IMPLEMENTATION GUIDE

STRMTG
SERVICE TECHNIQUE DES REMONTÉES MÉCANIQUES ET DES TRANSPORTS GUIDÉS

AUTOMATED ROAD TRANSPORT SYSTEMS

Implementation Guide on cybersecurity for ARTS

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

Version 1 of December 19, 2022

Purpose - Scope - Recipients

This implementation guide explains cybersecurity requirements 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 (ARTS) Decree).

It applies to automated road transport systems (ARTS), defined by Article R.3151-1 of the French Transport Code (supplemented 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 public transport sector, including: Public transport authorities, project owners, operators, project managers, engineering firms, approved qualified organizations (OQA), automated road transport system designers, and equipment manufacturers.

The purpose of this guide is to clarify and define the applicable requirements in terms of the measures to be implemented to limit cyber risks. These requirements have been formalized in consultation with the profession to provide a framework to facilitate the work of professionals. They are not regulatory in nature, but their observance can be seen as an indication of compliance with regulatory requirements and/or the suitability of the approach adopted.

The scope of this guide is limited to cybersecurity risks that could affect the safety of occupants and third parties with regard to the operation of the automated road transport system, i.e. when a human driver is not carrying out the dynamic control of the vehicle on roads open to public traffic (i.e. roads where there is nothing to prevent use by the public).

This guide covers cybersecurity risks that could affect the safety of operating and maintenance personnel with respect to the operation of the system under these conditions:

- occupants, when they are on board the system's vehicles,
- third parties, when they are present on the route.

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

It is not a substitute for any other cybersecurity regulations applicable to such systems, including:

- Transposition of Version 2 of the European Network and Information System Security Directive (NIS2);
- European Regulation No. 2022/1426 of August 5, 2022 regarding type-approval of the automated driving system (ADS) of fully automated vehicles and UN Regulations No. 155 and No. 156 which it references;
- The French Military Programming Law and its implementing texts, if applicable.

This guide does not address:

- Internal cybersecurity issues for external actors: emergency services, road managers, etc.;
- Cybersecurity issues specific to public access buildings such as stations, except for their interfaces with the transport system;
- Consideration of potential cybersecurity risks generated by project works when they do not impact an existing automated road transport system;
- Psychological and mental safety that could be affected by a cyber attack;
- Potential damage to organizations and their image caused by a cyber attack:
- Potential damage caused to individuals by the breach of their personal data following a cyber attack;
- Potential impacts of a cyber attack on the availability of a system when the safety of the system's users and third parties is not impacted;
- The potential financial impact of a cyber attack.

This initial guide is intended to be supplemented incrementally as work on ARTS cybersecurity is enriched.

Revision history

Version number	Author	Date	Description
1	F. BRUN	12/19/2022	Created by the ARTS Cybersecurity Working Group

WRITTEN BY	EDITED BY	APPROVED BY
François Brun Automated Public Transport Project Manager	**Pierre Jouve** Head of the Automated Public Transport Department	**Daniel PFEIFFER** Director
Signature numérique de François BRUN francois.brun Date : 2023.09.01 15:15:50 +02'00'	Signature numérique de Pierre JOUVE pierre.jouve Date : 2023.09.04 17:06:02 +02'00'	Le Directeur du Service Technique des Remontées Mécaniques et de Transports Guidés Daniel PFEIFFER Date : 2023.09.04 17:31:19 +02'00'

Service Technique des Remontées Mécaniques et des Transports Guidés (STRMTG)
1461 rue de la piscine
38400 St Martin d'Hères, FRANCE
Tel.: +33 (0)4 76 63 78 78
email: strmtg@developpement-durable.gouv.fr
www.strmtg.developpement-durable.gouv.fr

Table of contents

Table of illustrations

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). This decree is referred to in the rest of this document as the "ARTS Decree".

It makes the commissioning of an automated road transport system on a predefined route or traffic area conditional on a safety demonstration formalized through a technical system design file (DCST), a preliminary safety file (DPS) and a safety file (DS). These files are each accompanied by the opinion of a qualified organization approved (OQA) by STRMTG.

Once the ARTS is commissioned, the operator will have an OQA perform an annual external audit of the operational safety management system.

The assessments conducted by OQAs cover a number of technical areas, including cybersecurity.

The purpose of this guide is therefore to specify the cybersecurity requirements that apply throughout the life cycle of an ARTS, whether it be:

- ***Prior to commissioning**, from design studies to installation of the system on a predefined route or traffic area, or*
- ***After commissioning**, with regard to the operation and maintenance of the system until its removal from service.*

*Demonstrating compliance with these requirements **prior to commissioning** is an integral part of the safety demonstration. Because cybersecurity risks can affect all components of a system and all phases of its development, cybersecurity requirements can impact all aspects of the safety demonstration. The components of this demonstration are not included in this guide. However, some of them present elements concerning cybersecurity, which should be taken into account with the following precautions:*

- *Vehicles covered by the Automated Road Transport Systems Decree are first subject to prior approval under the French Highway Code. Approval (or homologation) is the administrative certification of the conformity of the vehicle to the requirements of the technical regulations in order to allow its registration and operation. This process is not addressed in this guide. Approval is a prerequisite for demonstrating safety, but it is not enough to demonstrate the safety of the systems. By definition, the scope of the approval is limited to the vehicle and any of its interfaces. Therefore, while the results of the approval and its associated standards/reference documents serve as input data for the safety demonstration of an ARTS, the analyses performed as part of the approval cannot replace system-level analyses.*
- *Similar to the demonstration of compliance with safety requirements, the demonstration of compliance with cybersecurity requirements applicable to the technical system or ARTS is performed at the system level. It is performed:*
    - *For each technical system, in its technical design domain,*
    - *For each ARTS, in its operational domain for a predefined route or area.*

  The implementation of these requirements must take into account reasonably foreseeable operating conditions, accessibility of system equipment, etc.
- *The GAME (Globally at least equivalent) demonstration is covered by an implementation guide and a technical guide that do not address cybersecurity but contain elements that may relate to the applicable requirements described in this guide. These elements will nevertheless need to be the subject of a specific cybersecurity analysis.*

***Post-commissioning** compliance with applicable cybersecurity requirements must be assessed and documented at various times:*

- *During the annual external audit of safety in operation, which must assess the implementation of the safety management system in operation, the effectiveness of internal control and whether the safety management system meets changing operational safety issues.*
- *During the diagnosis that may be requested by the prefect in the event that the annual report on the operational safety of the system prepared by the operator is lacking, or if there is serious doubt concerning the implementation of the safety management system or the intervention and safety plan, or about their adequacy in relation to safety issues.*

- *At the request of the prefect, during assessment of the operator's analysis of a serious accident or incident.*

Bibliography

Legislation

- [01] French 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
- [02] UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system [2021/387]
- [03] French Order of August 11, 2016, setting the security rules and reporting procedures for vital information systems and security incidents relating to the vital “Land Transport” sub-sector pursuant to Articles R. 1332-41-1, R. 1332-41-2 and R. 1332-41-10 of the French Defense Code
- [04] UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system [2021/388]
- [05] Decree No. 2017-440 of March 30, 2017 on the safety of public guided transport systems

Standards

- [06] ISO/SAE 21434:2020 - Road vehicles — Cybersecurity engineering
- [07] CLC/TS 50701:2021 - Railway Applications - Cybersecurity
- [08] ISO 26262:2018 - Road vehicles - Functional safety
- [09] EN 50126-1 October 2017 - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
- [10] EN 50126-2 October 2017 - Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
- [11] ISO/IEC 15408:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Parts 1 to 5
- [13] IEC 62443-1-1:2009 - Industrial communication networks – Network and system security
- Part 1-1: Terminology, concepts and models
- [14] IEC 62443-3-3:2009 - Industrial communication networks – Network and system security
- Part 3-3: System security requirements and security levels
- [15] SAE J3016 2021-04-30 – Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
- [16] ETSI TR 102 893 – Intelligent Transport Systems (ITS) – Security – Threat, Vulnerability and Risk Analysis (TVRA)
- [17] ISO 21448:2022 - Safety of the intended functionality (SOTIF)
- [18] NF EN 50159 August 2021 - Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems
- [19] ISO/IEC/IEEE 15026-2:2011 - Systems and software engineering — Systems and software assurance
- [20] ISO/TR 4804:2020 - Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation

Guides and best practices

- [21] GAME Implementation Guide for ARTS
- [22] Technical Guide for GAME demonstration for ARTS
- [23] EBIOS Risk Manager Method
- [24] AFNOR Publication - Voluntary standards and innovative approaches to cybersecurity
- [25] ENISA - Good practices for security of Smart Cars
- [26] Implementation guide concerning the mission of the approved qualified organization for the safety assessment and the operational safety audit for ARTS

Definitions

The definitions below are taken from Articles R311-1, R311-1-1 of the French Highway Code and Article R.3151-1 of the French Transport Code (these definitions are not limited to cybersecurity):

Technical system designer	The natural or legal person responsible for the overall design of the technical system and for defining its functionalities and conditions of use.
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.
Operator	A natural or legal person who, directly or at the request of the transport authority, operates the transport system and manages and maintains it. The operator may be the same entity as the transport authority or the designer of the technical system. In the case of multiple operators, the term operator refers to the lead operator.
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, in order to: 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.
Substantial modification	Any change to an existing automated road transport system or part of a system, where the modification alters the safety assessment;
Transport authority	For public transport services provided under Article L. 1221-3 of the French Transport Code, the local authority responsible under Article L. 1221-1 or L. 1241-1 of the Transport Code; for public transport services organized under Part III, Book 1, Title 1, Section 3 of the Transport Code, the company referred to in Article L. 3111-17 of the Transport Code; for private public transport services, the operator under Article L. 3122-1 of the Transport Code; for private services, the natural or legal persons mentioned in R. 3131-1 and R. 3131-2 of the Transport Code.
Approved qualified organization (*Organisme qualifié agréé - OQA*)	Organization approved to conduct the safety assessment of the design, implementation and operation of automated road transport systems.
Automated driving system	System combining hardware and software enabling the sustained dynamic control of a vehicle.
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.

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".*
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 takeover of control during a maneuver performed within its operational design domain. 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, clarification of the following terms is provided on the basis of definitions from existing publications or those developed within the specific framework of this guide:

Accident	An unexpected event or series of events causing damage, which may involve the safety of people (this refers to the occupants and third parties with respect to the functioning of the system in operation).
Traffic accident	A collision between a vehicle and another vehicle or a moving or fixed obstacle.
Cybersecurity activity	Activity performed in accordance with one or more applicable cybersecurity requirements
Risk analysis	Systematic use of all available information to identify hazards and estimate the risk (EU Regulation 402/2013).
Attacker	See "Threat source/actor".
Need to know	Compelling need to know information in the context of a specific function and in order to properly perform a specific mission (source: IGI 1300).
Supporting asset	Asset to be protected in view of its role in the safety of the occupants and third parties.
Compromise of a system-level function	Cybersecurity breach of a system-level function resulting in loss, disclosure and/or corruption of data (inspired by CLC/TS 50701)
Constraint	Contextual element against which no cybersecurity objectives can be set (as opposed to an assumption); this may take the form of regulatory or factual elements that are imposed on the project.
Hazard	A condition that could lead to an accident (EU Regulation 402/2013 of April 30, 2013).
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).
Ecosystem	All the stakeholders who interact with the object of the study and help it achieve its missions (EBIOS Risk Manager method guide).

Responsible Entity	A legal entity that is responsible for deliverable(s) or activity(ies) involving assessment and/or audit by an OQA.
Hazardous event	An unwanted event that can cause a dangerous situation and an accident under certain conditions.
Cybersecurity event	Expression of the direct impact of an attack on a task or a function of the system under consideration
Cybersecurity requirement[1]	Requirement or expectation explicitly or implicitly stated in this guide.
Cybersecurity functional requirement	Elements required to achieve cybersecurity objectives.
System-level function	Action or activity specified at the system level that can be performed by technical means and/or humans with a defined output in response to a defined input (according to EN 50126-1).
Assumption	An existing situation that makes it possible to dispense with a cybersecurity objective and thus reduce the scope of cybersecurity risk assessment (as opposed to a constraint). The assumption is formulated in cases of risk sharing or risk retention; it is recommended that reasons be given for choosing the assumption.
Impact	Direct or indirect consequence of unmet security needs on the system and/or on its environment due to a hazardous event.
Digital infrastructure	All the equipment required to communicate and connect to 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 supervision equipment.
Interface	Logical and/or physical input or output that provides access to the system for information flows (inspired by IEC 62443-1-1:2009).
Cybersecurity maintenance	All activities aimed at ensuring that the system maintains a constant level of cybersecurity, adapted to the changing threat (inspired by the ANSSI security rules concerning the protection of OIV).
Threat	Generic term used to designate any hostile intent to do harm in cyberspace. A threat can be targeted or not on the studied object. (EBIOS Risk Manager Method)
Cybersecurity measure	Measures identified to meet functional cybersecurity requirements.
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).
Mission of the system	Function, end purpose, reason of existence of the system under consideration (EBIOS Risk Manager method)
Cybersecurity objective	The goal to be achieved in order to reduce an identified risk to an acceptable level, by acting on the attractiveness, difficulty, vulnerability or impacts.
Stakeholder	Any individual or organization in the ecosystem that can affect, be affected by or perceive itself to be affected by a decision or activity (inspired by ISO Guide 73 and the EBIOS Risk Manager method).

[1] Explicitly formulated requirements are identified by “EX-X.XX” in the rest of the guide (see parts 4 and 5 of the guide).

Attack potential	A combination of the motivation and capabilities of a threat source. Capabilities include the available resources and expertise of the threat source (inspired by ISO 18045).
Cybersecurity risk	Scenario, with a given level, combining a cybersecurity event with a threat scenario and an impact scenario. Its level corresponds to the estimation of its severity and likelihood. [ISO Guide 73]
Residual risk	Risk remaining after risk treatment. [ISO Guide 73]
Hazardous situation	A situation in which persons are (or could have been) exposed to one or more hazards.
Threat source	Source or person responsible for threats. It can be characterized by its type (human or environmental), by its cause (accidental or deliberate) and, depending on the case, by its available resources, expertise, motivation. (According to [ISO Guide 73])
Collection strategy	Identifies the list of collection sources, collectors, events to be collected, describes the collection methods (protocols, applications, security properties, etc.) and identifies the frequency of collection in cybersecurity performance monitoring. [PDIS Requirements reference document Version 2.0]
Analysis strategy	Includes a precise description of the implementation of detection rules for detecting security incidents based on the events collected under the collection strategy as part of cybersecurity performance monitoring. [PDIS Requirements reference document Version 2.0]
Notification strategy	Identifies the list of security incidents to be reported, including the format, content, time limit, and the level of sensitivity or classification of the reports, as well as the persons to be notified, particularly with respect to the security incident and its level of severity. [PDIS Requirements reference document Version 2.0]
System under consideration	Term used generically. It can designate a complete automated road transport system, a technical system, a subsystem, a component or equipment.
Risk treatment	A sub-process of risk management for selecting and implementing security measures to modify information security risks. [ISO Guide 73]
Vulnerability	The propensity of an environment, property or person to suffer harmful consequences as a result of an event. In itself it does not generate the consequences.

Abbreviations

CAL: Cybersecurity Assurance Level

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*)

PMD: Personal Mobility Device

ERP: Public access building (*Etablissement recevant du public*)

GAME: Globally at least equivalent or Globally at least as good (*Globalement au moins équivalent*)

MRM: Minimal Risk Maneuver

OIV: Operator of Vital Importance (*Opérateur d'Importance Vitale*)

OQA: Approved qualified organization (*Organisme qualifié agréé*)

OSI: Open Systems Interconnection

SMS: Safety Management System

ARTS: Automated Road Transport System

1 Scope

1.1 Constituent or interfacing elements

An ARTS can be made up of various specific 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 other 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.

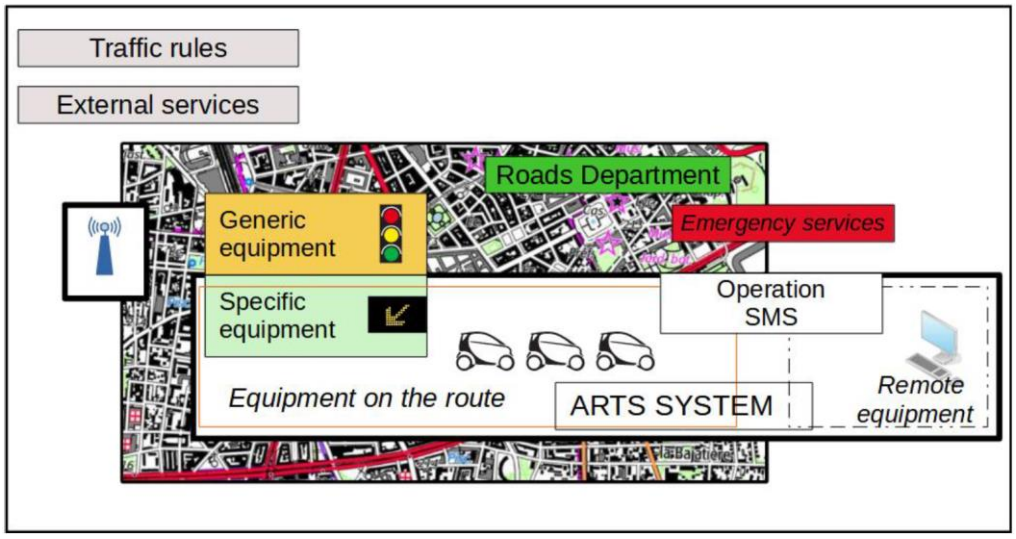


Figure 1: Organic breakdown of an ARTS

1.2 Regulatory context

This guide applies to transport systems covered by Article R.3152-2 of the French Transport Code. It therefore applies to automated road transport technical systems deployed on predefined routes or traffic areas, and is 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.

The ARTS decree introduces the obligation for technical automated road transport systems and automated road transport systems to be assessed at different stages of their life cycle by approved

qualified organizations (OQA). Cybersecurity is one of the technical fields for which the accreditations from these organizations are issued.

This requirement is introduced in the following terms in Articles R.3152-26 and R.3152-28 of the French Transport Code:

"Art. R.3152 -26. - The organization whose opinion is attached to the files mentioned in articles R. 3152-6 to R. 3152-8, has been approved by the authority mentioned in Article R. 3152-1. […]"

"Art. R.3152 -28. - I. - Approval is granted by the authority referred to in Article R. 3152-1, which ensures that the organization has the necessary skills to carry out its missions in the technical fields concerned.

II. - The approval is issued for one or more of the following technical areas:

1. *Operational safety of embedded systems;*
2. *Operational safety of connection or positioning equipment;*
3. ***Cybersecurity;***
4. *Safety of road infrastructure and equipment;*
5. *Safety of vehicle road behavior;*
6. *Operational safety management systems;*
7. *Overall system safety assessment. "*

Within the framework of this assessment, the tasks of the approved qualified organization for technical field 3 (Cybersecurity) are defined in the STRMTG "Implementation guide for approved qualified organizations for the safety assessment and operational safety auditing of ARTS".

The purpose of this guide is to describe the cybersecurity requirements applicable to the systems considered (see Section 1.3), referred to in the rest of this document as "applicable cybersecurity requirements", as well as the conditions for demonstrating compliance with these requirements.

It also provides a number of methodological principles to help meet certain requirements.

This document does not claim to be exhaustive:

- Some aspects 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 responsible entity (see Section 1.3) to supplement the various aspects of this guide as necessary in order to cover the specificities of the system under consideration (see Section 1.3).

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 under consideration (see section 1.3).

1.3 System under consideration and responsible entity

The applicable cybersecurity requirements are primarily the responsibility of the responsible entities, i.e. the legal persons responsible for deliverables or activities requiring assessment and/or auditing by an OQA.

Responsible Entity	Associated deliverable and/or activity
Technical system designer	DCST
Transport authority	DPS, DS
Operator	Implementation of the SMS and intervention and safety plan, accident analysis, annual report

Table 1: Responsible entities and associated deliverables and/or activities

The applicable cybersecurity requirements apply to the system under consideration.

In this document, the term “system under consideration” is used generically. It can therefore refer to a complete automated road transport system, a technical system, a subsystem, a component or equipment.

Each responsible entity is responsible for ensuring compliance with applicable cybersecurity requirements for the systems under its responsibility.

Responsible Entity	System under consideration/
Technical system designer	Technical system
Transport authority	ARTS
Operator	ARTS

Table 2: System under consideration by responsible entity

Each responsible entity must ensure that the organizations and/or individuals responsible for cybersecurity activities are appropriately qualified.

This reference guide of applicable cybersecurity requirements can also be used by any stakeholder who wishes to do so, for example for the supply of equipment or subsystems that can be integrated into an ARTS. In this case, the stakeholder must provide a deliverable containing a demonstration of compliance with applicable cybersecurity requirements.

In exercising its responsibility, a responsible entity may choose to impose all or part of these requirements on another stakeholder (supplier, subcontractor, etc.) if it deems it necessary, with the exception of the vehicle manufacturer who is subject to specific requirements as part of the approval process. In this case, the responsible entity shall require a deliverable containing a demonstration of the relevant stakeholder’s compliance with applicable cybersecurity requirements.

In both of the above cases:

- The responsible entity remains responsible for compliance with these requirements,
- The system under consideration must be defined,
- The term “responsible entity” in these requirements should be understood to mean “stakeholder”.

The applicable cybersecurity requirements cover the entire life cycle of the system under consideration. An explicit cybersecurity requirement is identified by [EX-NN] where NN is a number (see Annex A).

1.4 Coordination with the safety demonstration

As stated in the introduction, demonstrating compliance with applicable cybersecurity requirements prior to commissioning an ARTS is an integral part of the safety demonstration.

The safety demonstration is introduced in the following terms in Article R.3152-5 of the French Transport Code:

“Art. R. 3152-5. - Safety shall be demonstrated prior to the automated road transport system being put into service, by verifying that, within its intended operational domain, the system’s responses to all the risks associated with the operation of the system and to reasonably foreseeable and identifiable traffic risks meet the conditions set out in Articles R. 3152-2 to R. 3152-4.

This demonstration is conducted on the basis of the files referred to in Articles R. 3152-6 to R. 3152-8, together with the opinions of the approved qualified organizations referred to in Articles R. 3152-25 and R. 3152-26. […]”.

As such:

- The applicable cybersecurity requirements are intended to ensure that any automated road transportation system or automated road transportation technical system is designed to avoid accidents that may result from reasonably foreseeable cybersecurity situations within its operational domain or technical design domain (Article R3152-2. II. 1°).
- The field, scope and limits of application of the applicable cybersecurity requirements are those of the safety demonstration (Article R3152-2 II, III and IV).
- Demonstration of compliance with applicable cybersecurity requirements prior to the commissioning of an ARTS must be included in the regulatory files subject to an OQA opinion: DCST, DPS and DS (Articles R3152-25 and R3152-26). Since the demonstration of compliance with applicable cybersecurity requirements is not explicitly formalized in the contents of the regulatory files (DCST, DPS and DS in Articles R. 3152-6 to R. 3152-8, respectively) provided for by the decree, several possibilities are proposed:
    - Add one or more chapter(s) containing cybersecurity related elements;
    - Include elements related to cybersecurity in the chapters defined in the decree;
    - Create a subfile for each regulatory file containing cybersecurity related elements.

  This means that when changes are deemed substantial (see section 1.5), the relevant regulatory files must be updated by the responsible entity and reassessed by an OQA.

The scope of the demonstration of compliance with the applicable cybersecurity requirements must include all of the elements that contribute to the safety of the ARTS from among the constituent or interfacing elements included in Section 1.1.

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 responsible entity. 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.

Evidence of compliance with applicable cybersecurity requirements must be formalized and documented in the file(s) or document(s) under the responsibility of the responsible entity:

Responsible Entity	Files or documents containing evidence and their documentation
Technical system designer	DCST
Transport authority	DPS, DS
Operator	SMS, Intervention and Safety Plan

Table 3: Files or documents containing evidence and their documentation

Therefore, studies concerning the operational safety of the system under consideration must be taken into account for the implementation of the applicable cybersecurity requirements.

As such:

- If available and relevant to cybersecurity, the models of the system (for example the different types of architecture: operational, technical, functional, organic, etc.) must be taken into account.
- The dysfunctions identified during these studies, when they may result from a cyber attack, must be taken into account in the cyber risk analyses.

1.5 Operations concerned

Applicable cybersecurity requirements must be implemented for:

- Any new automated road transport technical system
- Any new automated road transport system
- Any modification, even if not substantial, of an existing automated road transport technical system
- Any modification, even if not substantial, of an existing automated road transport system
- The operation, maintenance and decommissioning of an existing, new or modified automated road transport system.

“Substantial modification” is defined in the following terms in Article R.3151-1 of the French Transport Code: “18. Substantial modification: any change to an existing automated road transport system or part of a system, where the change alters the safety assessment. ”

The applicable cybersecurity requirements in the operational phase may or may not require substantial modifications to the system under consideration. Each modification of the system under consideration must first be analyzed for its impact on the safety assessment.

However, there are two cases that need to be addressed specifically:

- Cybersecurity maintenance (see Section 5.5): installing updates, applying patches, responding to incidents, etc. In this case, the modification is not considered substantial if its impacts only concern cybersecurity. However, if the modification impacts other aspects of the safety demonstration, it should be considered substantial.
- Reassessment of risks in the operating phase, following a change in the environment of the system under consideration, revealing one or more unacceptable risks. In this case, the resulting modification of the system under consideration changes the safety assessment formalized in the regulatory files subject to an opinion of the OQA. It must therefore be considered substantial.

1.6 Cybersecurity scope

Article R.3152-2 of the French Transport Code defines 3 major “populations”:

- Users of the transportation system;

- Operating personnel;
- Third parties,

for whose safety the system should be protected in the context of any new system and any modification of an existing system.

The requirements in this guide are intended to ensure the safety of occupants and third parties during the operation of the system, including operating personnel when they are passengers of the system in the same capacity as users of the transport system or when they are present on the route as third parties.

2 Modeling the system under consideration and assessment of cybersecurity risks

This section contains the elements (formal descriptions, methods, examples) for performing some of the cybersecurity activities required in Sections 4 and 5 of this document. It is supplemented in the annex by generic models and the results of work already done in the field of ARTS (taxonomies, knowledge bases, examples).

2.1 Modeling the ecosystem of the system under consideration

An increasing number of cyber attacks exploit the most vulnerable links in an ecosystem to achieve their objective (e.g.: compromising the availability of a service via a cyber attack on a support service provider; targeting the supply chain to introduce hidden functions in developments, etc.).

The ecosystem includes all the internal or external stakeholders that gravitate around the system under consideration and contribute to the achievement of its missions, including:

- Stakeholders external to the responsible entity:
    - Partners and co-contractors
    - Service providers and suppliers
    - Approved qualified organizations
    - Customers and users
    - Public or private third party services
    - Etc.
- Stakeholders external to the responsible entity:
    - Technical-related departments (e.g.: support services provided by an IT department)
    - Business-related departments (e.g.: ticketing services)
    - Etc.

Within the specific scope of ARTS, the ecosystem can be structured according to several complementary approaches:

- An approach by types of responsible entities:
    - The technical system designer
    - The transport authority
    - The service operator
- An approach by type of subsystems and components that contribute to the services provided by the system under consideration, distinguishing:
    - The automated vehicle ecosystem, including all subsystems and components integrated into the automated vehicles (navigation system, V2X system, etc.)
    - The technical installations ecosystem, including equipment installed within the infrastructure
    - The service ecosystem, including nominal services managed by the transport authority or external services (public or private services)
    - The ecosystem associated with the routes/areas, including the specificities of the routes and areas, the infrastructure and their managing entities, third parties (people or vehicles) and occupants
- An approach by life cycle contribution of a subsystem or component, whatever its type:
    - Designer
    - Manufacturer
    - Operator
    - Maintenance operator
    - Etc.

Each stakeholder of the ecosystem is in contact with the system under consideration via a tangible interface (technical interface, physical interface, etc.) and/or intangible interface (contract, service delegation, etc.) that must be specified when the ecosystem is modeled.

An example of an ecosystem model for an ARTS is provided in Annex B of this document.

2.2 Modeling the system under consideration

2.2.1 Functional modeling of the system under consideration

Functional modeling will structure the cybersecurity risk analysis and should guide the development of the technical model detailed in Section 2.2.2. In this sense, it must be consistent with the scope of this document, and in particular with the issues specific to the safety of occupants and third parties.

The system under consideration must be modeled according to a functional approach (complementary to the technical approach detailed in section 2.2.2) which specifies the tasks of the system under consideration. A standard functional model for an ARTS is given in Annex C of this document, to be adapted according to the specificities of the system.

Functional modeling of the system under consideration must take into account the interfaces of the system and the limits of organizational responsibility, in relation to the ecosystem. In particular, a cyber attack in one system can spread through its interfaces and have impacts that can only be controlled by another stakeholder in the ecosystem.

The functional modeling of the system under consideration can be facilitated by a hierarchical approach to further refine its tasks; the level of detail expected should be that which best characterizes the system's issues during the risk assessment (in the hazardous event analysis phase, see Section 2.3 and Annex D). Successive refinements should produce the technical model detailed in Section 2.2.2 to ensure the continuity of the development process.

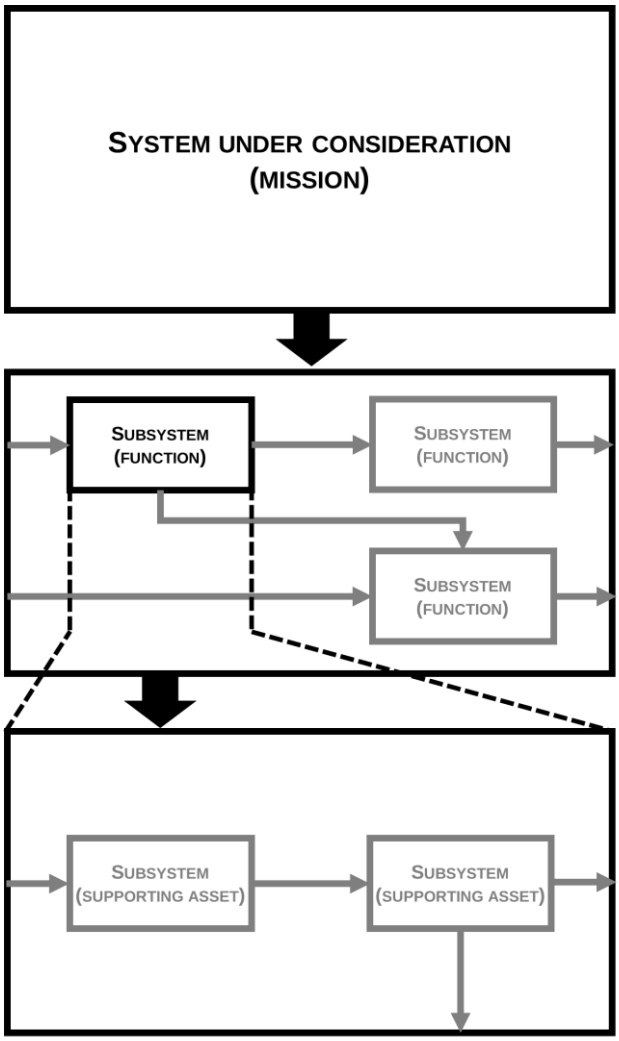


Figure 2: Hierarchical approach to functional modeling

Functional modeling of the system may be inspired by models produced in the context of operational safety analyses, provided that the relevance to cybersecurity is justified.

2.2.2 Technical modeling of the system under consideration

The system under consideration must be modeled according to a technical approach driven by the functional approach detailed in Section 2.2.1, which aims to specify the supporting assets of the system under consideration, among all its subsystems and components.

The supporting assets of the system under consideration may be characterized according to type for easier handling:

- Geographic assets:
  - Premises (building, facility, etc.) and areas (restricted areas, etc.)
  - Essential building services (energy, etc.) and general resources
- Hardware assets
  - Hardware platforms (hardware servers, equipment, etc.)
  - Network and telecom equipment (routers, switches, Wi-Fi access points, etc.)
  - Connection infrastructure (fiber-optic cables, copper cabling and connections, etc.)
  - Media (storage media, etc.)

- Cyber assets:
  - Complex digital systems (embedded systems, automatons, etc.)
  - Unitary digital systems (operating system, middleware, application, etc.)
  - Data flows (wireless flows, flows linked to the connection infrastructure)
  - User environments (workstations, human-system interfaces, embedded and remote systems, communication tools, etc.)
- Organizational assets:
  - Internal or external entity (legal entity, directorate, department, subsidiary, etc.)
  - Natural persons (users by function, users, etc.)

Depending on the project phase, the technical modeling of the system under consideration can be part of a (high level) preliminary architecture, a detailed architecture specification, or a technical architecture file used in production.

This document contains annexes with reusable standard models to facilitate the technical modeling of the system and the resulting risk assessment:

- Annex D: a projection of technical modeling on a stratified model of the space, highlighting the specificities of the supporting assets of the system under consideration
- Annex G: a link between the functional modeling and the technical modeling of the system under consideration, by associating the supporting assets to the tasks of the system

2.3 Cybersecurity risk assessment

2.3.1 General approach

A cybersecurity risk is the combination of a threat scenario (the cause) and an impact scenario (the effect). The list of cybersecurity risks that apply to the system under consideration is the outcome of all the combinations of the threat scenarios and impact scenarios for the system.

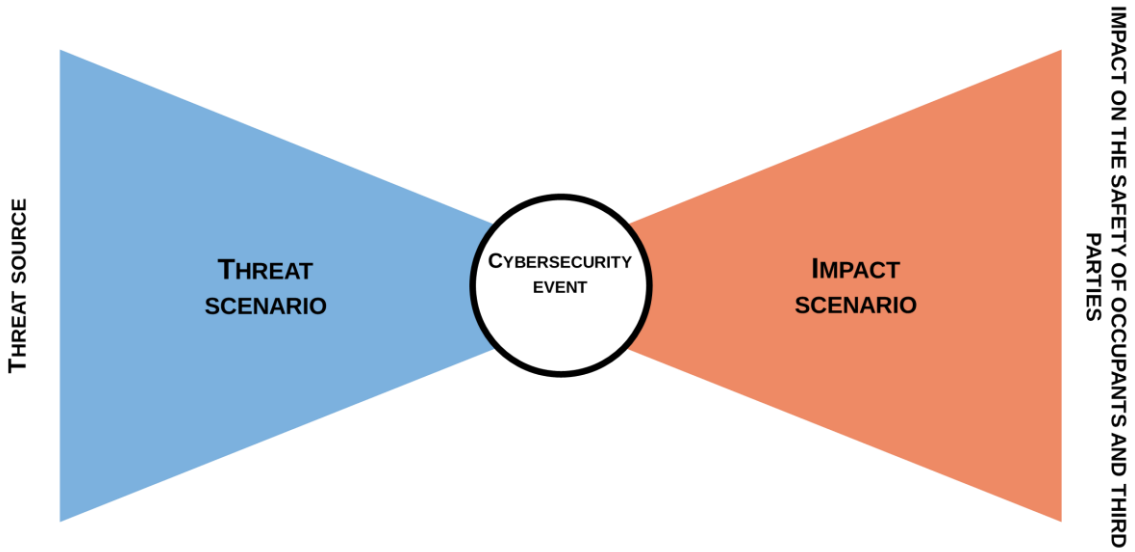


Figure 3: Construct of a cybersecurity risk

The system under consideration must therefore undergo a cybersecurity risk assessment based on the following methodological principles:

- Identification of cybersecurity risks
  - Identification of impact scenarios
  - Identification of threat scenarios
  - Comparison of threat and impact scenarios
- Cybersecurity risk assessment:
  - Evaluation of the severity of the impact scenarios
  - Evaluation of the likelihood of threat scenarios
  - Evaluation of cybersecurity risks

2.3.2 Identification and evaluation of impact scenarios

The assessment of cybersecurity risks in terms of impact scenarios must identify and evaluate all situations that impact the service or operation and which impact the safety of occupants and third parties, including (cases specified in Article R.3152-2 of the Transport Code):

- Accidents that may result from reasonably foreseeable situations in the operational domain or technical design domain (see Annex E);
- Cases of failure and cases where the vehicle leaves the operational domain or technical design domain.

Cybersecurity events are the inputs for the impact scenario (see Figure 4). They correspond to all the cases where the availability or integrity of a function of the system under consideration is affected (see Annex C). The purpose of the impact scenarios is to describe the scenarios that initiate from a cybersecurity event (see Figure 4), and result in a system level accident.

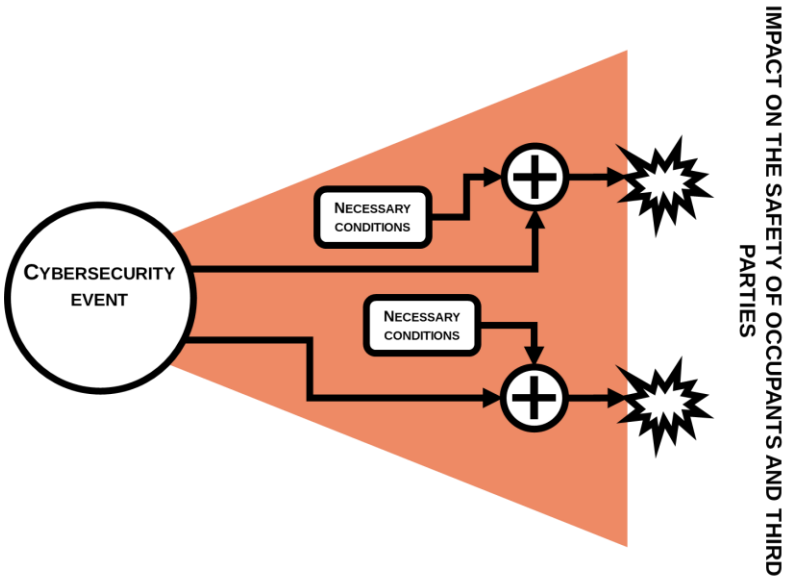


Figure 4: Typical impact scenario

A high-level view of cybersecurity events, based on threat scenarios applied to the standard functional modeling of an ARTS, is provided in Appendix G of this document.

The impact scenarios should be determined:

- By comparing each cybersecurity event with situations that impact service or operations and which impact the safety of occupants and third parties, in order to determine the conditions necessary for these situations to occur

- By comparing the necessary conditions identified above with the technical design domain and/or operational domain for the system under consideration

Each identified impact scenario must be evaluated for its severity, expressed in terms of the level of impact of the impact scenario on the safety of occupants and third parties. The 4-level scale (G0 to G3) to be used for this purpose is provided in Annex H.

2.3.3 Identification and evaluation of impact scenarios

Threat scenarios are formed according to the following “grammar” (see Figure 5):

A [threat source] exploits one or more [vulnerability(ies)] of one or more [supporting asset(s)] of the system under consideration to carry out one or more [attack(s)] inducing one or more [cybersecurity event(s)]

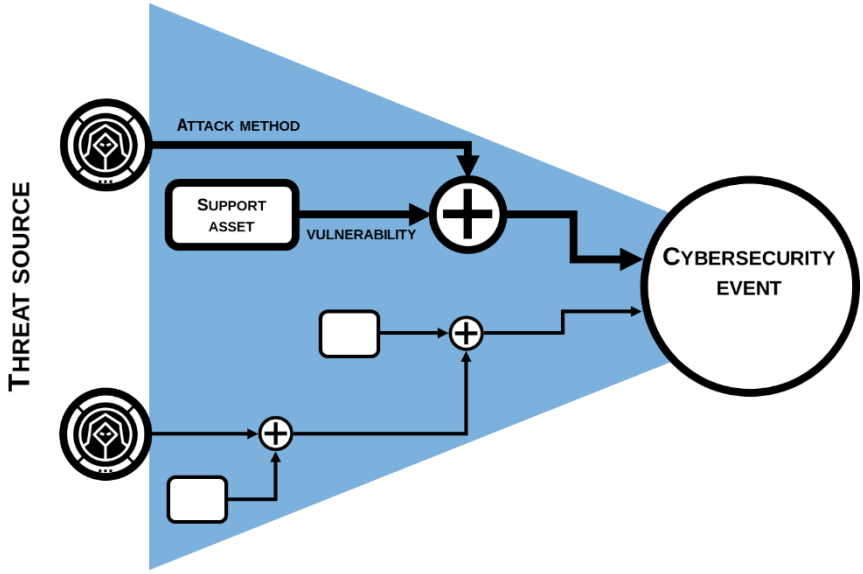


Figure 5: Typical threat scenario

Threat scenarios should be identified by analyzing each of the components:

- The [threat sources] applicable to the system under consideration

  Detailed characterization of threat sources/actors requires precise information on the state of the threat. It depends on many factors: sector, location, context of the activity (geopolitical, economic, etc.).

  Threat sources are primarily characterized by their nature (e.g., criminal or cybercriminal groups, state-sponsored attacker groups, activist or hacktivist groups, isolated individuals with various motivations, etc.).

  Identifying threat sources makes it easier to characterize them, through their attack potential, which is based on the following two key characteristics:

  - The motivation of the threat source: these are very diverse in nature (political, economic, etc.) and are not always easy to express.

    If a motivation cannot be directly determined, it can be materialized through the threat source’s intention and expressed in the form of a desired end result (the overall outcome that the attacker wants to achieve after the attack).

Furthermore, the motivation of a threat source is directly related to the attractiveness of its target (the system under consideration).

- The capabilities of the threat source, which include available resources and expertise:

  A distinction is made between intelligence capabilities (providing information to prepare and carry out operations), offensive capabilities (executing the operations), and defensive capabilities (protecting committed resources).

  In addition, threat source capabilities are projected onto the stratified space, yielding usable resources on the physical space, cyber space, and anthropogenic space.

Elements for characterizing threat sources/actors and examples of types and metrics for motivation and capability are provided in Annex F.

- The [vulnerabilities] of the [supporting assets] of the system under consideration

  Vulnerabilities are primarily properties of supporting assets that can be exploited by a threat source to carry out an attack. In this sense, this exploitability is directly related to the capabilities of the threat source, on several levels:

  - On a topological level: some vulnerabilities can only be exploited if they are “visible” to the threat source (e.g., physical proximity)
  - On a time-related level: some vulnerabilities can only be exploited within a given time window
  - On a capability level: some vulnerabilities require significant capabilities (resources, expertise, etc.)

  The vulnerabilities of the supporting assets of the system under consideration are very diverse and depend on the types of supporting asset. Based on the technical modeling of the system under consideration (see Section 2.2.2), each supporting asset must be identified and its vulnerabilities characterized.

  A lack of cybersecurity measures (e.g., lack of clearance and access rules, lack of a cybersecurity patch management process, etc.) may constitute a vulnerability of the system under consideration.

- Applicable [attack methods]

  Attack methods are the methods used by the threat source to exploit vulnerabilities. They are related to the capabilities of the threat source and exploitable vulnerabilities.

- [Cybersecurity events]

  A threat scenario induces a cybersecurity event:

  - Attack on the integrity of a function or sub-function of the system under consideration
  - Attack on the availability of a function or sub-function of the system under consideration

  The cybersecurity event is not the final effect sought by the attacker, nor is it the final impact of the threat scenario; it reflects a hazardous situation that only leads to an event under certain conditions.

A high-level view of threat scenarios that apply to an ARTS based on the standard functional modeling of an ARTS, is provided in Annex G of this document. The content of the annex is a high-level inventory of threat scenarios that should be considered.

Each identified threat scenario must be evaluated in terms of the likelihood of the threat scenario. This involves a composite value (see Figure 6) that incorporates:

- The attack potential of the threat source, resulting from the motivation of the threat source and the level of exploitability of the vulnerabilities (depending on topological, time-related, and capability aspects) in relation to the capabilities of the threat source.
- The level of difficulty in carrying out the attack due to the cybersecurity measures already implemented within the system under consideration (and, in turn, the vulnerabilities of the system)

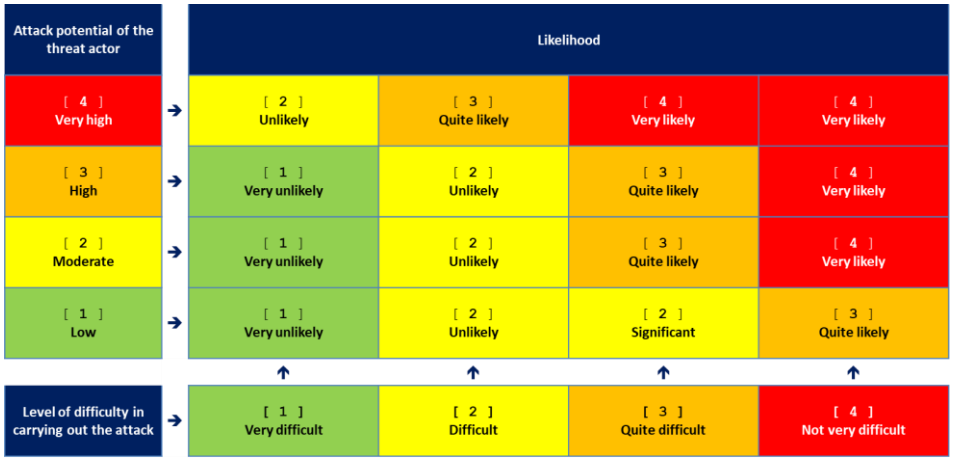


Figure 6: Levels of likelihood

2.3.4 Identification and evaluation of cybersecurity risks

Cybersecurity risks should be identified by systematically comparing the threat scenarios and impact scenarios for the system under consideration. By doing so, a list of relevant risks to be taken into account for the system is identified.

Cybersecurity risks must be evaluated on the basis of a risk matrix taking into account the levels of likelihood of the threat scenario and the severity of the impact scenario specific to the risk under consideration. The risk matrix should be adapted and defined according to the project and system under consideration.

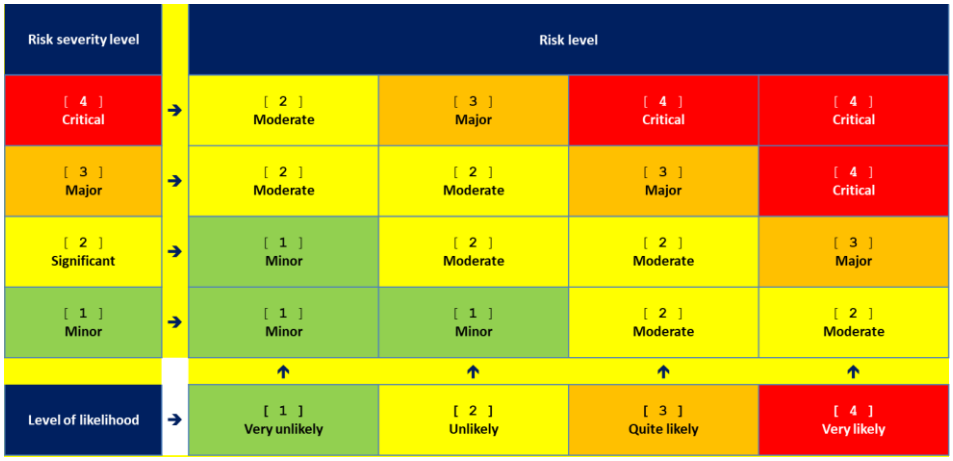


Figure 7: Standard risk matrix and expression of risk levels

The result of the identification and evaluation of cybersecurity risks should take the form of a prioritized list of risks according to level of risk so that cybersecurity management measures can be taken.

2.4 Cybersecurity risk treatment

The purpose of the cybersecurity risk treatment plan is to reduce cybersecurity risks to an acceptable level, based on the cybersecurity risk acceptance criteria and the previously established risk level.

Cybersecurity risk treatment therefore requires that the following be specified beforehand:

- Cybersecurity risk acceptance principles, among the following principles:
    - Compliance with industry practices or best practices (e.g.: Interministerial Order No. 901 on the protection of sensitive information systems)
    - Comparison with a reference system
    - The use of an explicit risk assessment based on a severity/likelihood matrix
- Cybersecurity risk acceptance criteria derived from risk acceptance principles

The options for managing risks determined to be unacceptable are:

- Denial of cybersecurity risks: changing the context or system so that the system is no longer exposed to them
- Reducing cybersecurity risks: applying cybersecurity measures to the system under consideration or exporting functional cybersecurity requirements to another stakeholder to reduce impact and/or likelihood

Management measures can be implemented by taking into account the following:

- Cybersecurity risk components (threat source, threat scenario, supporting asset, cybersecurity event, etc.) that help determine whether the measures are feasible
- The invariants of cybersecurity risk assessment: constraints, assumptions and identified elements
- Risk management criteria that are defined elsewhere or inferred (e.g.: difficult to act on the likelihood of a very unlikely risk)

Management options for each cybersecurity risk must be substantiated and documented. Several options can be chosen to manage the same cybersecurity risk.

If the chosen option is to mitigate or maintain a risk, one or more corresponding cybersecurity objectives must be specified, taking into account the assumptions. The security objectives consist of comprehensive, open specifications (that do not predetermine the solutions to be adopted) and adapted to the system under consideration:

- In the case of risk mitigation, cybersecurity objectives are aimed at reducing the risk to an acceptable level.
- In the case of risk maintenance, cybersecurity objectives are aimed at keeping the risk at an acceptable level.

3 Cybersecurity assurance

3.1 Introduction

Cybersecurity Assurance Levels (CALs) are a classification system that describes the requirements that must be met to ensure that cybersecurity is addressed at each stage of the life cycle of the system under consideration, in proportion to the cybersecurity risks to the system. Once determined, a CAL specifies the rigor expected in performing the cybersecurity activities within the life cycle of the system under consideration.

3.2 Determining applicable CALs

The CAL is intended to ensure that a cybersecurity objective is achieved with the required level of trust, and therefore that the cybersecurity risk under that cybersecurity objective is at an acceptable level (see Section 2.4). Consequently, the CALs are determined, for a given system (the system under consideration or one of its subsystems), on the basis of a matrix taking into account the values of the attack potential from the threat source(s) and the severity of the impact scenario(s) within this scope.

The CAL matrix should be adapted and defined according to the project and system under consideration. Figure 8 gives an example of how to determine CALs.

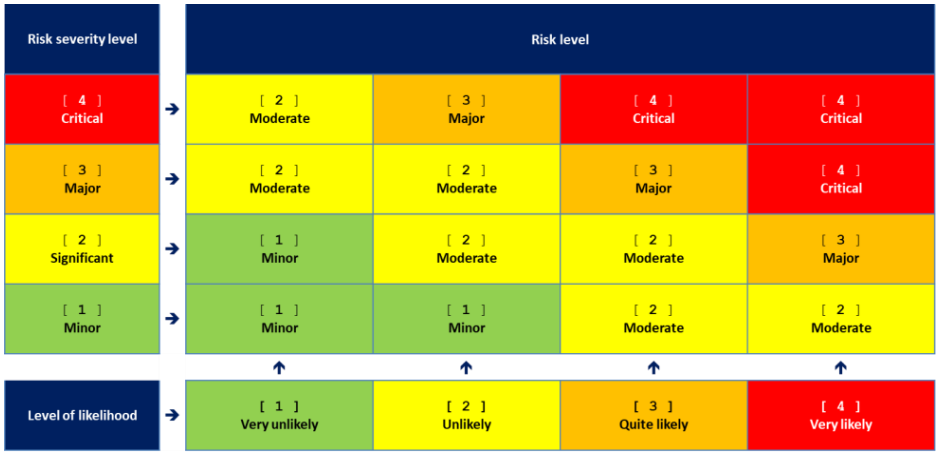


Figure 8: Example of determining CALs based on severity and attack potential

CALs are applied to the system under consideration and/or its subsystems, with a variable level of detail, derived from the assessment of cybersecurity risks.

Since CALs are linked to cybersecurity risk levels, a subsystem of the system under consideration may inherit a different CAL from another subsystem, if it is subject to its own cybersecurity risks. By default, a given system will inherit the maximum risk level from the scenarios that apply to it, and therefore the associated CAL.

In the case of a high CAL for a given system (the system under consideration or one of its subsystems), it is recommended that the scope be broken down into subsystems to separate the subsystems with the highest importance, and therefore requiring high CALs, from less critical subsystems. In particular, this breakdown inherits from:

- The functional breakdown of the system under consideration, which is a natural approach to fine-tune the system (see Section 2.2.1)
- The ability to apply one or more risk scenarios to a given system (the system under consideration or one of its subsystems)

All systems (the system under consideration or all of its subsystems) must be assigned a CAL, even when the risk is deemed acceptable as is (see Section 2.4). Consequently, this means that a CAL is applied to each system, regardless of the risk treatment option chosen.

3.3 Determining CAL criteria and metrics

For each CAL, metrics are defined to ensure that the required cybersecurity assurance level is achieved, based on the following three criteria:

- The level of rigor, which determines the manner in which the activities must be carried out, the degree of justification that must be provided, the degree of formalization of the analysis or verification methods used, as well as the traceability of the actions carried out and decisions made
- The level of detail, which determines the life cycle phases during which cybersecurity activities must be performed, and the requirements for the content and detail of the deliverables for each phase
- The level of independence, which determines the expectations in terms of role separation

Applying the CAL criteria to the various cybersecurity activities within the life cycle of the system under consideration is strongly dependent on the type of activities.

Two examples of CAL criteria for cybersecurity activities are given in the tables below for information purposes only. They should be re-adapted and re-defined according to the project and cybersecurity activity.

As an example, the independence criterion may be irrelevant to some of the cybersecurity activities within the life cycle (but naturally applies to testing and assessment activities). In particular, cross-functional and continuous cybersecurity activities (see Sections 4.1 and 4.2) require specific metrics because they are not specifically associated with a given system.

Future versions of the guide will include CAL scales specifically for ARTS cybersecurity activities.

Level	Description	Level of rigor	Level of detail	Level of independence
CAL1	Low to moderate cybersecurity assurance is required.	The assessment is based on a search for potential vulnerabilities from published vulnerabilities or known information	The assessment is based on compliance with the requirements expressed.	Not required
CAL2	Moderate cybersecurity assurance is required.	The assessment is based on a search for potential vulnerabilities using exploratory methods	The assessment is based on compliance with the requirements expressed.	The assessment is carried out someone other than the person in charge of carrying out the activity
CAL3	Moderate to high cybersecurity assurance is required	The assessment is based on a search for potential vulnerabilities using exploratory methods and on penetration testing to confirm that the vulnerabilities cannot be exploited in the operational environment	The assessment takes into consideration the functional and technical specifications of the architecture	The assessment is carried out by a person in the same organization who is not in charge of carrying out the activity
CAL4	High cybersecurity assurance is required	The assessment is based on a search for potential vulnerabilities using exploratory methods and on penetration testing to confirm that the vulnerabilities cannot be exploited in the operational environment	The assessment takes into consideration the functional and technical specifications of the architecture	The assessment is carried out by a person from another organization who is not in charge of carrying out the activity.

Table 4: Example of CAL metrics for cybersecurity assessment

Level	Description	Level of rigor	Level of detail	Level of independence
CAL1	Low to moderate cybersecurity assurance is required.	Awareness activities are conducted in accordance with the cybersecurity awareness plan	Awareness activities concern all the staff involved with the system under consideration.	N/A
CAL2	Moderate cybersecurity assurance is required.	Awareness activities are conducted in accordance with the cybersecurity awareness plan	Awareness activities concern all the staff involved with the system under consideration and are adapted to their duties.	N/A
CAL3	Moderate to high cybersecurity assurance is required	Awareness activities are conducted in accordance with the cybersecurity awareness plan	Awareness activities concern all the staff involved with the system under consideration and are adapted to their duties and cybersecurity issues specific to their duties.	N/A
CAL4	High cybersecurity assurance is required	Awareness activities are carried out in accordance with the awareness plan addressing cybersecurity issues and their effectiveness is measured with performance indicators	Awareness activities concern all the staff involved with the system under consideration and are adapted to their duties and cybersecurity issues specific to their duties.	N/A

Table 5: Example of CAL metrics for cybersecurity awareness

4 Cross-functional and continuous cybersecurity activities

This section describes the requirements for cross-functional, continuous cybersecurity activities applicable to the responsible entity that must be implemented within the scope of the system under consideration. These activities may already be implemented. Some cybersecurity activities may also be "not applicable" due to the type of system. In this case, the "not applicable" nature of the cybersecurity activity must be substantiated.

4.1 Comprehensive cybersecurity management

4.1.1 Objectives

The purpose of this theme is to ensure that cybersecurity management processes within the responsible entity function properly, in support of cybersecurity activities carried out in project mode, regardless of the life cycle phase of the system under consideration.

4.1.2 Cybersecurity activities

[EX-0.01] Define and implement a cybersecurity reference framework	
A cybersecurity framework must be developed and implemented to ensure cybersecurity governance within the responsible entity.	
Inputs	**Outputs**
	EX-1.03; EX-1.04; EX-1.05; EX-5.06; EX-5.07

The cybersecurity reference framework includes:

- Documentation relating to cybersecurity governance (cybersecurity master plan, general or specific cybersecurity policy, etc.)
- Operational documentation for cybersecurity implementation (all implementation documents: local cybersecurity policy, cybersecurity-specific process, etc.)

Operational documentation includes all of the cybersecurity framework processes, which are applicable and applied to all the different phases of the life cycle, including but not limited to:

- The cybersecurity risk management process
- The cybersecurity incident management process
- The cybersecurity crisis management process
- The vulnerability and patch management process

The senior management of the responsible entity must be involved in the adoption of this cybersecurity framework and support its implementation, by understanding the cybersecurity risks and committing to managing them.

[EX-0.02] Define and implement an organization dedicated to cybersecurity	
An organization dedicated to cybersecurity governance and implementation must be defined and implemented within the responsible entity.	
Inputs	**Outputs**
	EX-5.06; EX-5.07

The cybersecurity organization specifies:

- The organization and composition of the cybersecurity chain of command and, if applicable, of a functional cybersecurity chain of command adapted to the organization of the responsible entity
- The description of the cybersecurity-related missions of each of the stakeholders these chains of command, in the form of job descriptions or descriptions of duties and responsibilities
- The description of the cybersecurity committee (members, frequency of meetings and agenda) necessary for cybersecurity governance and implementation

The general management of the responsible entity must commit to defining this organizational structure and supporting its implementation, in particular by assigning the roles defined in the chain of command and by committing to providing the resources for people to perform their duties.

[EX-0.03] Develop a cybersecurity culture at all levels	
A cybersecurity awareness plan and a cybersecurity skills management plan must be developed and implemented to continuously develop a cybersecurity culture within the responsible entity.	
Inputs	**Outputs**
	EX-1.03; EX-5.04

The cybersecurity awareness plan concerns all the responsible entity's staff; the topics and ways to raise awareness may vary according to the jobs performed but must ensure:

- Comprehension of the cybersecurity risk
- Comprehension of their cybersecurity roles and responsibilities
- Knowledge of cybersecurity rules and best practices

The cybersecurity skills management plan covers the responsible entity's staff whose job requires cybersecurity expertise (e.g., technical administrator).

Awareness and skills management plans must take into account the specific technological, regulatory and other issues and characteristics of the ARTS for the staff concerned.

[EX-0.04] Conduct continuous monitoring and use the results	
A cybersecurity monitoring process must be developed and implemented to ensure a proactive approach to cybersecurity within the responsible entity.	
Inputs	**Outputs**
Internal sources; Open sources; Government sources and specialized organizations	*EX-1.03; EX-2.01; EX-3.01; EX-5.01; EX-5.08; EX-5.10; EX-5.11*

The monitoring process specifies the organization and information flows implemented within the responsible entity. The monitoring process should specify:

- Monitoring topics, including:
  - General cybersecurity monitoring
  - Sectoral monitoring in the transport sector
  - Specific monitoring for each type of subsystem or component
- Types of monitoring, including:
  - Legal and regulatory monitoring
  - Documentary monitoring (standards, publications, etc.)
  - Event monitoring (cybersecurity news, threat monitoring, etc.)
  - Tool monitoring
  - Vulnerabilities and patch monitoring
- Monitoring sources (ecosystem stakeholders, see Section 2.1 and Appendix B):
  - Internal sources (legal department, technical department, etc.)
  - Open sources (including social media)
  - Authorities (including ANSSI) or specialized organizations (including CERT)
  - Hardware or software solution providers / maintainers

The monitoring process also specifies the actions to be taken in response to information received from the monitoring process:

- Sorting and prioritizing information
- Information reporting or alert escalation if necessary

The monitoring process must take into account the specific technological, regulatory and other issues and characteristics of ARTS.

[EX-0.05] Define and implement a cybersecurity management system	
A cybersecurity management system must be developed and implemented to ensure continuous improvement of cybersecurity within the responsible entity.	
Inputs	**Outputs**
	EX-0.06; EX-0.07; EX-0.08; EX-1.03; EX-1.09; EX-5.01; EX-5.05; EX-5.06; EX-5.07; EX-6.01

The cybersecurity management system must comply with international or equivalent standards. It should be based on:

- A document management system

- Measurement of cybersecurity effectiveness, via:
    - Cybersecurity indicators and dashboards
    - Cybersecurity incident assessment information
    - Cybersecurity audit results
    - Information from cybersecurity monitoring
- Cybersecurity comitology ensuring continuous improvement, via:
    - Consideration of feedback from stakeholders
    - The definition of corrective action plans
    - The definition of preventive action plans
    - The definition of improvement action plans

4.2 Project cybersecurity management

4.2.1 Objectives

The purpose of this theme is to ensure that cybersecurity is properly integrated into project management processes within the responsible entity, in support of cybersecurity activities carried out in project mode, regardless of the life cycle phase of the system under consideration.

4.2.2 Cybersecurity activities

[EX-0.06] Establish the cybersecurity quality plan for the project	
A cybersecurity quality plan must be developed and implemented to ensure that the cybersecurity activities to be performed for the project are assigned and integrated into the project life cycle.	
Inputs	**Outputs**
EX-0.05	*EX-0.07; EX-1.04; EX-2.05; EX-3.05; EX-4.02; EX-5.01*

The cybersecurity quality plan is used to manage the implementation of the requirements of this reference guide. In particular, it specifies:

- The documents or inputs required to perform each cybersecurity activity
- The deliverables or outputs expected from each cybersecurity activity
- Inspection plans carried out at the end of each cybersecurity activity
- Evidence of compliance with the requirements of this reference guide
- The resources required to perform each cybersecurity activity
- The planning of each cybersecurity activity
- The roles and responsibilities associated with each cybersecurity activity for the project

The cybersecurity quality plan specifies the project comitology, including the comitology required to validate cybersecurity objectives and accept residual risks, at each phase of the life cycle.

The cybersecurity quality plan is developed at the beginning of the project and updated at each phase of the project life cycle by the responsible entity in charge of the cybersecurity activities of the phase concerned.

[EX-0.07] Manage project documentation from a cyber security perspective	
The project documentation must be covered by necessary and sufficient protection measures, in line with the sensitivity of the information in the documents, for all phases of the document life cycle.	
Inputs	**Outputs**
EX-0.05; EX-0.06	*EX-5.01; EX-6.01*

Project-specific documentation and documentation useful to the project owned by third parties must be covered by necessary protection measures, in line with the sensitivity of the information in the documents:

- Information classification and document marking measures
- Protection measures for stored or archived data
- Data protection measures for data transfer

Project-specific documentation and third-party documentation relevant to the project must be readily available to any project stakeholder with a need to know, based on information exchange processes and means defined in the cybersecurity quality plan.

[EX-0.08] Establish a cybersecurity risk management process for the project	
A cybersecurity risk management process must be developed and implemented to ensure that cybersecurity risks are controlled throughout the project life cycle.	
Inputs	**Outputs**
EX-0.05	*EX-1.05; EX-2.01; EX-3.01; EX-5.01; EX-5.11*

The risk management process should specify the following, in accordance with the principles described in Section 2.3 of this document:

- That the cybersecurity risk assessment is carried out at the specification/design phase of the project and updated at each phase of the project
- That the risk assessment is documented and that all decisions are formally recorded
- Criteria for re-evaluating risk assessment
- That the cybersecurity risk assessment is reviewed as soon as the results of monitoring indicate a change in the threat environment or an emerging trend
- That the cybersecurity risk assessment is reviewed as soon as a new vulnerability is identified that can affect a system in operation
- That the result of the cybersecurity risk assessment must be submitted to the person in charge of risk acceptance, as part of the cybersecurity governance implemented under the cybersecurity quality plan, for acceptance of the risk treatment plan and residual risks
- That all changes resulting from risk treatment are documented and recorded.

[EX-0.09] Establish a cybersecurity assurance level assignment process for the project	
A process for assigning cybersecurity assurance levels must be developed and implemented to ensure that cybersecurity assurance levels are defined and assigned to the system under consideration and/or its subsystems.	
Inputs	**Outputs**
EX-0.05	*EX-1.05; EX-2.01; EX-3.01; EX-5.01; EX-5.11*

Cybersecurity assurance levels are assigned following each iteration of the risk assessment for the system under consideration, according to the principles described in Section 3 of this document, including:

- Determining CAL criteria and metrics
- Determining applicable CALs
- Assignment of CALs in relation to cybersecurity risk

5 Life cycle of the system under consideration

This section describes the requirements for cybersecurity activities integrated into the life cycle of the system under consideration. Each cybersecurity activity applies to the responsible entity. Some cybersecurity activities may also be “not applicable” due to the type of system. In this case, the “not applicable” nature of the cybersecurity activity must be substantiated and recorded.

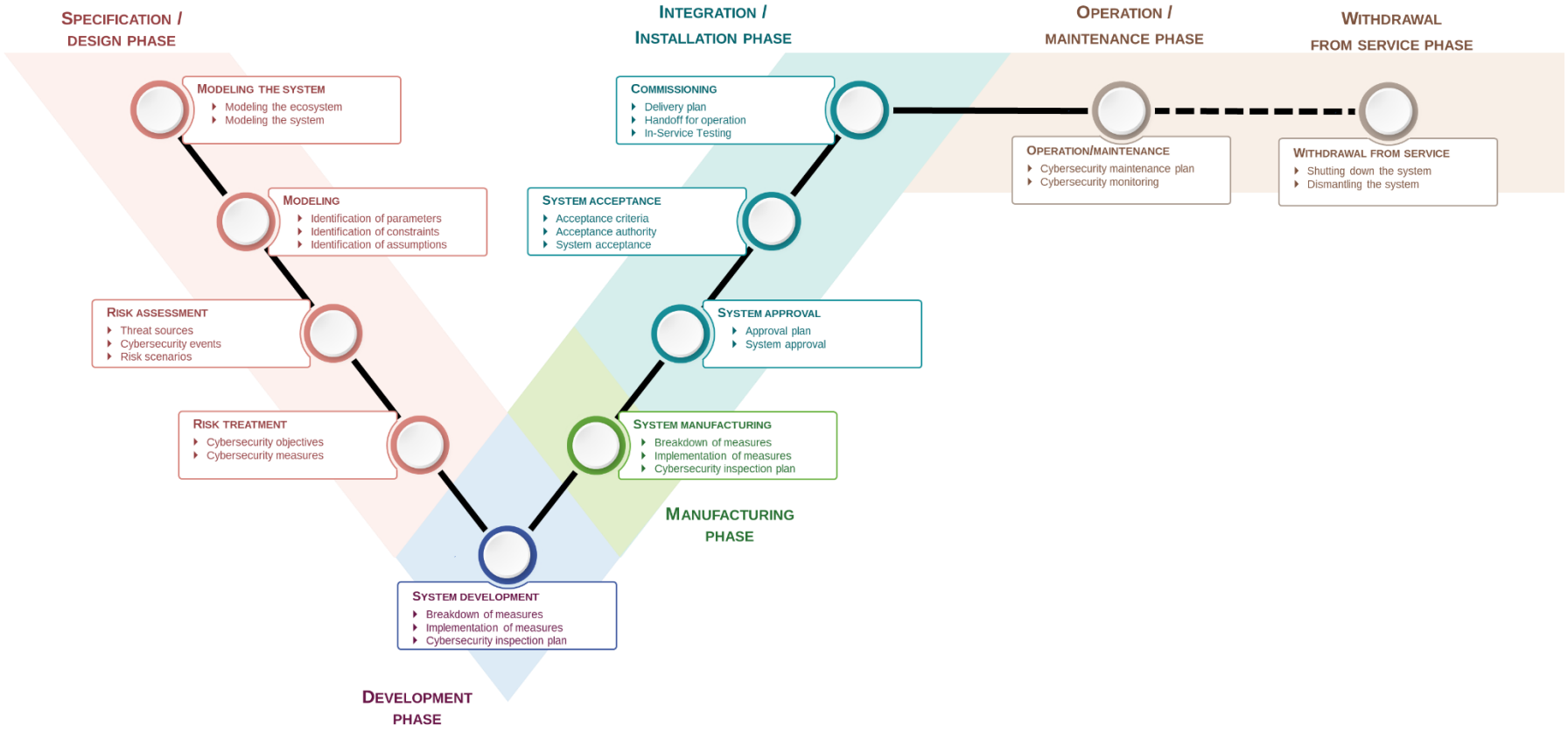


Figure 9: Cybersecurity activities integrated into the life cycle of the system under consideration

5.1 Specification / design phase

5.1.1 Objectives

The specification/design phase of the system under consideration integrates the system modeling and initial cybersecurity risk assessment activities. At the end of this phase, the cybersecurity objectives and the cybersecurity measures applicable to the system under consideration are specified.

The cybersecurity objective of this phase of the life cycle is to specify the cybersecurity measures for the system under consideration, based on a risk assessment. These specifications will be translated into intrinsic or exported properties for the system under consideration in the later phases. They can be refined or re-evaluated in subsequent phases.

5.1.2 Cybersecurity activities

[EX-1.01] Modeling the ecosystem of the system under consideration	
All the stakeholders involved in the system under consideration must be identified and characterized, as they constitute the ecosystem of the system.	
Inputs	**Outputs**
	EX-1.05; EX-2.01; EX-3.01; EX-4.01; EX-5.11

The ecosystem of the system under consideration should be modeled according to the principles described in Section 2.1 of this document. The following should be analyzed:

- The relationships between the different stakeholders of the system under consideration
- The interfaces between the stakeholders and the system
- The stakeholders' cybersecurity issues and concerns
- The cybersecurity roles and responsibilities of stakeholders
- The cybersecurity policies implemented by the stakeholders regarding the system under consideration

[EX-1.02] Modeling the system under consideration	
All the subsystems and components of the system under consideration must be identified and characterized, as they constitute the modeling of the system.	
Inputs	**Outputs**
	EX-1.04; EX-1.05; EX-2.01; EX-3.01; EX-4.01; EX-5.11

The system under consideration should be modeled according to the principles described in Section 2.2 of this document. The following should be characterized:

- The tasks of the system under consideration, which include the safety of the occupants and third parties

- The content of the system under consideration and any exceptions (e.g. a subsystem subject to a specific regulation)
- The limits of the system and its external interfaces, in relation with the ecosystem
- Supporting assets, including:
    - Sub-systems and components of the system under consideration
    - Users and user communities of the system
    - Internal interfaces of the system (interfaces between one supporting asset and another)
    - Information about the nature of these supporting assets (physical asset, software asset, etc.)
    - Information on the location of these assets
    - Data that is sensitive from a security perspective

At this stage of modeling, relevant information about the system's operational environment (including shared installations - such as traffic lights - or even shared service - 5G communication, GPS location, etc.) with respect to cybersecurity should be described, and the relationships between the elements should be specified

[EX-1.03] Identify the elements to be taken into account for the system under consideration	
All factors affecting the risk management of the system under consideration must be identified and characterized.	
Inputs	**Outputs**
EX-0.01; EX-0.04; EX-0.05	*EX-1.04; EX-1.05*

The elements to be taken into account for the system under consideration and for all the system's subsystems and components, include:

- The responsible entity's internal cybersecurity references to consider:
    - Cybersecurity or similar policy
    - Implementation documents (processes, procedures and operating procedures, etc.)
- External cybersecurity references to be implemented:
    - Legal and regulatory references
    - Standards
    - EU references
    - Sector references
- Feedback/field experience on ARTS or similar systems:
    - Cybersecurity objectives
    - Input elements
    - Previously obtained cybersecurity assurance levels
    - Previously obtained indicators and dashboards
    - Threats and threat sources considered
- Existing information about the system under consideration:
    - Cybersecurity activities already carried out
    - The results of cybersecurity audits already carried out as part of the project
    - Qualifications already obtained (certification, approval, etc.) for a subsystem or component

[EX-1.04] Identify the constraints and assumptions of the system under consideration	
All constraints and assumptions affecting the risk management of the system under consideration must be identified and characterized.	
Inputs	**Outputs**
EX-0.01; EX-0.06; EX-1.02; EX-1.03	*EX-1.05; EX-1.06; EX-1.08; EX-2.02; EX-2.03; EX-3.02; EX-3.03; EX-4.01*

The constraints to be taken into account for the system under consideration and for all the system's subsystems and components, include:

- Constraints on the responsible entity
- Constraints that are specific to the system under consideration

The assumptions to be taken into account for the system under consideration and for all the system's subsystems and components, are imposed by the responsible entity of the study. Assumptions can also be an a priori accepted risk in a given environment. If assumptions concern another responsible entity or stakeholder, they must be formalized and communicated.

Some constraints and assumptions may be inherited from the operational design domain if the system under consideration is the automated vehicle, from the technical design domain if the system under consideration is the technical system, or from the operational domain if the system under consideration is the ARTS.

[EX-1.05] Perform a risk assessment of the system under consideration	
A cybersecurity risk analysis of the system must be performed and documented.	
Inputs	**Outputs**
Annex E; Annex G; Figure 7; EX-0.01; EX-0.08; EX-1.01; EX-1.02; EX-1.03; EX-1.04	*EX-1.06; EX-1.07; EX-2.01*

A risk assessment of the system under consideration must be performed based on the principles described in Section 2.3 of this document. This risk assessment must be documented to provide clear and detailed evidence of the methodologies, data, judgments and interpretations used to perform it.

In the specification/design phase, the system under consideration can only be modeled at a high level of abstraction. As a result, all the vulnerabilities that can be exploited by threat sources cannot be fully identified. The risk assessment will highlight high-level threat scenarios that will be refined in subsequent phases of the system's life cycle.

If a risk assessment performed elsewhere for a subsystem or a component of the system under consideration is inherited, the following must be verified:

- That the context of the system under consideration is compatible with the analysis
- That the subject of the analysis is adapted to the specific context of the intended application

[EX-1.06] Develop a cybersecurity risk treatment plan	
A cybersecurity risk treatment plan for the system under consideration must be developed in order to reduce the risks to an acceptable level according to formally defined criteria.	
Inputs	**Outputs**
EX-1.04; EX-1.05	*EX-1.07*

A risk assessment must be performed for each identified risk of the system under consideration, based on the principles described in Section 2.4 of this document.

The risk treatment plan must formalize the cybersecurity risk acceptance principles and cybersecurity risk acceptance criteria derived from these principles.

[EX-1.07] Define the cybersecurity objectives for the system under consideration	
Cybersecurity objectives to reduce risks to an acceptable level must be defined, in relation to the risk assessment.	
Inputs	**Outputs**
EX-1.05; EX-1.06	*EX-1.08; EX-2.05; EX-3.05; EX-4.02; EX-5.05*

If cybersecurity risk treatment measures consist in reducing the risk in question, one or more corresponding cybersecurity objectives must be specified.

Cybersecurity objectives may concern:

- The components of the system under consideration and its ecosystem and/or the components of the risk (threat source/actor, events, etc.)
- All or part of the life cycle phases, including phases after the phase in which they are specified
- All or part of the implementation aspects of the supporting assets (technical design, technical architecture, physical or geographical location, type of users, etc.)

[EX-1.08] Translate cybersecurity objectives into functional cybersecurity requirements	
Cybersecurity objectives must be translated into functional cybersecurity requirements.	
Inputs	**Outputs**
EX-1.04; EX-1.07	*EX-1.09*

The cybersecurity objectives translated into functional cybersecurity requirements constitute the cybersecurity concept which must:

- Match the cybersecurity objectives
- Fully take into account cybersecurity objectives

- Match the assumptions and constraints of the system under consideration

The functional cybersecurity requirements may need to be taken into account by the entity responsible for the system under consideration or be exported to the various actors of the ecosystem.

[EX-1.09] Specify the cybersecurity measures for the system under consideration	
Cybersecurity measures to reduce risks to an acceptable level, in relation to cybersecurity objectives, must be specified.	
Inputs	**Outputs**
EX-0.05; EX-1.08	*EX-2.03*

Cybersecurity measures can be incorporated into the specifications of the system under consideration or be detailed in separate specifications.

The cybersecurity measures can be applied by the entity responsible for the system under consideration or describe measures exported to various actors of the ecosystem.

Like the cybersecurity objectives, cybersecurity measures can concern:

- The components of the system under consideration, its ecosystem, the risk
- All or part of the life cycle phases
- All or part of the implementation aspects of the supporting assets

Cybersecurity measures can be technical, functional, organizational or contextual in nature; they can address different aspects of the system under consideration:

- Cybersecurity aspects of system functions
- Cybersecurity aspects of internal and external interfaces
- Cybersecurity aspects of the architecture
- Cybersecurity performance aspects
- Operation and maintenance aspects
- Aspects relating to users of the transport system and third parties
- Consideration of related systems that provide cybersecurity services

The stakeholders responsible for implementing risk treatment measures, whatever the life cycle phase, must be formally identified.

If a risk assessment performed elsewhere for a subsystem or a component of the system under consideration is inherited, the following must be verified:

- That imported functional cybersecurity requirements can be met and translated into cybersecurity measures for the system under consideration
- That there is enough available documentation to support cybersecurity activities. The available documentation must specify the assumptions, constraints, and risk components (in particular the risk sources).

5.2 Development phase

5.2.1 Objectives

The development phase of the system under consideration includes architecture development aspects of the information system, and hardware and software components of the system under consideration without distinction.

The cybersecurity objective of this phase of the life cycle is to implement the cybersecurity measures expressed in the specifications/design phase of these developments. During the development phase, the cybersecurity specifications become specific, intrinsic or exported properties of the system under consideration.

5.2.2 Cybersecurity activities

[EX-2.01] Refine the risk assessment in the development phase	
The risk assessment must be refined by taking into account the specific constraints of the development phase and the new inputs to improve the operational scenarios.	
Inputs	**Outputs**
EX-0.04; EX-0.08; EX-1.01; EX-1.02; EX-1.05	*EX-2.02; EX-3.01*

The development phase can provide new inputs that better characterize the operational scenarios of cybersecurity risks, particularly for the following aspects:

- By analyzing the technological choices made for the development of the system under consideration or its interfaces
- By analyzing the changing context (e.g.: increased activity of a threat source/actor, discovery of a major vulnerability, etc.)
- By refining the threat sources (e.g., if particular tool or technology choices attract new threat sources)
- By refining attack paths following the technical implementation of the development phase (e.g.: technological choices, vulnerability by design, etc.).

These inputs are part of the risk assessment methodology, the principles of which are described in Section 2.3 of this document.

[EX-2.02] Refine the functional cybersecurity requirements in the development phase	
The functional requirements must be refined in relation to the risk assessment refined in the development phase.	
Inputs	**Outputs**
EX-1.04; EX-2.01	*EX-2.03*

The refined functional cybersecurity requirements change the cybersecurity concept which must:

- Match the cybersecurity objectives

- Fully take into account cybersecurity objectives
- Match the assumptions and constraints of the system under consideration

[EX-2.03] Refine the cybersecurity measures in the development phase	
The cybersecurity measures identified from the risk assessment must be refined and adapted for the development phase, taking into account the specific constraints and opportunities provided by the development phase.	
Inputs	**Outputs**
EX-1.04; EX-1.09; EX-2.02	*EX-2.04; EX-3.03*

Cybersecurity measures must be refined and adapted by taking into account:

- Cybersecurity measures from the previous phase of the life cycle
- Cybersecurity measures from already completed regulatory files
- Cybersecurity measures imported as a result of interfaces with new systems
- The maintainability of cybersecurity measures implemented in the development phase
- Constraints on the technical architecture that limit cybersecurity functions
- Development constraints that limit cybersecurity functions
- Development opportunities that offer cybersecurity functions
- Opportunities provided by the architecture that offer cybersecurity functions

The stakeholders responsible for implementing risk treatment measures, whatever the life cycle phase, must be formally identified.

Cybersecurity measures refined in the development phase can also concern cybersecurity measures that apply to the operation/maintenance phase.

[EX-2.04] Complete development in accordance with cybersecurity specifications	
The development of the system under consideration must implement the cybersecurity specifications that apply to the development phase.	
Inputs	**Outputs**
EX-2.03	*EX-2.05*

The cybersecurity measures that apply to the development phase are applied to the components of the system under consideration and become specific properties of it.

[EX-2.05] Establish and implement a cybersecurity inspection plan in the development phase	
A cybersecurity inspection plan must be established and implemented in the development phase of the system under consideration in order to deliver a system that complies with the specifications and the cybersecurity quality plan.	
Inputs	**Outputs**
EX-0.06; EX-1.07; EX-2.04	*EX-4.02*

Cybersecurity inspections in the development phase should include:

- Verification of the cybersecurity quality plan that applies to this phase (see Section 4.2)
- Verification that there are no cybersecurity vulnerabilities in the developments made
- Verification that there are no unexpected functionalities within the system under consideration

5.3 Manufacturing phase

5.3.1 Objectives

The manufacturing phase of the system under consideration includes the manufacturing, configuration and assembly aspects of the system without distinction, including the architecture of the information system supporting the system under consideration.

The cybersecurity objective of this phase of the life cycle is to implement the cybersecurity specifications expressed in the previous phases in the manufacturing process. During the manufacturing phase, the cybersecurity specifications become specific intrinsic or exported properties of the system under consideration.

5.3.2 Cybersecurity activities

[EX-3.01] Refine the risk assessment in the manufacturing phase	
The risk assessment must be refined by taking into account the specific constraints of the manufacturing phase and the new inputs to improve the operational scenarios.	
Inputs	**Outputs**
EX-0.04; EX-0.08; EX-1.01; EX-1.02; EX-2.01	*EX-3.02*

The manufacturing phase can provide new inputs that better characterize the operational scenarios of cybersecurity risks, particularly for the following aspects:

- By analyzing the interdependencies between the different components or subsystems of the system under consideration
- By analyzing the interdependencies with the various components or subsystems interfacing with the system under consideration
- By analyzing the changing context (e.g.: increased activity of a threat source/actor, discovery of a major vulnerability, etc.)
- By refining the threat sources (e.g., if specific architecture choices attract new threat sources)
- By refining attack paths following the technical implementation of the manufacturing phase (e.g.: particular exposure to risk, vulnerability by design, etc.)

These inputs are part of the risk assessment methodology, the principles of which are described in Section 2.3 of this document.

[EX-3.02] Refine the functional cybersecurity requirements in the manufacturing phase	
The functional requirements must be refined in relation to the risk assessment refined in the manufacturing phase.	
Inputs	**Outputs**
EX-1.04; EX-3.01	*EX-3.03*

The refined functional cybersecurity requirements change the cybersecurity concept which must:

- Match the cybersecurity objectives
- Fully take into account cybersecurity objectives
- Match the assumptions and constraints of the system under consideration

[EX-3.03] Refine the cybersecurity measures in the manufacturing phase	
The cybersecurity measures identified from the risk assessment must be refined and adapted for the manufacturing phase, taking into account the specific constraints and opportunities provided by the manufacturing phase.	
Inputs	**Outputs**
EX-1.04; EX-2.03; EX-3.02	*EX-3.04; EX-4.01*

Cybersecurity measures must be revised and adapted by taking into account:

- Cybersecurity measures from the previous phase of the life cycle
- Cybersecurity measures from already completed regulatory files
- Cybersecurity measures imported as a result of interfaces with new systems
- The maintainability of cybersecurity measures implemented in the manufacturing phase
- Constraints on the technical architecture that limit cybersecurity functions
- Manufacturing constraints that limit cybersecurity functions
- Opportunities provided by manufacturing that offer cybersecurity functions

The stakeholders responsible for implementing risk treatment measures, whatever the life cycle phase, must be formally identified.

Cybersecurity measures refined in the manufacturing phase can also concern cybersecurity measures that apply to the operating/maintenance phase.

[EX-3.04] Complete manufacturing in accordance with cybersecurity specifications	
The manufacturing of the system under consideration must implement the cybersecurity specifications that apply to the manufacturing phase.	
Inputs	**Outputs**
EX-3.03	*EX-3.05; EX-4.01*

The cybersecurity measures that apply to the manufacturing phase are applied to the components of the system under consideration and become specific properties of it.

[EX-3.05] Establish and implement a cybersecurity inspection plan in the manufacturing phase	
A cybersecurity inspection plan must be established and implemented in the manufacturing phase of the system under consideration in order to deliver a system that complies with the specifications and the cybersecurity quality plan.	
Inputs	**Outputs**
EX-0.06; EX-1.07; EX-3.04	*EX-4.02*

Cybersecurity inspections in the development phase should include:

- Verification of the cybersecurity quality plan that applies to this phase (see Section 4.2)
- Verification that the interfaces, interactions, behavior and system functions work securely
- Verification that related systems that support cybersecurity services work properly
- Verification of the cybersecurity behavior and interactions between the system under consideration and the external environment.

5.4 Integration / installation phase

5.4.1 Objectives

The integration/installation phase of the system under consideration includes the approval, acceptance and commissioning activities for the system. During this phase in particular, acceptance of the system under consideration is formally determined.

The cybersecurity objectives of this phase of the life cycle are as follows:

- For the approval of the system under consideration, provide objective evidence that the system meets the cybersecurity functional requirements and implements the specified cybersecurity measures, and that cybersecurity management complies with the cybersecurity quality plan
- For acceptance of the system under consideration, formally confirm that the system meets the cybersecurity objectives in its operational environment
- For the commissioning of the system under consideration, ensure that the system under consideration is able to keep cybersecurity risks at an acceptable level.

5.4.2 Cybersecurity activities

<table>
<tr><th colspan="2">[EX-4.01] Refine the cybersecurity measures in the integration/installation phase</th></tr>
<tr><td colspan="2">The cybersecurity measures identified from the risk assessment must be refined by taking into account the specific constraints of the integration/installation phase.</td></tr>
<tr><th>Inputs</th><th>Outputs</th></tr>
<tr><td>EX-1.01; EX-1.02
EX-1.04; EX-3.03; EX-3.04</td><td>EX-4.02; EX-4.03; EX-5.01; EX-5.02</td></tr>
</table>

Cybersecurity measures must be revised by taking into account:

- Cybersecurity measures and functional requirements from the previous phase of the life cycle
- Cybersecurity measures and functional requirements from already completed regulatory files
- Cybersecurity measures and functional requirements imported as a result of interfaces with new systems
- Constraints on integration/installation that limit cybersecurity functions
- Constraints of the information system architecture supporting the system under consideration
- Constraints from the operational environment, including:
    - The physical or geographical environment of the operational environments
    - The stakeholders of the operational environments

The stakeholders responsible for implementing risk treatment measures, whatever the life cycle phase, must be formally identified.

[EX-4.02] Approve the cybersecurity of the system under consideration	
A cybersecurity approval plan for the system under consideration incorporating appropriate methods and techniques must be prepared and implemented to ensure that cybersecurity measures are properly implemented and meet cybersecurity objectives.	
Inputs	**Outputs**
Results of the tests from the previous phases *EX-0.06; EX-1.07; EX-2.05; EX-3.05; EX-4.01*	*EX-4.03*

The approval plan is implemented after the integration/installation activities and prior to system acceptance. It includes:

- The type of methods and techniques used among:
  - Cybersecurity acceptance actions
  - Technical audits (architecture audit, configuration audit, code audit, etc.)
  - Organizational audits (physical audit, process audit, etc.)
  - Penetration testing (penetration testing is the basis for a cybersecurity robustness assessment)
  - "*Red team*" testing
  - Staff security testing
- The depth of the methods and techniques used:
  - Document audits
  - Declarative audits
  - Field observations and technical tests
- Qualification of the people in charge of performing approval actions:
  - Their independence from the stakeholders of the system under consideration
  - Their expertise in the methods and techniques used
  - Their technical and organizational cybersecurity expertise
  - Their professional ethics
- Planning of approval tasks

Sufficient protective measures must also be taken to prevent potential compromises during testing performed under the approval plan.

[EX-4.03] Accept the system under consideration with regard to cybersecurity	
Acceptance of the system under consideration with regard to cybersecurity must be formally determined, by accepting in full knowledge of the residual cybersecurity risks, in connection with the risk assessment and the approval actions performed.	
Inputs	**Outputs**
EX-4.01; EX-4.02	*EX-4.04; EX-4.05*

Acceptance of the system under consideration with regard to cybersecurity requires a formal decision in an ad hoc committee which entails:

- Formal definition of acceptance criteria, including the level of acceptable risk
- Formal designation of the person in charge of acceptance

- Formal definition of a comitology in charge of acceptance

This comitology is defined in the cybersecurity quality plan.

Acceptance of the system under consideration with regard to cybersecurity is carried out on the basis of tangible evidence which must be documented.

Acceptance of the system under consideration may identify a cybersecurity debt (actions contributing to control the risk for the system under consideration that have yet to be carried out, including the actions identified from the approval plan). This cybersecurity debt must:

- Be formalized, including the end date of the actions
- Be accepted for acceptance of the system under consideration

[EX-4.04] Integrate cybersecurity into handoff actions to the responsible entity	
A cybersecurity delivery plan for the system under consideration must be prepared and implemented to ensure that the level of risk to the system is at an acceptable level when handed off for operation/maintenance.	
Inputs	**Outputs**
SMS Project; EX-4.03	*If system under consideration = ARTS: Updated SMS (operator as the responsible entity)* *If system under consideration = TS: delivery process, user manual etc. (to be defined) to the SO (as responsible entity)* *EX-4.05; EX-5.01*

The delivery plan for the system under consideration must include the cybersecurity-related actions to be performed as part of handoff to the responsible entity, incorporating:

- Detailed action plans for dealing with the cybersecurity debt resulting from the approval phase of the system under consideration
- Delivery of cybersecurity documents for the system under consideration (processes, procedures, operating procedures, guides)
- Training for those involved in the operation/maintenance phase on cybersecurity actions specific to the system under consideration

[EX-4.05] Integrate cybersecurity into the In-Service Testing period	
The In-Service Testing period must determine that the cybersecurity measures implemented allow cybersecurity risks to be kept at an acceptable level.	
Inputs	**Outputs**
EX-4.03; EX-4.04	*EX-5.01*

The means implemented for the In-Service Testing period must be formalized and include:

- Enhanced monitoring measures for cybersecurity performance
- Involvement of stakeholders from previous phases
- Ability to call on specific expertise

- The implementation of a specific organization.

The requirements of the operation/maintenance phase (Chapter 5.5) must be implemented.

5.5 Operation / maintenance phase

5.5.1 Objectives

The objective of this phase of the life cycle is to operate and maintain the system under consideration in such a way as to ensure that the level of risk to the system is kept at an acceptable level.

The requirements that apply during this phase must be translated into the operating/maintenance procedures for the system under consideration and appear, as such, in the regulatory file(s) provided in support of the system under consideration, and prepared before commissioning.

5.5.2 Cybersecurity activities

[EX-5.01] Prepare a cybersecurity maintenance plan	
A cybersecurity maintenance plan must be developed and implemented for the system under consideration, including all the processes expected to maintain the level of risk to the system at an acceptable level.	
Inputs	**Outputs**
EX-0.04; EX-0.05; EX-0.06; EX-0.07; EX-0.08; EX-4.01; EX-4.04; EX-4.05	*EX-5.02; EX-5.03*

The cybersecurity maintenance plan for the system should include:

- Expectations in terms of cybersecurity expertise during the operation and maintenance phase
- The process and resources for monitoring cybersecurity performance
- The process and resources for monitoring changes in the system and its environment
- The process and resources for monitoring vulnerabilities and patches
- The process and resources for performing updates
- The process and resources for managing cybersecurity incidents
- The process and resources for responding to cybersecurity incidents
- The cybersecurity crisis management process and resources.

[EX-5.02] Carry out routine cybersecurity operations	
Routine cybersecurity operations for the system under consideration must be documented and performed continuously.	
Inputs	**Outputs**
EX-4.01; EX-5.01; EX-5.04; EX-5.05; EX-5.06; EX-5.07; EX-5.08; EX-5.09	*EX-5.03*

Routine cybersecurity operations for the system should include:

- Operational activities as such, especially for handling errors (vulnerabilities related to improper configuration)
- Signature updates for all detection methods (antivirus, intrusion detection, etc.)

- Configuration management activities in order to maintain a complete and up-to-date configuration management database
- Activities for performing and managing backups and activities for testing and managing restorations
- Access authorization management activities over time, particularly taking into account staff movements

[EX-5.03] Ensure that the risks to the system under consideration are kept to an acceptable level during and after maintenance operations	
Maintenance operations must not increase the level of risk to the system under consideration or expose it to new cybersecurity risks.	
Inputs	**Outputs**
EX-5.01; EX-5.02; EX-5.05; EX-5.08	

All aspects related to cybersecurity in maintenance operations must be taken into account, including:

- Ensuring the authenticity and integrity of updates
- Ensuring that maintenance staff can be trusted
- Ensuring controlled exposure in the event of connected maintenance

In addition, the implementation of a cybersecurity function must not degrade the performance of the system (e.g.: filtering function on real-time equipment).

[EX-5.04] Ensure that staff are skilled in cybersecurity	
Staff involved with the system under consideration must be continuously trained and made aware of cybersecurity issues related to their function and tasks.	
Inputs	**Outputs**
EX-0.03	*EX-5.02*

The type of training and awareness-raising actions must be adapted to:

- The type and criticality of the components on which they work
- The level of privileges on the components on which they work.

Staff receive cybersecurity qualification via:

- A training plan for cybersecurity in routine tasks
- A cybersecurity awareness plan, including
    - Awareness of the basics of cyber hygiene
    - Awareness of cybersecurity risks.

[EX-5.05] Monitor cybersecurity performance	
A system for monitoring the cybersecurity performance of the system under consideration must be implemented and operated on a continuous basis in order to detect cybersecurity events on a continuous basis, trigger corrective or preventive actions if necessary, and measure the level of cybersecurity risk.	
Inputs	**Outputs**
EX-0.05; EX-1.07; EX-5.11	*Ex-5.02; Ex-5.03; Ex-5.08; Ex-5.09*

The cybersecurity performance monitoring system must be able to detect and respond to events related to incidents involving cybersecurity risks to the system under consideration. It must therefore implement:

- A data collection strategy adapted to the events to be detected, and consequently, a storage capacity for these events
- An analysis strategy for the collected data adapted to the events to be detected, and consequently, ways to index and query this data
- A strategy for reporting detected events, integrating all the stakeholders of the system under consideration depending on the type of event
- Procedures to support the operational implementation of collection, analysis and reporting strategies
- The production of indicators and dashboards to measure trends and detect weak signals

[EX-5.06] Ensure the management of cybersecurity incidents	
A cybersecurity incident management process must be specified and implemented in order to ensure that incidents are handled and that corrective or preventive actions are taken to resolve them.	
Inputs	**Outputs**
Emergency Response Plan; EX-0.01; EX-0.02; EX-0.05	*EX-5.02; EX-5.09*

The cybersecurity incident management process must include:

- Procedures for qualifying the incident and criteria for qualifying the incident
- Procedures for analyzing the incident
- The roles and responsibilities associated with the actions to be taken
- Procedures for reporting the incident
- Procedures for monitoring actions
- Procedures for launching a digital investigation
- Procedures for launching cybersecurity crisis measures
- Procedures for closing the incident and closure criteria

The cybersecurity incident management process should include the potential support of specialized private or public services.

The cybersecurity incident management process must allow for the capitalization of cybersecurity incidents, and therefore collect and store necessary information.

The incident management process must comply with the decree: Articles R.3152-20 to R.3152-22.

[EX-5.06] Manage cybersecurity crises	
A cybersecurity crisis management process must be defined and implemented in order to manage cybersecurity crisis situations.	
Inputs	**Outputs**
Emergency Response Plan; EX-0.01; EX-0.02; EX-0.05	*EX-5.02*

The cybersecurity crisis management process must include:

- Decision-making criteria for declaring a crisis
- The specific organization of crisis management
- Provisions relating to the organization of the crisis unit
- Provisions for reporting the crisis
- The resources required for crisis support
- Decision-making criteria for closing a crisis
- Capitalization provisions (immediate or later analysis)

The cybersecurity crisis management process must interface with the Intervention and Safety Plan for the system under consideration.

[EX-5.08] Ensure that vulnerabilities and patches for these vulnerabilities are constantly monitored	
A process for monitoring vulnerabilities and patches for the components of the system under consideration must be detailed and implemented in order to quickly identify and take into account vulnerable and/or obsolete components.	
Inputs	**Outputs**
EX-0.04; EX-5.05	*EX-5.02; EX-5.03*

The vulnerability monitoring process must include:

- Consideration of all the vulnerabilities on the components of the system under consideration, and consequently, the link with the configuration management of the system
- Qualification of the intrinsic criticality of the vulnerability (without context) and qualification of the contextual criticality of the vulnerability (within the system under consideration)
- The documented decision to accept the vulnerability, fix the vulnerability or apply compensatory measures

In addition, the monitoring process should include obsolescence or end-of-support cases in the alerts it reports to the monitoring unit.

[EX-5.09] Ensure that components are updated	
An update management process must be detailed and implemented in order to prevent obsolescence and/or ensure the timely application of cybersecurity patches for vulnerable components of the system under consideration.	
Inputs	**Outputs**
EX-5.05; EX-5.06	*EX-5.02*

The update management process must include:

- Testing procedures
- Provisions to ensure that the operational performance of the system under consideration does not regress following updates.

[EX-5.10] Constantly monitor changes to the system and its environment	
A process for monitoring changes to the system under consideration and its environment must be detailed and implemented in order to reassess the risks to the system.	
Inputs	**Outputs**
EX-0.04 *Detailed report* *Operator's annual report*	*EX-5.11*

Changes to the system under consideration or its environment are closely tied to cybersecurity risks. The criteria for re-evaluating the risk assessment must be specified in the monitoring process.

The changes to be considered include:

- Changes to the system itself:
  - Functional changes
  - Changes to cybersecurity objectives (resulting from poor inspection or audit results, incident analysis report, etc.)
  - Changes to the technical architecture or one of the components (e.g.: new software or hardware connection)
- Changes to the environment of the system under consideration:
  - Change to the ecosystem
  - Change to the functional design domain
  - Change to the root
  - Change in threat / threat sources
  - Change in vulnerabilities

[EX-5.11] Reassess risks in the operation/maintenance phase	
The risk analysis of the system under consideration must be reassessed periodically and when the change to the system under consideration or its environment affects the risks to the system.	
Inputs	**Outputs**
EX-0.04; EX-0.08; EX-1.01; EX-1.2; EX-5.10	*EX-5.05*

The risk reassessment covers all the steps described in Section 2.3 of this document, including the risk analysis.

The reassessment of the analysis should also verify:

- The consideration of measures from the previous phase of the life cycle
- The consideration of measures from already completed regulatory files
- The assumptions made and consistency between these assumptions

The stakeholders responsible for implementing new risk treatment measures, whatever the life cycle phase, must be formally identified. The responsible entity must decide on the substantiality of the risk treatment measure, i.e. whether it involves a substantial change to the automated road transport system (see Section 1) as per Article R.3152-18 IV.

It is a prerequisite for the diagnosis of the system’s cybersecurity described in Article R3152-16 of the decree, if the diagnosis concerns cybersecurity.

5.6 Withdrawal from service phase

5.6.1 Objectives

The withdrawal from service phase for the system under consideration includes without distinction, the aspects of removing or dismantling a subsystem or component of the system under consideration and the aspects of stopping a service offered by the system. Withdrawal of a service is part of the life cycle of the system and is taken into account in the earlier phases of the project.

The cybersecurity objective of this phase of the life cycle is to implement the cybersecurity measures required to ensure that withdrawal of the service has no impact on the cybersecurity of the system under consideration.

5.6.2 Cybersecurity activities

[EX-6.01] Establish and implement a cybersecurity inspection plan in the End of Life phase	
A cybersecurity inspection plan must be developed and implemented in the End of Life phase of the system under consideration in order to manage the impacts of related systems on cybersecurity in accordance with the cybersecurity quality plan.	
Inputs	**Outputs**
EX-0.05; EX-0.07	

Cybersecurity inspections in the End of Life phase should include:

- Verification of the cybersecurity quality plan that applies to this phase (see Section 4.2)
- Verification that the remaining interfaces, interactions, behavior and system functions work securely after End of Life
- Verification that related systems that support cybersecurity services work properly after End of Life
- Verification of the cybersecurity behavior and interactions between the system under consideration and the external environment after End of Life.
- Verification that no replaced equipment, components or equipment can be used to carry out intelligence in preparation for an attack on the system under consideration.
- Informing the stakeholders affected by the End of Life phase, either as dependents or as users of the service.

ANNEXES

Annex A: Index of requirements

Annex B: Standard ecosystem of an ARTS

The following standard ecosystem is provided as a guide only. The right-hand column in particular is not exhaustive and should be clarified according to the project and the activity concerned.

Vehicle Ecosystem		
Designer	➡	Navigation system, Telematics, Infotainment, Radar, Lidar, On-board camera, V2X system, Automotive equipment (e.g. chassis)
Manufacturer		
Maintainer		
Infrastructure and equipment ecosystem		
Manager[2]	➡	Roadway equipment: road markings (on the road, crosswalks, specific lanes such as bus lanes / bicycle paths), sidewalks
Designer	➡	Smart or regular traffic lights, Traffic signs, Display panels, Surveillance cameras, traffic enforcement cameras, Dynamic signage
Manufacturer		
Maintainer		
Maintainer	➡	Road markings / posts
Service ecosystem		
Transport authority	➡	Maintenance staff, Command Centre, Fleet management software, Website, Mobile app for customers, Bus station, Parking area, Customer reception area (stores)
Service operator		
Public or private services	➡	Specific service vehicle (ambulance, police, fire department), Roadside monitoring station, Service station (fuel, charging), Warehouses, Tolls
Route / area ecosystem		
Third parties	➡	Vehicles and people: Vehicles, Pedestrians, Residents, Cyclists, PMD, Trams, etc.
Route	➡	Route characteristics: Road, Highway, Private right-of-way, Bridge, Tunnel, etc.
Zones	➡	Specific zones: emergency lanes, turning lanes, reserved lanes (bus, cab), parking, tolls, etc.
Cross-functional ecosystem		
Monitoring sources	➡	Internal sources: Legal department, technical department, etc. Open sources: Social media networks Government sources: ANSSI, GIP ACYMA Specialized organizations: CERT, hardware and software publishers and maintainers, universities and research centers, specialized cybersecurity associations
Cybersecurity third parties	➡	OQA Service and consulting organizations

Table 6: Standard ARTS ecosystem

[2] Designates the manager(s) of all the equipment, whether or not it is delivered with the technical system: traffic lights, traffic signs, billboards, surveillance cameras, traffic enforcement cameras, dynamic signage, etc.

Annex C: Standard functional modeling of an ARTS

The information provided below has been taken from bibliographic source [22], Technical Guide for GAME Demonstration for ARTS.

This functional breakdown 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 functional modeling presented here is limited to the first two levels (refer to the technical guide on GAME demonstration for ARTS for more details).

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 breakdown 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 a supplement once the methodological report "Characterization of remote intervention functions" of the DGITM is published.

Level 1 function	Level 2 function
1-Define, monitor and control the vehicle trajectory	1.1-Perceive the surroundings (sense)
	1.2-Locate the vehicle on the route / area in relation to the defined route
	1.3-Make decisions about dynamic control (plan)
	1.4-Perform dynamic control (act)
2-Signal the vehicle to other road users (sound, visual signals, etc.)	2.1-Signal the automated driving mode
	2.2-Signal the vehicle's maneuvering intentions
	2.3-Signal a significant deceleration of the vehicle
	2.4-Signal the vehicle's position
	2.5-Signal the vehicle's situation
	2.6-Signal an imminent danger
3-Manage access to automated vehicles	3.1-Manage the transfer of people at authorized locations
	3.2-Keep the automated vehicle closed when not transferring people/evacuating
	3.3-Enable evacuation and emergency access
4- Ensure proper transport conditions for passengers	
5- Enable users to interact with system components	5.1-Enable the users to communicate with operating personnel (COM)
	5-2 Allow passengers to request that the vehicle be stopped
	5.3-Provide users with access to services
6-Manage dynamic infrastructure components controlled by the system	6-1 Control dynamic signaling
	6-2-Control mobile dynamic equipment
7- Ensure operation of the system	7.1-Define the mission of each vehicle
	7.2 Intervene remotely on technical components of the system
	7.3-Enable communication between the operating personnel
	7.4-Enable communication between the system and external actors
	7.5-Record data
	7.6-Inform about the status of the system components
	7.7-Enable the operator to see the situation in the vehicle
	7.8- Enable the operator to see the situation outside the vehicle
	7.9-Enable information to be communicated to passengers
	7.10-Enable the safe intervention of emergency services
8- Detect and manage specific situations	8.1-Detect and manage fires
	8.2-Detect impacts against the vehicle
9 - Ensure that the system is kept in safe conditions	9.1-Adapt operating instructions to traffic conditions
	9.2-Detect if the system leaves its operational domain
	9.3-Perform an MRM suitable for the situation
	9.4-Perform an emergency maneuver adapted to the situation
	9.5-Perform a "final" shutdown

Table 7: Functional breakdown of an ARTS (limited to levels 1 and 2)

Annex D: Modeling via the stratified model

The information provided below has partly been taken from bibliographic source [24], AFNOR Guide – Voluntary standards and innovative approaches to cybersecurity.

Innovative ways of representing a cyber threat environment are discussed, particularly in French military doctrine for offensive cybersecurity. It involves taking into account the complexity of human, digital and physical components and their interdependencies.

One way consists in modeling the space, and by extension, the system under consideration, by introducing a representational model stratified into three fundamental strata:

- The ANTHROPIC stratum which represents human actors and groups of human actors organized in social networks
- The DIGITAL stratum which represents the logical processes and computer data, including the avatars of human actors
- The PHYSICAL stratum which represents the physical components and geographical location of the components and people

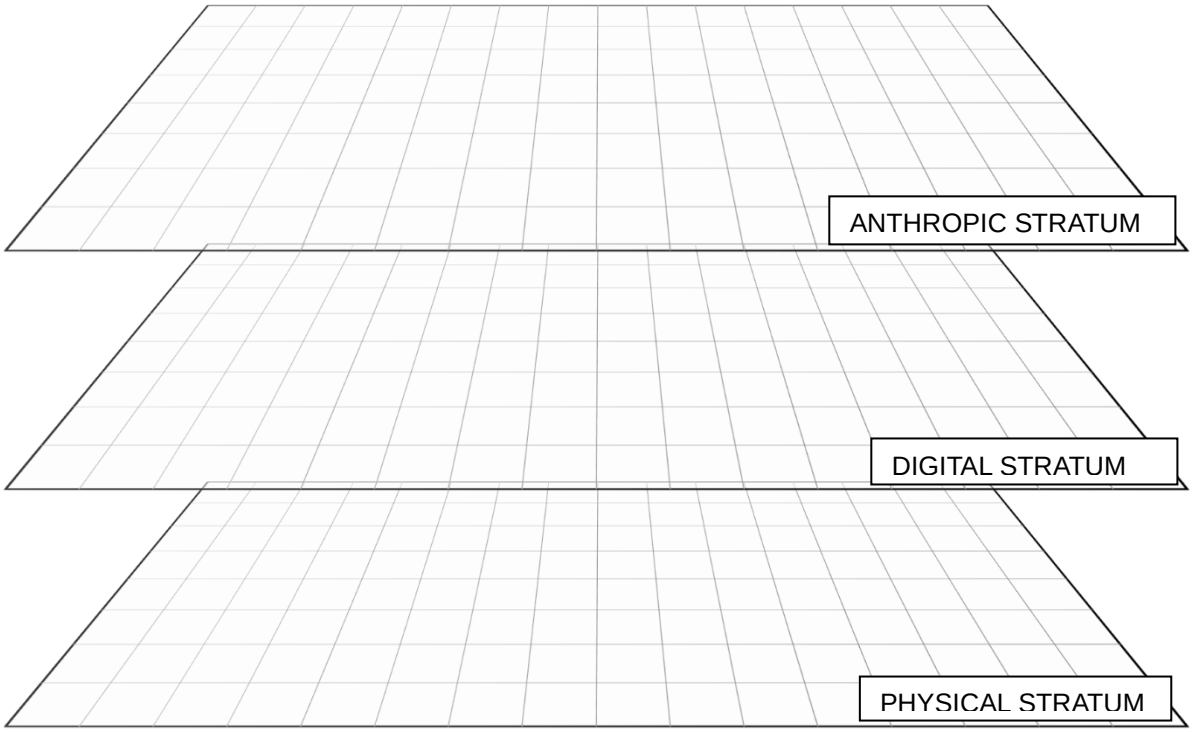


Figure 10: Projection of the threat environment on a model of the stratified space

The stratified representational model allows the system under consideration and its ecosystem to be modeled with a level of detail determined by the analyst depending on the depth of analysis required, while keeping the model unchanged. These three basic layers can also be subdivided for specific analyses.

Each stratum is populated by nodes and intra-stratum links crossed by flows (see Table 8), of very different types depending on the stratum concerned, which constitute the projection of the system under consideration on this stratum. Projections are facilitated by the use of knowledge bases. Their level of detail is up to the analyst, depending on the aim of the study and the complexity of the system observed.

Stratum	Characteristics
Anthropic stratum	Fractal model: the unit is the person who can form groups or interconnecting social networks • Nodes: individuals and groups of individuals • Links: various forms of social links (authority, partnership, antagonism, etc.) • Flows: flows associated with social links (subornation, collaboration, confrontation, etc.)
Digital stratum	Fractal model: each logical system can be made up of logical subsystems and can part of larger systems: • Node: computer process • Link: communication protocol • Flows: information flows
Physical stratum	Fractal model: variable level of detail (land use plan, structure of a building, topographic map, etc.). The stratum is subject to the laws of physics. • Node: movable property • Link: pipe [material], electric cable [energy], Ethernet cable [information] • Flows: material flows, energy flows, information flows

Table 8: Type of components by stratum

The strata communicate with each other; the exchanges between different strata are materialized by inter-stratum links (see Table 9). Each of these links has its own nature.

Strata concerned	Nature of the inter-stratum links
anthropic ↔ digital	Identity link: digital identities of a human actor (email address, user account, avatar on a social media network, etc.) Knowledge link: the human actor's knowledge of a digital identity (e.g.: a social media network avatar) Access link: access of a human actor to a digital component (in the control / command sense of the term)
anthropic ↔ physical	Location link: geographical location (in an area, a building, etc.) of a human actor Knowledge link: the human actor's knowledge of physical or geographical location information Access link: ability of a human actor to access a physical component and/or a geographical area
digital ↔ physical	Location link: location of the physical components that host data (potentially highly distributed) Implementation link: location of physical components that run a program (possibly highly distributed) Control / command link: ability of a program to interact with a physical component (e.g.: sensor / actuator)

Table 9: Types of the inter-stratum links

The resulting representation provides a topological view of the system under consideration, facilitating the development of threat scenarios. This model should be applied to the ARTS in two steps:

- Identify and explain the components specific to the system under consideration on each of the representation strata (see Figure 11, Figure 12, Figure 13)
- Identify and characterize the links between the different components on each of the strata (see Figure 14)

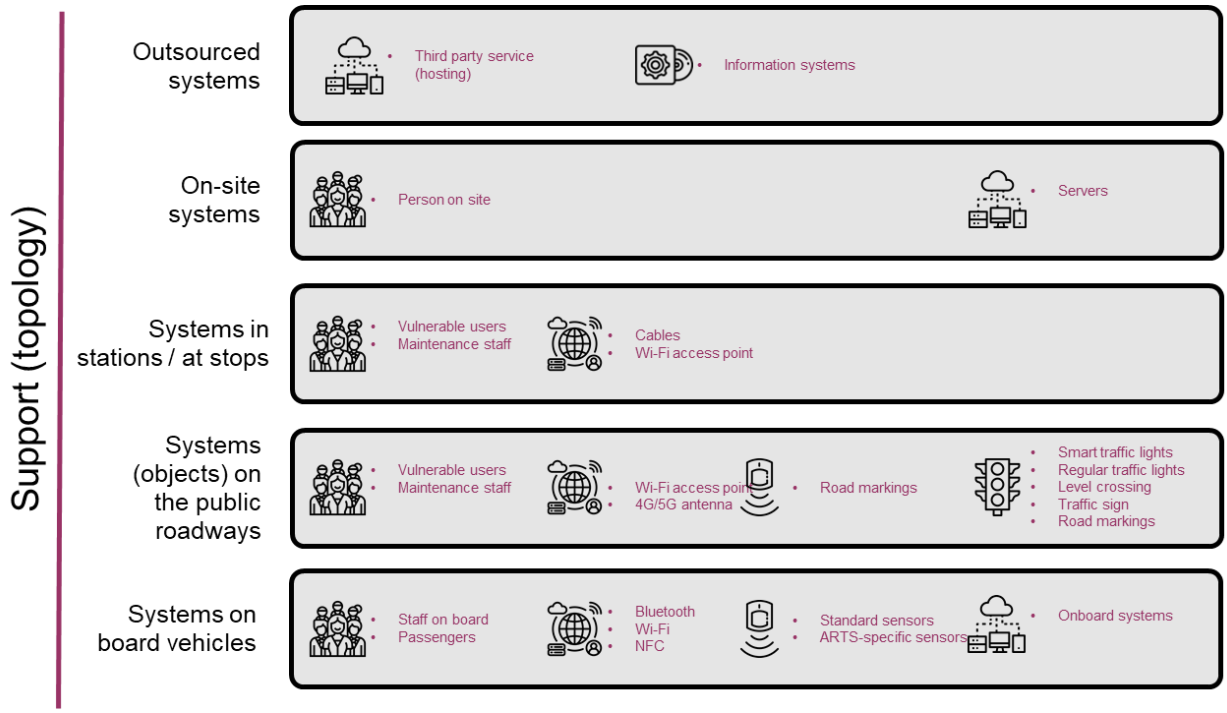


Figure 11: Topological approach for modeling the system under consideration (physical space)

Figure 12: Topological approach for modeling the system under consideration (numerical space)

Figure 13: Topological approach for modeling the system under consideration (anthropic space)

The fractal character of the stratified representational model allows precise interactions between two distinct strata to be modeled. In other words, as many strata as necessary can be introduced, as long as they are used to better represent reality. The most common subdivisions are the following:

- Subdivision of the physical stratum (see Figure 14) into a “geographic” stratum (physical topology of the space and geographical location of components and people) and a “component” stratum (physical components of the space, including the equipment that make up the ARTS)
- Subdivision of the digital stratum into a “cyber” stratum (computer processes and data, which can itself be subdivided if necessary into the layers of the OSI model - see Figure 14) and a “cyber-persona” stratum (digital identities necessary for exchanges).

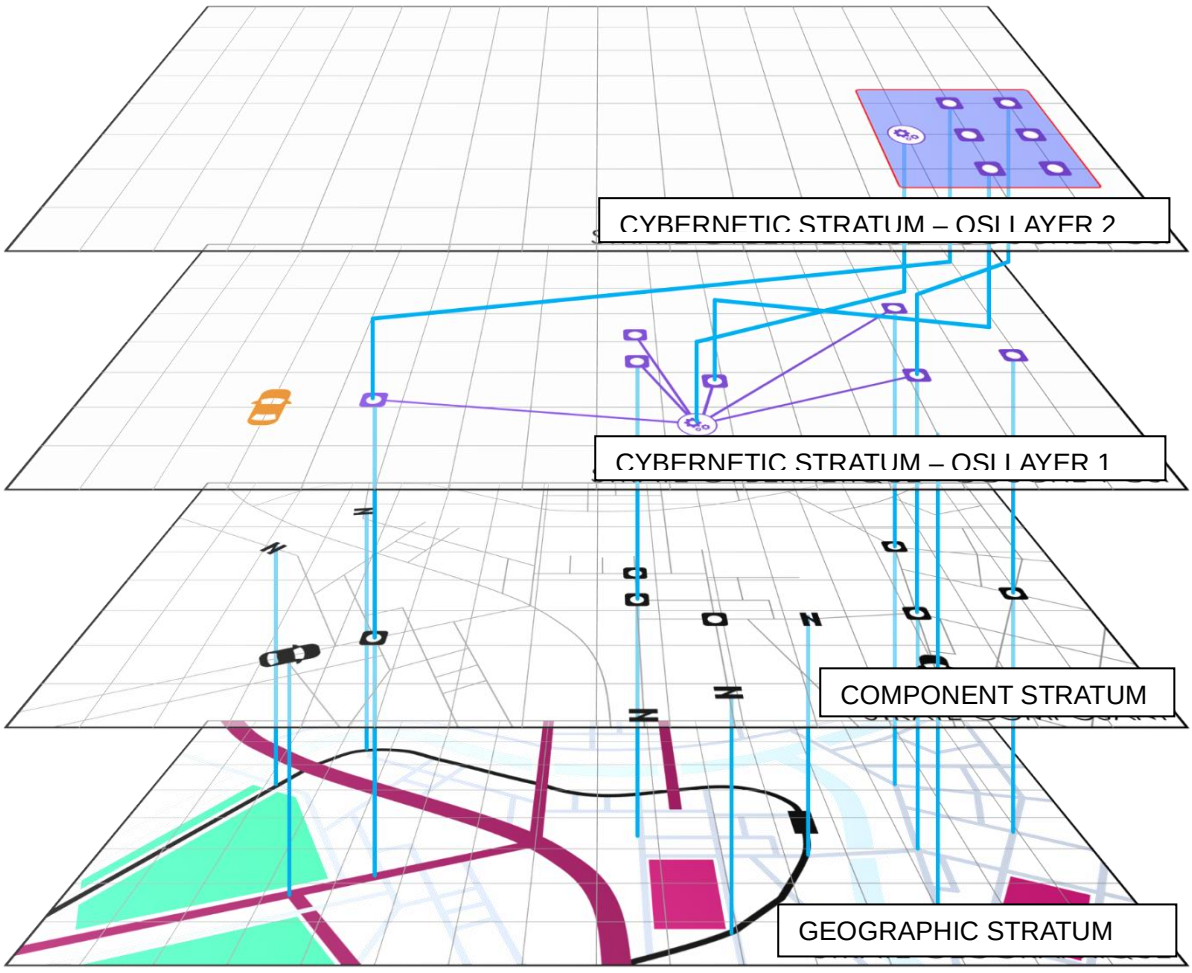


Figure 14: (Partial) projection of an ARTS in the stratified model of the space

Annex E: List of system-level accidents

The information provided below has been taken from bibliographic source [22,] Technical Guide for GAME Demonstration for ARTS

Please note the following for this table:

- The list is not exhaustive and is intended to be expanded.
- 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, or 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.
- A cyber attack can be the cause of these accidents.
- Some of the accidents included may be grouped together if the analysis shows that they should be managed in the same way.

Type	ID	Potential accidents
Collision	1.1	Collision with a vulnerable road user (cyclist, pedestrian, etc.)
	1.2	Side/head-on collision with a solid obstacle (containers, animals, falling trees, etc.)
	1.3	Collision with another road vehicle
	1.4	Collision with the vehicle of a guided transport system (trams, etc.) or rail transport system (heavy rail)
	1.5	Collision with another type of vehicle
Falls	2.1	A person falling inside the vehicle
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
Rollover	3.1	Vehicle rollover
Electric shock/Electrocution	4.1	Electric shock/Electrocution in the vehicle
	4.2	Electric shock/Electrocution in station
Electric shock/Electrocution	4.3	Electric shock/Electrocution on the route from system equipment
Fire/smoke/explosion	5.1	Fire/smoke in the vehicle
	5.2	Fire/smoke at a station
	5.3	Fire/smoke on the route from system equipment
	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
	6.2	Passengers trapped/pinched by a moving part of system component
	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)
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
	7.2	Passengers hit by a falling / projected / lost part of a vehicle in its passenger compartment
	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.)

Table 10: List of system-level accidents

Annex F Characterization of threat sources/actors

The information provided below has partly been taken from bibliographic source [24], AFNOR Guide – Voluntary standards and innovative approaches to cybersecurity.

Identification of threat sources/actors

Threat sources/actors can first be structured into general categories (aggressive nation states, organized crime, terrorist groups, sectarian movements, etc.) and into categories reflecting the specific relationship between the system under consideration and an actor in the ecosystem that may develop antagonism (competitors, suppliers, employees, etc.).

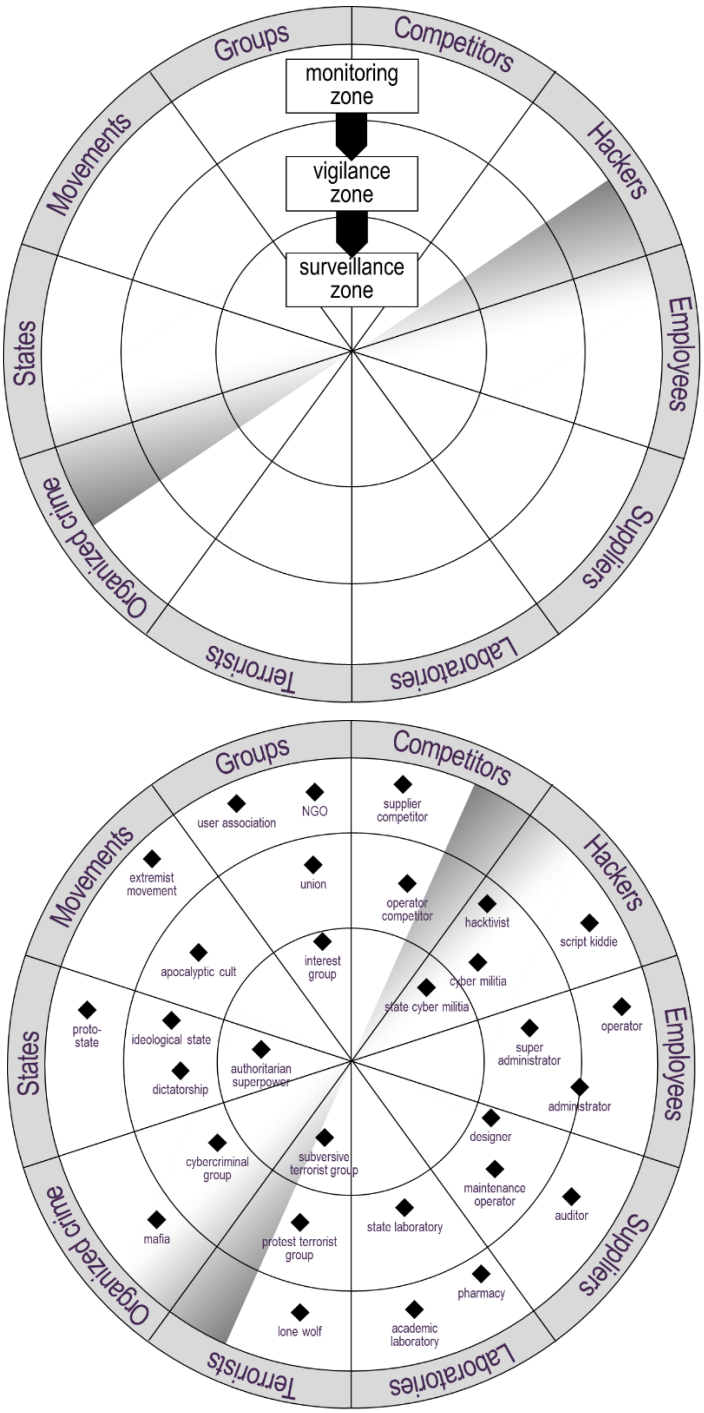


Figure 15: Characterization of threat sources/actors into general categories

Characterization and assessment of threat source motivations

There are a wide variety of motivations that can be classified according to a systematic typology (one model in the following list, other models of motivation exist, see Figure 16):

- Political motivation (involves notions of authority, prestige, power, etc.).
- Economic motivation (involves notions of wealth, possession, influence, etc.).
- Ideological motivation (involves notions of culture, religion, ethics, etc.).
- Social motivation (involves notions of recognition, influence, etc.).
- Idiosyncratic motivation (specific to each individual and therefore unpredictable).
- Survival motivation (involve notions of subsistence, resilience, etc.).

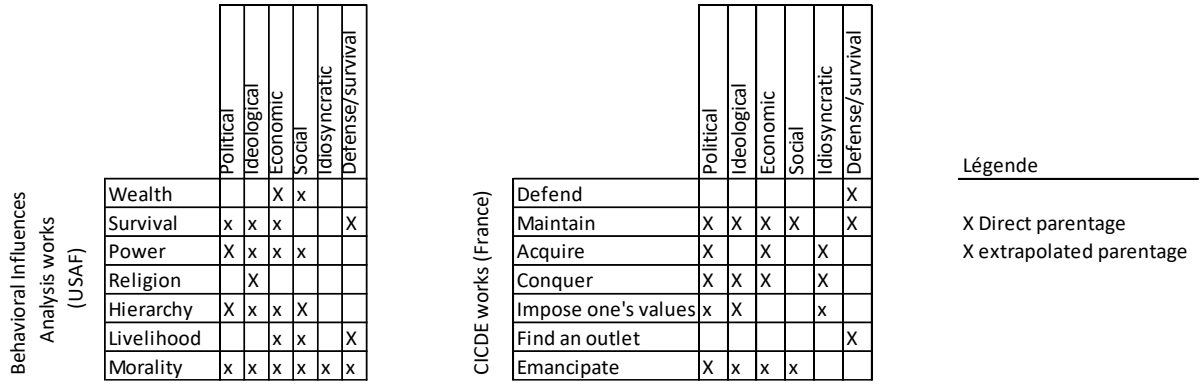


Figure 16: Relationship between the different motivation models

Using this taxonomy, it is possible to establish a motivation graph that is contextual to the system under consideration for each threat source (see Figure 17).

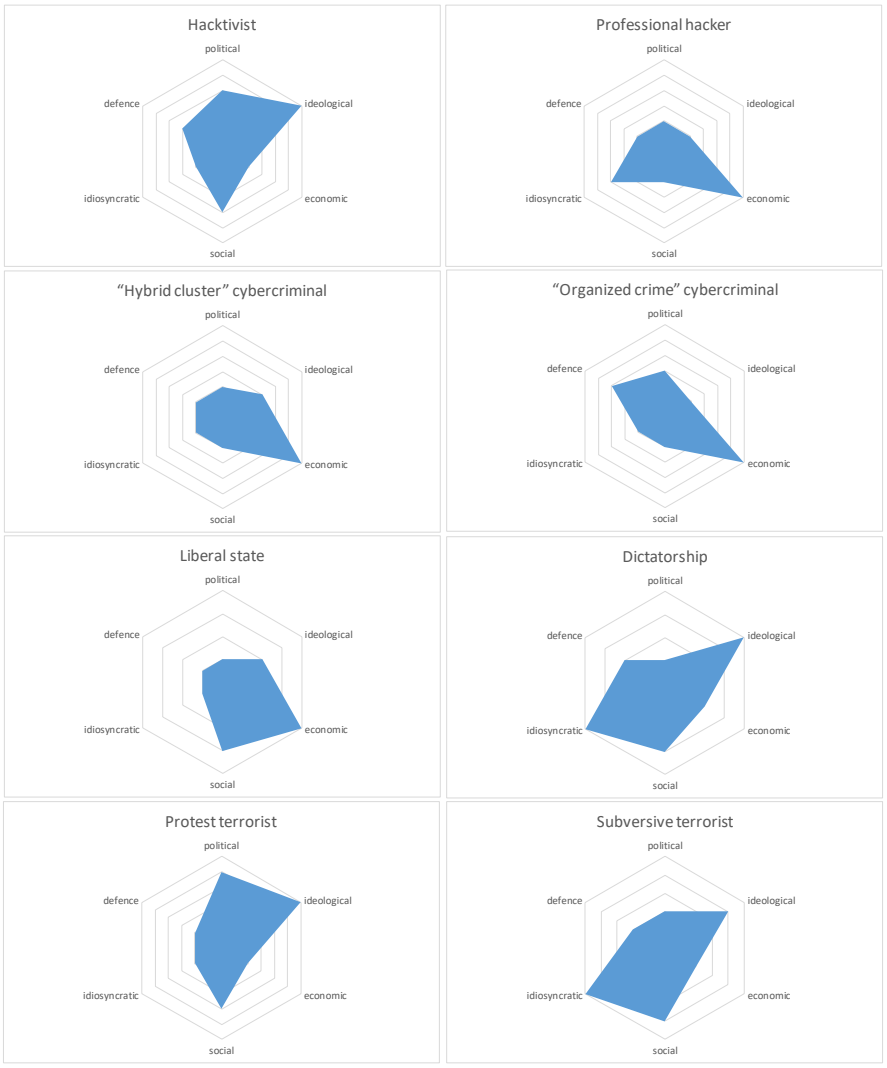


Figure 17: Examples of motivation graphs for a given system

If a motivation cannot be directly expressed, it can be materialized through the threat source's intention and expressed in the form of an end goal (the overall outcome that the attacker wants to achieve after the attack).

End goals are thus structured along two lines:

- The nature of the threat source's motivation (see above)
- The goals of the threat source, depending on its position in relation to the target
    - Conquer: Achieve supremacy (total superiority)
    - Depose: Achieve superiority by neutralizing the adversary
    - Acquire: Achieve superiority by appropriating new resources
    - Push back: preserve parity by restricting adverse development
    - Maintain: preserve parity by maintaining its position
    - Defend: limit the situation of inferiority
    - Survive: continue to exist

The combination of these two factors makes it possible to determine end goals that depend on both contextual elements and the nature of the hostility itself (see **Erreur ! Source du renvoi introuvable.**). T his involves working on a multi-criteria analysis rather than scales of motivation.

GOAL	Ideological	Political	Economic	Social	Idiosyncratic
Conquer (domination)	Impose values	Gain absolute power	Dominate a market	Control other social groups	Megalomania
Depose (elimination)	Restrict values	Restrict power	Eliminate an economic actor	Ban Deprive	Hate Revenge
Acquire (superiority)	Have one's values recognized	Participate in power	Obtain market share	Acquire social capital or rights	Ambition
Push back (inferiority)	Revert values	Chase from power	Cause others to lose market share	Compromise a reputation	Fear
Maintain (status quo)	Protect one's values	Maintain power	Keep market share	Protect one's reputation	Pride
Prevent (status quo)	Prevent progress	Restrict access to power	Confine a market position	Hinder awareness	Jealousy Envy
Defend (survival)	Limit the decline of values	Limit the loss of power	Limit market loss	Limit the loss of social capital	Instinct

Table 11: Comparison of motivating factors and goals of the threat source

Threat source	Targeted objective End goal	Type of attack Strategic objectives	Attack scenario Operational Level
Authoritarian state	Acquire a strategic attack vector	Subversion of critical infrastructure	Deployment of stealthy, persistent malware in the supply chain
Aggressive company	Obtain a monopoly in a market	Influence of the regulator	Corruption of a decision maker
Mafia	Development of illegal activities	Extortion	Spread of ransomware

Table 12: Examples of end goals that may apply to an ARTS

Characterization and assessment of threat source capabilities

The capability of the threat source is the ability to perform a certain action. It expresses the intellectual and material resources that it is able to mobilize and combine to produce effects on the targeted resources. These may be pre-existing or developed resources for this particular attack, or resources provided through support.

To refine the description of the threat source, the capabilities can be subdivided along the following lines, by projecting onto the stratified model of the space:

- Into several operational categories, on each of the strata (physical, anthropic, digital), including:
    - Logistics capabilities that manage the coordinated provision of necessary resources
    - Intelligence capabilities that provide information essential to preparing and conducting operations

  - The defensive capabilities required to protect the resources used by the attacker in the attack
  - Offensive capabilities that execute the attack

- Into types of resources to be activated, on each of the strata (physical, anthropic, digital), including:
  - Doctrine: set of principles and best practices that guide the threat source's activities
  - Organization: how human resources are arranged to perform all activities (logistics, operations, intelligence, etc.)
  - Resources: quantity and quality (knowledge and skills) of the threat source's human resources.
  - Equipment: physical resources and facilities available to the threat source to conduct its activities.
  - Support: categories of external financial, material, intellectual or moral support for the threat source.
  - Training: how the threat source's human resources acquire and maintain knowledge (exercises, simulations, etc.)
  - Finance: financial resources that can be mobilized by the threat source

Using this taxonomy, it is possible to establish a capability graph that is contextual to the system under consideration, for each threat source.

Annex G: Risk scenarios - topological view

This annex provides a list of known threat scenarios and attack methods through the vignette approach and a functional breakdown. This list provides a knowledge base of the attack methods to consider.

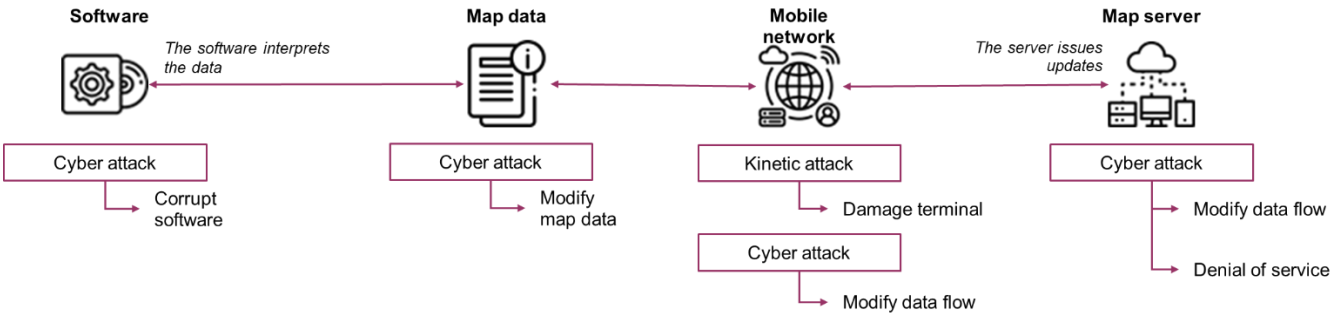
This list is not exhaustive and serves as a basis for the study of threats. It will be completed by taking into account the implementation of the ARTS, its technical design domain and its operational domain.

Define, monitor and control the vehicle trajectory

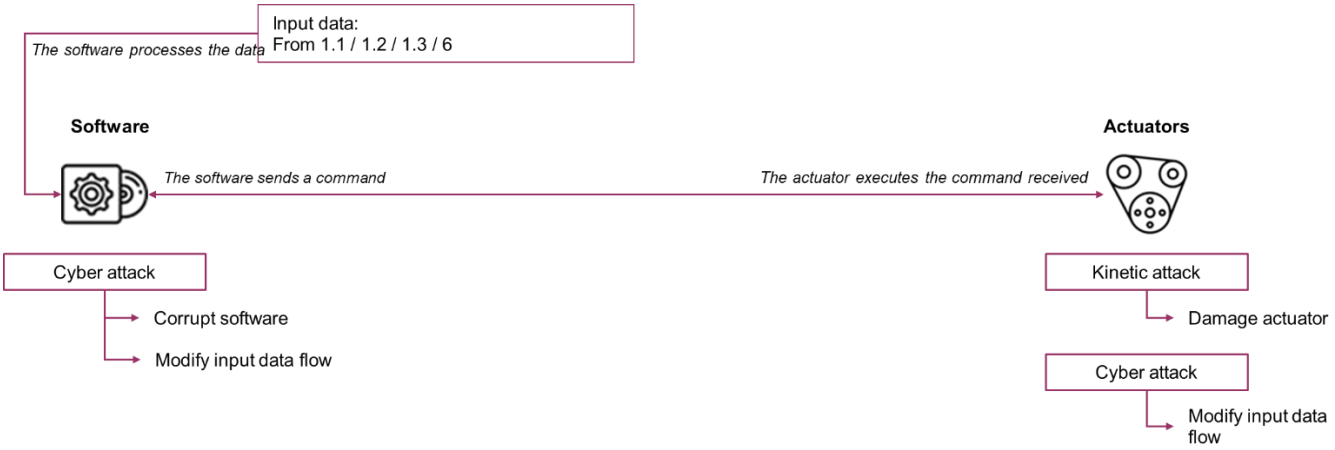
Vignette #1.1 Perceive

Vignette #1.2 Locate the vehicle on the route / area

Vignette #1.3 Make the decision about driving / guidance (plan)

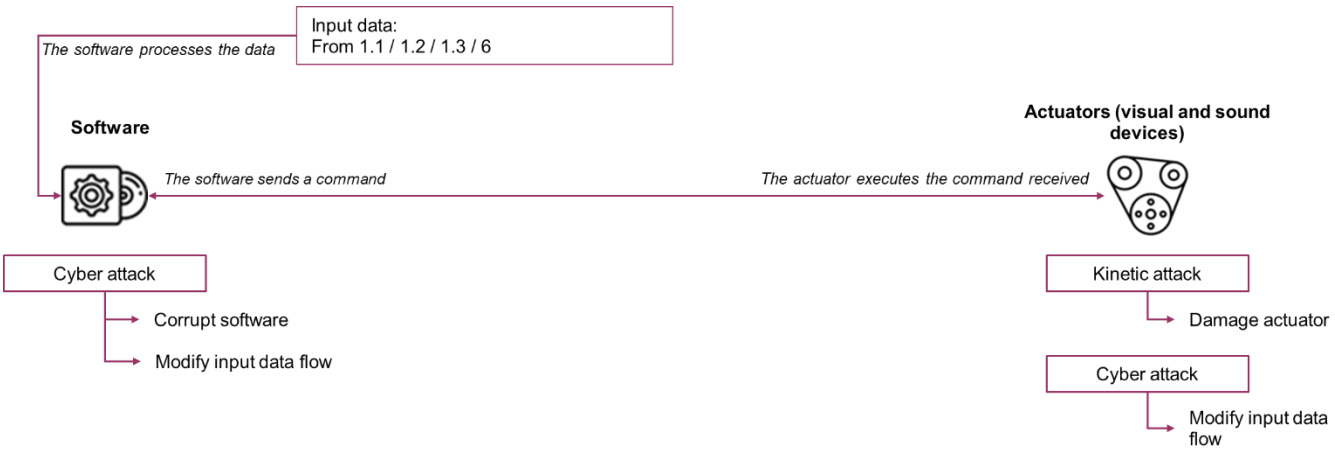


Vignette # 1.4 Perform dynamic control (act)



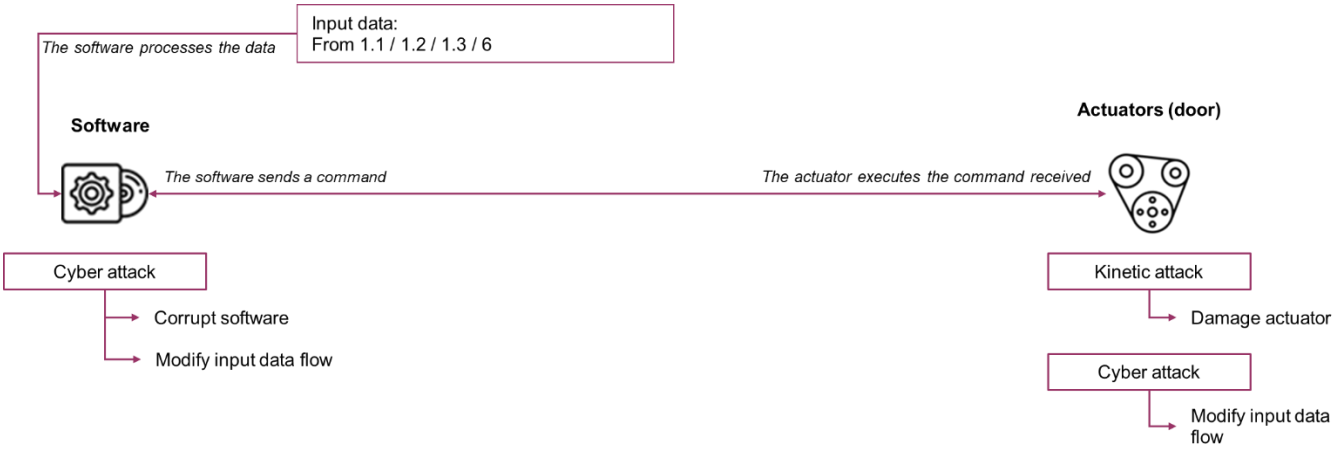
Signal to other road users

Vignette #2 Signal to other road users



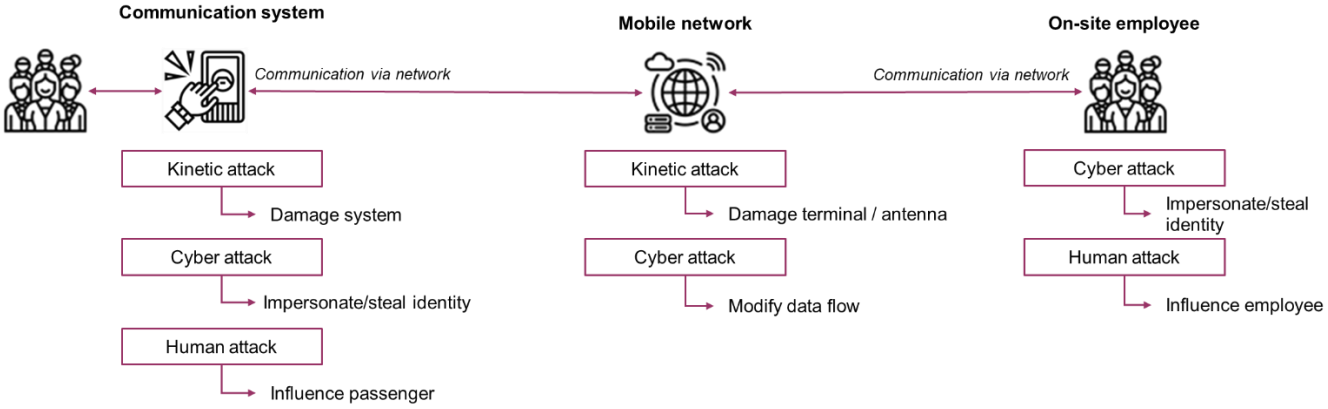
Manage access to automated vehicles

Vignette # 3 Manage access to automated vehicles

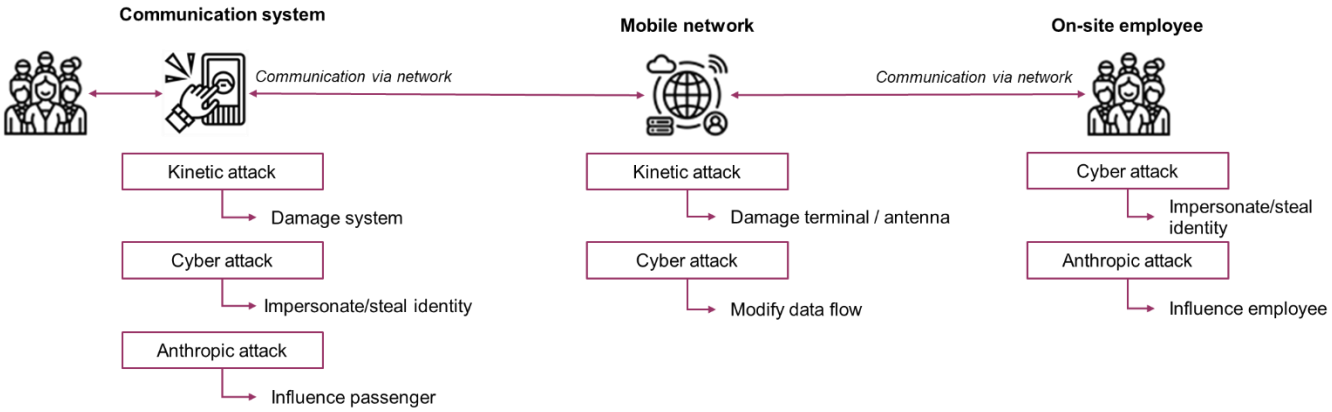


Enable users to interact with system components

Vignette #5.1 Enable communication between the operating personnel and passengers (COM)

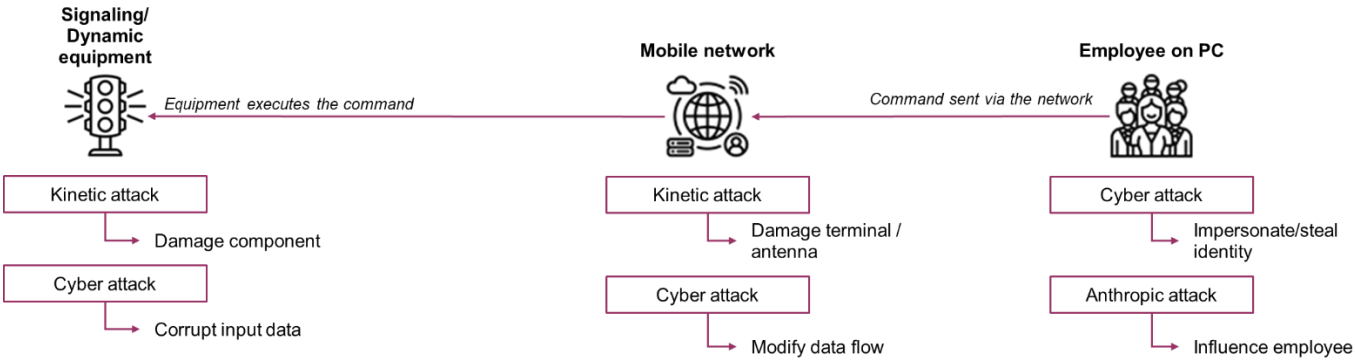


Vignette # 5.2 Provide users with access to services



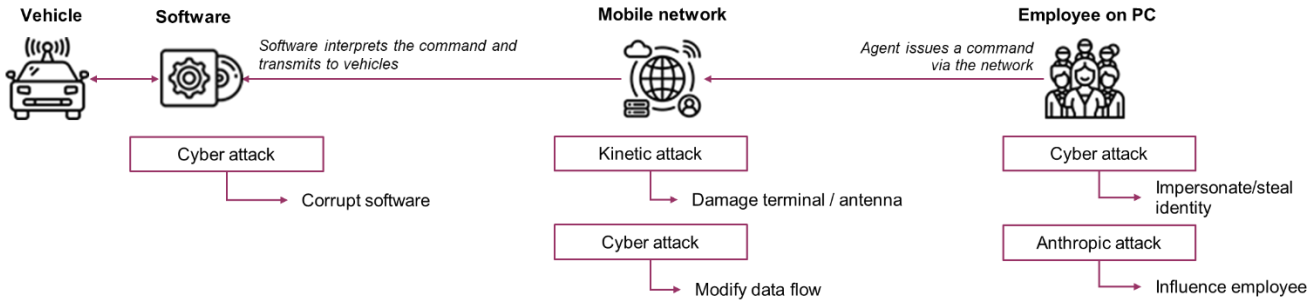
Manage dynamic infrastructure components controlled by the system

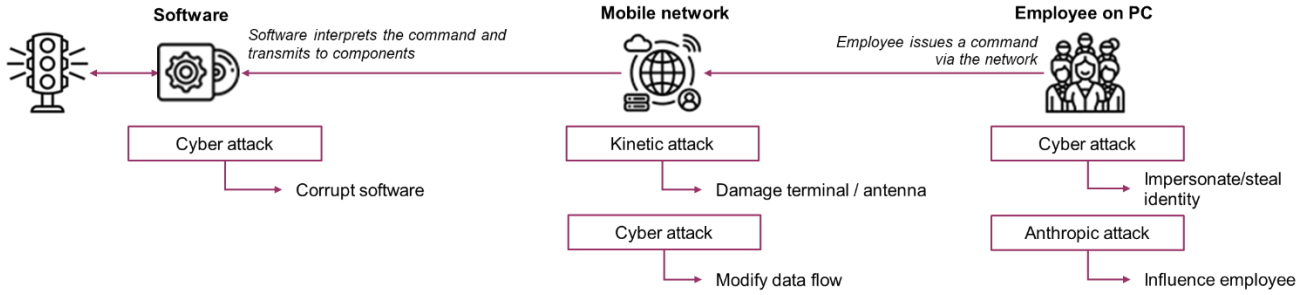
Vignette #6 Control dynamic signaling



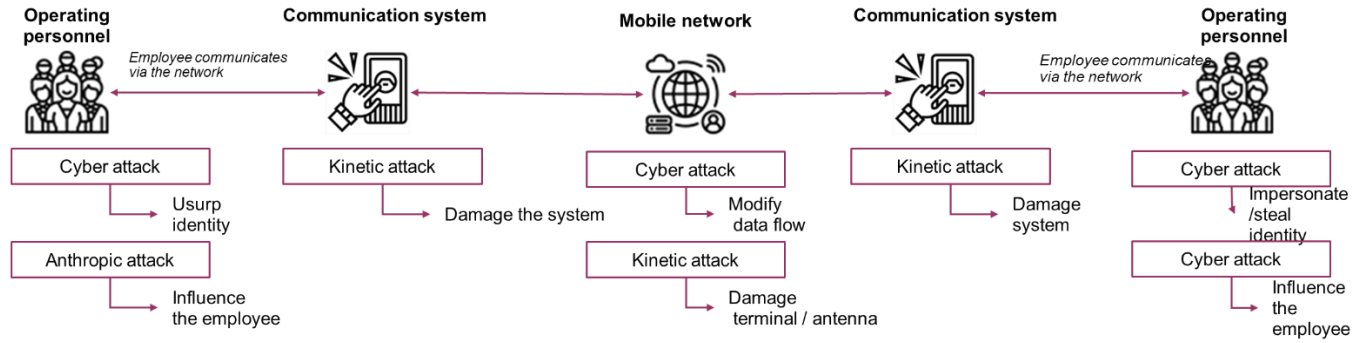
Ensure operation of the system

Vignette # 7.1 Intervene remotely on technical components of the system

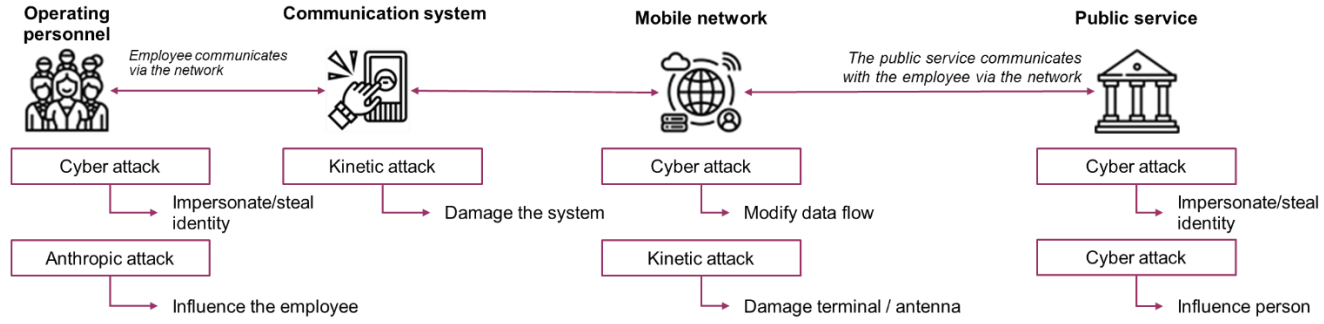




Vignette # 7.2 Enable communication between the operating personnel

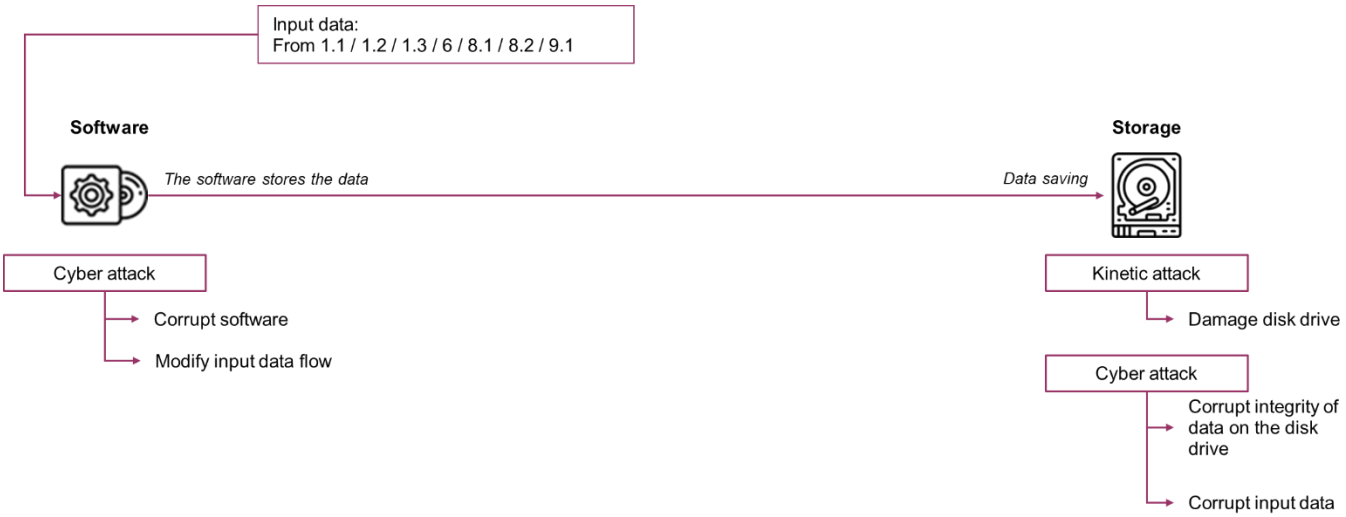


Vignette # 7.3 Enable communication between the system and external actors

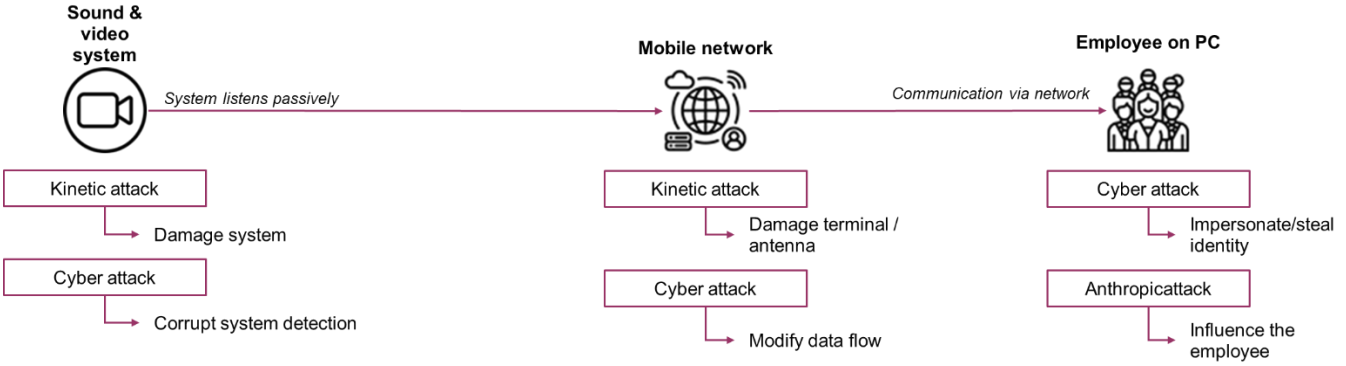


Vignette #7.4 Save data

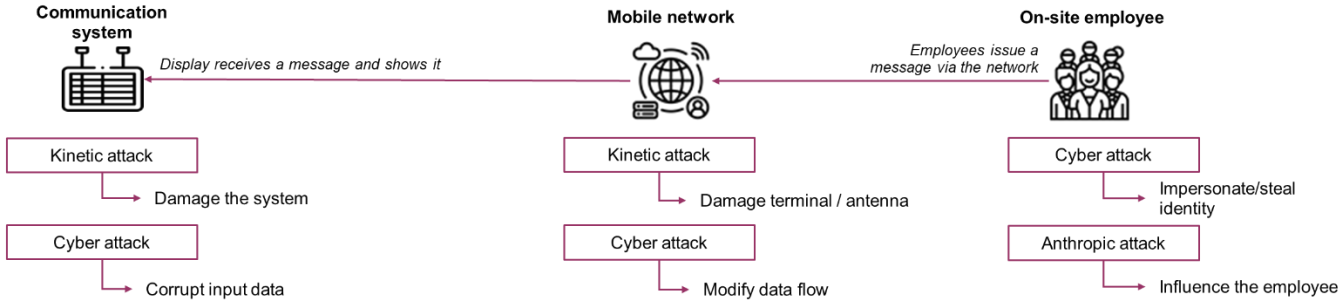
Vignette # 7.5 Inform about the status of the system components

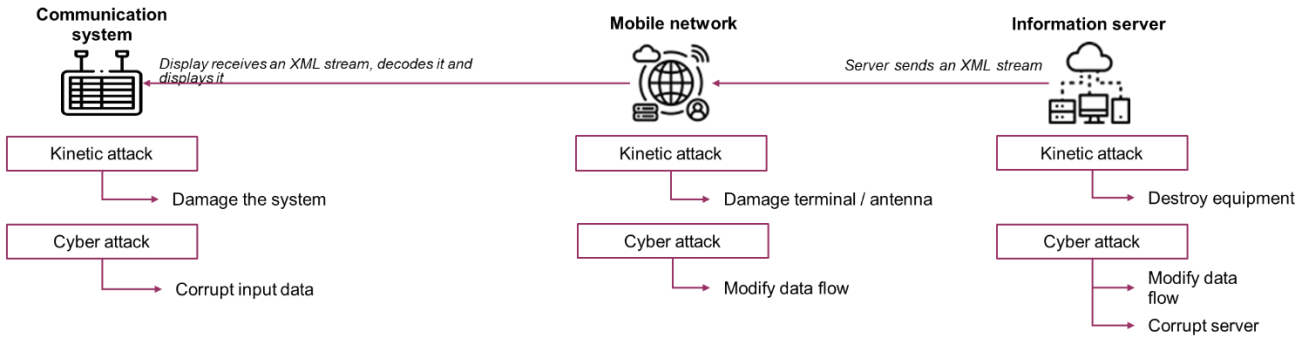


Vignette # 7.6 Enable the operator to see the situation in the vehicle



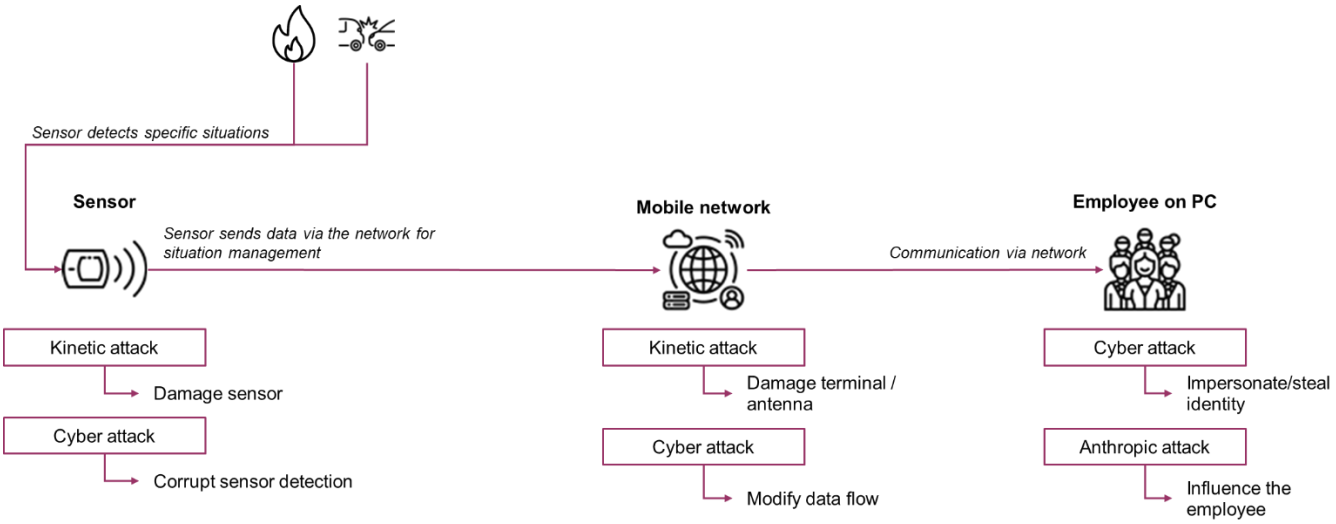
Vignette # 7.7 Enable information to be communicated to passengers





Detect and manage specific situations

Vignette # 8.1 Detect and manage specific situations



Ensure that the system is kept in safe conditions

Vignette # 9.1 Adapt operating instructions to traffic conditions

[Equivalent to vignette #1.4]

Annex H: Severity scale

The information provided below has been taken from bibliographic source [22], Technical Guide for GAME Demonstration for ARTS.

Below is a scale for rating the severity of an accident:

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

Table 13: Severity classifications

Use of this scale must comply with the conditions and requirements described in most recently published version of the Technical Guide for “GAME” demonstration for ARTS.

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 responsible for producing guides and standards/reference documents.

This document was prepared by the national ARTS CYBERSECURITY working group created by STRMTG, assisted by CONIX.

Director: François BRUN - STRMTG - Automated Public Transport Department
Secretary: Léo Maisonobe - STRMTG - Automated Public Transport Department
Project assistance: Sylvain CONCHON - CONIX, Samaad ALLADIN - CONIX

[List of WG participants]

SADIO BÂ	ANSSI
BRICE GILBERT	AFNOR
HEND HOUIMEL	AFNOR
PASCAL THOMAS	AFNOR
JEAN-MARC PAGLIERO	ALSTOM
JEAN-BAPTISTE RENAULT	ALSTOM
NICOLAS BONIAKOWSKI	BUREAU VERITAS
HAKIM NYAMPA	BUREAU VERITAS
DAMIEN DUCHASSIN	CEREMA
PIERRE-YVES TANNIOU	CEREMA
ARYLDO RUSSO	CERTIFER
TOILLIEZ THIBAUT	CERTIFER
LIONEL AUBERT	CETU
SÉVERINE BESSON	CETU
ERIC CHARLES	CETU
ELSA LANAUD	DGITM
ROMAIN DUPONT	EASYMILE
ARNAUD MOTTE	EASYMILE
JULIEN BURLET	GENDARMERIE
STÉPHANE MILET	GENDARMERIE
ARNAUD KAISER	IRT SYSTEMX
SAMUEL BELLANCA	KEOLIS
JULIEN TIN	KEOLIS
MARINE BRAULT	LSTI
ARMELLE TROTIN	LSTI
SAMMY HADDAD	OPPIDA
JEAN CAIRE	RATP
MBAYE SANKHE	RATP
ALEXANDRE AUBRY	STELLANTIS
STEPHANE GERONIMI	STELLANTIS
FRÉDÉRIC LENTI	STELLANTIS
MICHAEL BAKADAL	TRANSDEV
MICHEL DELHOM	TRANSDEV
NICOLAS DESMOINEAUX	TRANSDEV
JEAN CASSOU-MOUNAT	TRANSPOLIS
GUILLAUME MARTIN	TWINSWHEEL
VINCENT TALON	TWINSWHEEL
VIRGINIE DENIAU	UGE
LÉO MENDIBOURE	UGE
RAFAEL DE SOUSA FERNANDES	UTAC

SADIO BÂ	ANSSI
FABRICE HERVELEU	UTAC
YACINE LADJICI	UTAC
VÉRONIQUE DELEBARRE	SAFERIVER
ELENA TUSHKANOVA	SAFERIVER
PIERRE JOUVE	STRMTG
JEAN-MICHEL PASSELAIGUE	STRMTG
YVES SCHNEIDER	STRMTG
FLORENT SOVIGNET	STRMTG
ANISS ZIAD	STRMTG
BRICE GOMBAULT	SECTOR

Ludovic BRUN, STRMTG, also contributed to the review of this guide.