessary to prevent the risk of passengers falling; defogging of windows to allow passengers to see their surroundings may be important in the event of an evacuation.						
5- Allow users to interact with system components	-	5.1-Enable the users to communicate with operating personnel (COM)	Function 5.1 ensures sound and visual communication between users (on board the vehicle and at the station) and the operating personnel.	5.1.1 - Enable system users to interact with operating personnel	Vehicle intercom, station intercom, etc.	-	-
				5.1.2 - Enable system users to alert the operating personnel	e.g., via Passenger Assistance System (NAV URB AUT project)	-	-
		5.2 Allow passengers to request that the vehicle be stopped	Passenger emergency stop request system (NAV URB AUT project)	-	-	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
5- Enable users to interact with system components		5.3-Provide users with access to services	Function 5.3 provides access to services for users at the station/ on smartphones/ in vehicles, etc. (e.g., schedule, tickets, booking, etc.). Some of these functions may present safety risks	-	-	-	-
6-Manage dynamic infrastructure components controlled by the system	Function 6 allows the management of dynamic signaling (right of way management with traffic lights, speed, etc.), dynamic segregation components (barriers, bollards, etc.), etc.	6.1 Control dynamic signaling	e.g., control of smart traffic lights	-	-	-	-
		6.2 Control mobile dynamic equipment	e.g., control of mobile barriers, retractable bollards, etc.	-	-	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system	Manage the fleet and missions, overall service, monitor the environment of the system components on the route/area, change/plan missions, activate a fall-back mode (refuge).	7.1 - Define the mission of each vehicle	- Define the route constraints for the transport service allocated to the vehicle, including passenger stations, on-demand stops, possible evacuation locations - Define the time constraints (date, departure time, arrival time, scheduled stops, frequency, etc.) The mission can be defined beforehand according to the conditions expected on the route, or be modified during operation according to the events encountered or known. (requires communication with external services. See 8.4)	-	-	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system		7.2- Intervene remotely on technical components of the system	Function 7.2 ensures the different types of remote intervention provided by the system. Remote intervention: Action performed by an authorized person located outside an automated road transport system for the purpose of: • activating or deactivating the system, or to giving instructions to perform, modify or interrupt a maneuver, acknowledging maneuvers recommended by the system • instructing the system to choose or modify the schedule of a route or stops for users (in particular in response to incidents or failures).	7.2.1 - Stop the vehicle(s)	immediate in station area, next stop, ASAP, etc.	-	-
				7.2. 2 - Activate/deactivate automated driving mode		-	-
				7.2.3 - Give instructions to the vehicle(s)	speed reduction, maximum speed set point	-	-
				7.2.4 - Acknowledge a proposed maneuver		-	-
				7.2.5 - Order a vehicle maneuver		-	-
				7.2.6 - Interrupt a maneuver	Define the status after an interruption	-	-
				7.2.7 - Modify a maneuver		-	-
				7.2.8 - Control vehicle equipment	windshield wipers, lighting, etc. ramps doors, etc.	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system				7.2.9 - Perceive the traffic surroundings around the vehicle	Detection of third parties in the vicinity according to the maneuver to be performed or the command to be carried out in order to perform the maneuver	-	-
				7.2.10 - Perceive the surroundings of the controlled equipment, to give the authorizations to maneuver or start	door surroundings if doors are controlled remotely or in the event of a fault, PRM ramp surrounding if it is controlled remotely	-	-
		7.3-Enable communication between the operating personnel	Function 7.3 ensures communication between operating personnel. For example, communication between operating personnel located at the command center and operating personnel on site or in the vehicle	-	-	-	-
		7.4-Enable communication between the system and external actors	Function 7.4 provides communication between the operating personnel and external actors (e.g., law enforcement, PCC operators, Prefect in the case of an ORSEC crisis-management plan or emergency services	7.4.1 - Enable the initiation of communication with the system at the request of the external actor	means for the actor to establish communication	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system			such as firefighters, emergency medical services (SAMU), service providers (EDF, telecom), the city authorities, and utility and public roadwork workers (Gas, local traffic department (DDE), electricity (EDF), etc.).	7.4.2 - Enable communication between the operating personnel and external actors	communication at the initiative of the personnel or at the initiative of the external actor (e.g., law enforcement officer, emergency services)	-	-
				7.4.3 - Enable communication of necessary information to the external actor	e.g., vehicle documents for law enforcement officers	-	-
		7.5-Record data	Function 7.5 provides data recording to meet the operating needs.	7.5.1 - Record data from the various subsystems for continuous improvement of the system	-	-	-
				7.5.2 - Record data from the various subsystems for accident analysis	See ARTS decree, Art R3152-22	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system		7.6- Inform about the status of the system components	Function 7.6 provides supervision/operation (display component status, alerts, events, conditions (weather, etc.), etc.)	7.6.1 - Inform about the vehicle status	Including battery charge level Including seat belts Including door status Including emergency exit status Including instantaneous speed, etc.	-	-
				7.6.2 - Inform about the vehicle operating conditions	e.g., vehicle being evacuated, vehicle on standby, vehicle automated driving status, stop following an emergency maneuver, stop following an MRM, stop following collision, event	-	-
				7.6.3 - Inform on the status of the system equipment, or equipment involved in system safety.	Including the command center Including pre-existing system equipment involved in safety	-	-
		7.7- Enable the operator to see the situation in the vehicle	passive listening cameras on passengers	7.7.1 - Perceive the sound environment inside the vehicle	-	-	-
				7.7.2 - Provide a view of the inside of the vehicle	-	7.7.2 - Provide a full view of the inside of the vehicle	e.g., manage passenger stop requests

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure operation of the system					-	7.7.3 - Provide a view of specific spots inside the vehicle	for example, to identify or remove doubts (door jamming areas, fire, etc.)
		7.8- Enable the operator to see the situation outside the vehicle	-	7.8.1 - Perceive the surroundings of the vehicle		7.8.1.1 - Perceive the traffic surroundings around the vehicle	Perception of evacuation or maneuver conditions, including weather conditions
						7.8.1.2 - Provide a view of specific spots outside the vehicle	for example, to identify or remove doubts: door areas on the platform side, ramp area, fire Verification that no one is trapped, that a passenger is not being dragged, etc.
				7.8.2- Enable the operator to know the situation along the route		7.8.2.1 -Know the foreseeable traffic conditions along the route	traffic and weather conditions in order to adapt the operating instructions (see 10.1)
						7.8.2.2 -Know the traffic conditions at specific points along the route	for example, remote view of a railway level crossing or accident zone
		7.9 - Enable information to be	Function 7.9 communicates sound and visual information to users (on board the vehicle and at the station).	7.9.1- Provide information to users at the station	audio or display messages	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
7- Ensure the operation of the system		communicated to passengers		7.9.2- Provide information to vehicle passengers	audio or display messages	-	-
		7.10 - Enable the safe intervention of emergency services	Existence of vehicle immobilization, electrical isolation and other means that are known and accessible to emergency services	-	-	-	-
8- Detect and manage specific situations	-	8.1 - Detect and manage fires	-	8.1.1 - Detect and manage fires in vehicles	-	-	-
				8.1.2 - Detect and manage fires in stations	-	-	-
				8.1.3 - Detect and manage fires in equipment along the route	Including equipment dedicated to supervision	-	-
				8.1.4 - Detect and manage fires in command center equipment	-	-	-
		8.2- Detect impacts against the vehicle	in the event of a collision affecting the safety of passengers or third parties (third parties, fixed obstacles, etc.)	-	-	-	-

level 1		level 2		level 3		level 4	
Functions	Comments	Functions	Comments	Functions	Comments	Functions	Comments
9 - Ensure that the system is kept in safe conditions	-	9.1 - Adapt operating instructions to traffic conditions	speed reduction, preventive stop of the service in the event of fall-back conditions > threshold (traffic and/or weather)	-	-	-	-
		9.2 - Detect if the system leaves its operational domain	Including malfunction of external safety equipment	-	-	-	-
		9.3 - Perform an MRM suitable for the situation	adapted to the context, to the situation of the route, etc. (including in case of failure to acknowledge on the part of the operator)	-	-	-	-
		9.4 - Perform an emergency maneuver adapted to the situation	-	-	-	-	-
		9.5 - Perform a "final" shutdown	function(s) related to meeting the requirement to maintain the ability to stop the vehicle even in the event of a major system failure resulting in the inability of the system to perform an MRM (FAILURE MITIGATION STRATEGY see SAE J3016_202104 3.11)	-	-	-	-

10 Annex

In accordance with Decree no. 2010-1580 of December 17, 2010, creating the Technical Service in Charge of Safety for Ropeways and Guided Transport (STRMTG). STRMTG is in charge of producing guides and standards.

This document was prepared by the national GAME ARTS working group created by STRMTG.

Director: Pierre Jouve - STRMTG - Automated Public Transport Department
Secretary: Mr Florent Sovignet - STRMTG - Automated Public Transport Department

Mr	Courtet	Alstom
Mr	Guesdon	Alstom
Mr	Poisson	Alstom
Mrs	Quiney	Alstom
Mr	Alliouche	Bureau Veritas
Mr	Boniakowski	Bureau Veritas
Mr	Clarissou	Bureau Veritas
Mrs	Dam	Bureau Veritas
Mr	Travers	Cara
Mr	Belloche	Cerema
Mr	Sautel	Cerema
Mr	Russo	Certifer
Mr	Testemale	Certifer
Mr	Willmann	CETU
Mr	Audige	DGITM
Mr	Delache	DGITM
Mr	Diez	DGITM
Mrs	Lanaud	DGITM
Mr	Launay	DSR
Mr	Dupont	Easymile
Mr	Pagliero	Easymile
Mr	Chauvin	GART
Mr	Lesot	Ile-de-France Mobilités
Mrs	Brini	IRT System X
Mr	Aubourg	Keolis
Mrs	Benmhalla	Navya
Mrs	Hu	Navya
Mr	Renaud	Ramsai
Mrs	Berthault	RATP
Mr	Boulineau	RATP

Mr	Arnoux	Renault
Mr	Rousseau	Renault
Mr	Sencerin	Renault
Mr	Geronimi	Stellantis
Mr	Lenti	Stellantis
Mr	Brun	STRMTG
Mr	Dusserre	STRMTG
Mr	Maisonobe	STRMTG
Mrs	Torelli	Systra
Mr	Tran	Systra
Mr	Dadou	SYTRAL
Mr	Negrier	SYTRAL
Mr	Bakadal	Transdev
Mr	Desmoineaux	Transdev
Mr	Baranowski	Gustave Eiffel University
Mrs	Cuvelier	Gustave Eiffel University
Mr	Herveleu	UTAC
Mr	De Sousa Fernandes	UTAC

Mr Ludovic Brun, STRMTG legal advisor, also contributed to the review of the guide