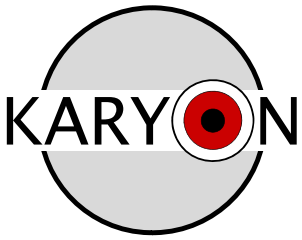

Kernel-based ARchitecture for safetY-critical cONtrol

KARYON

FP7-288195

D1.1 – Requirements Specification

Work Package	WP1		
Due Date	M5	Delivery Date	2012-04-24
Main Author(s)	Pedro Costa (GMV)		
Contributors	José Ricardo Parizzi (EMB), Rolf Johansson (SP), Elad Michael Schiller (CTHA), Oscar Morales (CTHA), Renato Librino (4SG), António Casimiro (FFCUL), Joerg Kaiser (OVGU), Siavash Aslani (4SG)		
Version	V1.2	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Requirements, use cases		

Part of the Seventh

Framework Programme

Funded by the EC - DG INFSO

Version history

Rev	Date	Author	Comments
V1.0	2012-02-29	Pedro Costa (GMV)	Document release.
V1.1	2013-04-18	Pedro Costa (GMV)	Update following first year project assessment review.
V1.2	2013-04-24	António Casimiro (FFCUL)	Final review and delivery.

Glossary of Acronyms

2G/3G/4G	Second/Third/Fourth-generation (wireless telephone technology)
ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance Systems
ADS	Air-Data System
ADS-B	Automatic Dependent Surveillance – Broadcast
ASIL	Automotive Safety Integrity Level
ATC	Air Traffic Control systems
ATM	Air Traffic Management systems
BSA	Basic Set of Applications
CAM	Co-operative Awareness Messages
CSMA	Carrier Sense Multiple Access
DAB	Digital Audio Broadcasting
DAL	Design Assurance Level
DbW	Drive-by-wire
DENM	Decentralized Environmental notification Messages
DME	Distance Measurement Equipment
DOW	Description of Work
DVB	Digital Video Broadcasting
EASA	European Aviation Safety Agency
E/E	Electrical or Electronic
ESC	Electronic Stability Control
ETSI	European Telecommunications Standards Institute
FAA	Federal Aviation Administration
I2V	Infrastructure to Vehicle
INS	Inertial System
ITS	Intelligent Transport System
G5	5 GHz communication for ITS
GBAS	Ground Based Augmentation System
GPS	Global Positioning System
LDM	Local Dynamic Map
LKAS	Lane Keep Assist Systems
LOS	Level of Service
MAC	Media Access Control

MS	Mobile Slotted
NM	Nautical Miles
OEM	Original Equipment Manufacturer
PASA	Preliminary Aircraft Safety Assessment
PICS	Protocol Implementation Conformance Statement
PSSA	Preliminary System Safety Assessment
RNP	Required Navigation Performance
RTIS	Real-time Traffic Information Systems
SIL	Safety Integrity Levels
STDMA	Self-Organizing Time Division Multiple Access
T-DMB	Terrestrial Digital Multimedia Broadcasting
TVRA	Threat, Vulnerability and Risk Analysis
UAS	Unmanned Aerial Vehicle
V2I	Vehicle to Infrastructure
V2X	Vehicle to Infrastructure or Vehicle
V2V	Vehicle to Vehicle
VANET	Vehicular Ad Hoc Network
VOR	Very high frequency Omni-directional Range
VTL	Virtual Traffic Light

Executive Summary

This deliverable contributes to the main KARYON objective, which is stated in the Description of Work (DoW):

"The key objective of KARYON is to provide system solutions for predictable and safe coordination of smart vehicles that autonomously cooperate and interact in an open and inherently uncertain environment."

The work in WP1 contributes to this overall objective by analysing use case scenarios in the automotive and avionic domains and deriving requirements to be considered in the remaining project activities. As stated in the DoW:

"The main objectives in this work package are to analyse the two demonstration scenarios under consideration in conjunction with the safety concepts being studied and derive a set of requirements. These requirements will form the necessary basis to the project and therefore must take into consideration the nature of the demonstrator scenarios, one avionic, the other automotive as well as the constraints associated with those two domains. Additionally a secondary objective is the detailed definition of the demonstrator use cases, taking into consideration the requirement set described above."

The activities in WP1 have started in the beginning of the project and will continue until month 18. The initial work, whose results are reported in the present deliverable, was devoted to produce a description of the considered use cases and requirements for safety (in relation to the particularities of each use case), as well as to identify an initial list of generic requirements, which are relevant when aiming for the safe coordination of autonomous and cooperative vehicles in general. These generic requirements are important for the provision of system solutions and for the definition of a design pattern that may be applicable in general, but with different instantiations in each case. However, this work needs to be done in close relation with architectural work and with the definition of system, fault and environment models, which are part of WP2 activities. Therefore, WP1 extends until month 18.

The deliverable is divided into five separate sections:

- Introduction – This section will provide the introduction to the KARYON concept
- Background and Terminology – This section will provide a description of the background as well establish some common terms for the project.
- Use Cases – This section will describe the two use cases used in the proof of concept of the KARYON concept.
- Requirements – This section will provide a generic description of a use case applicable to several transportation domains, as well as define the requirements for the concept.
- Methods of Validation – This section will provide a brief introduction to the methods through which it is intended to validate the KARYON concept.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Context and Problems

One of the emerging trends in future transportation is an increasing collaborative environment and vehicle interaction. Each year, automobile manufacturers strive to increase safety and road safety awareness through the use of autonomous sensory and decision capable systems embedded in the vehicles. The Avionics domain continuously improve safety through the use of increased sensor and communications systems which allow for a more capable decision making on the part of the pilots and ground support personnel. Unmanned Aerial Systems/Vehicles are becoming more and more one of the key units for border surveillance, fire detection or search and rescue, among other applications.

However, despite the continuous improvements regarding the amount and accuracy of the information obtained through sensors and communication networks, there are many challenges yet to overcome before it will be possible to allow the roads and air space to be shared between fully autonomous and human driven vehicles. In particular, there is a fundamental safety problem that arises when considering cooperative scenarios in which entities rely on external information, obtained from other entities through wireless communication networks. The existing and typical approaches for designing safety-critical systems, which use strict design rules and are based on worst case assumptions and pessimistic mechanisms for guaranteed (to a certain level) behaviour, are hardly applicable in these scenarios.

In cooperative scenarios we need different solutions. We face an extremely difficult to solve problem: on the one hand, the benefits of exploiting information coming from remote sources are substantial and obvious. They extend the range and quality of environment perception. On the other side, incorporating this information to control the mobile entities raises severe safety problems because of the inherently less predictable wireless communication, the difficult to assess trustworthiness and age of this information and other uncertainties emerging from such a cooperative scenario.

Understanding this performance-safety trade-off is key to achieve a reasonable solution, one which can be used to secure the needed safety without sacrificing performance and without requiring too conservative safety margins in normal, fault-free, system operation. KARYON proposes to explore this performance-safety trade-off, developing concepts and technologies for safe cooperation.

We envisage autonomous mobile systems, vehicles like cars, robots or aircrafts, which rely on sensory information for perceiving the state of their surrounding environment and being able to derive the correct control decisions. Additionally, we expect these systems to be able to cooperate with the purpose of obtaining additional sensory information, provided by other systems typically in the vicinity. Given that these vehicles operate in shared physical environments and, in particular, they are potentially in contact with humans, it is fundamental to ensure that their operation is safe with respect to their own integrity and to the integrity of the surrounding systems and humans. At each moment, the rules that dictate the allowed behaviour of such an autonomous system depends, at least, on the concrete state of the surrounding environment, on the range and accuracy of the perceived state, and on the health of the system components. It is always necessary to ensure, by construction, that a minimum level of service (or functionality) is available to exclude hazardous situations, while it should be possible to admit various levels of service, corresponding to different situations and combinations of environment state, perception quality and component integrity with respect to failures.

In this deliverable we describe the initial work that was done with the purpose of identifying the requirements that are in one hand generic, and common to the generality of autonomous mobile systems that we briefly described above, and on the other hand specific, as they are not appropriate for systems in general, but only for the considered systems. This allows us to reason in generic terms and to propose solutions that may have a wider applicability and are not constrained to one or two specific scenarios. However, for the purpose of exercising these generic requirements, our work also encompasses the analysis of specific use cases, deriving particular requirements that should have a relation with the generic ones.

This can be illustrated by the following figure:

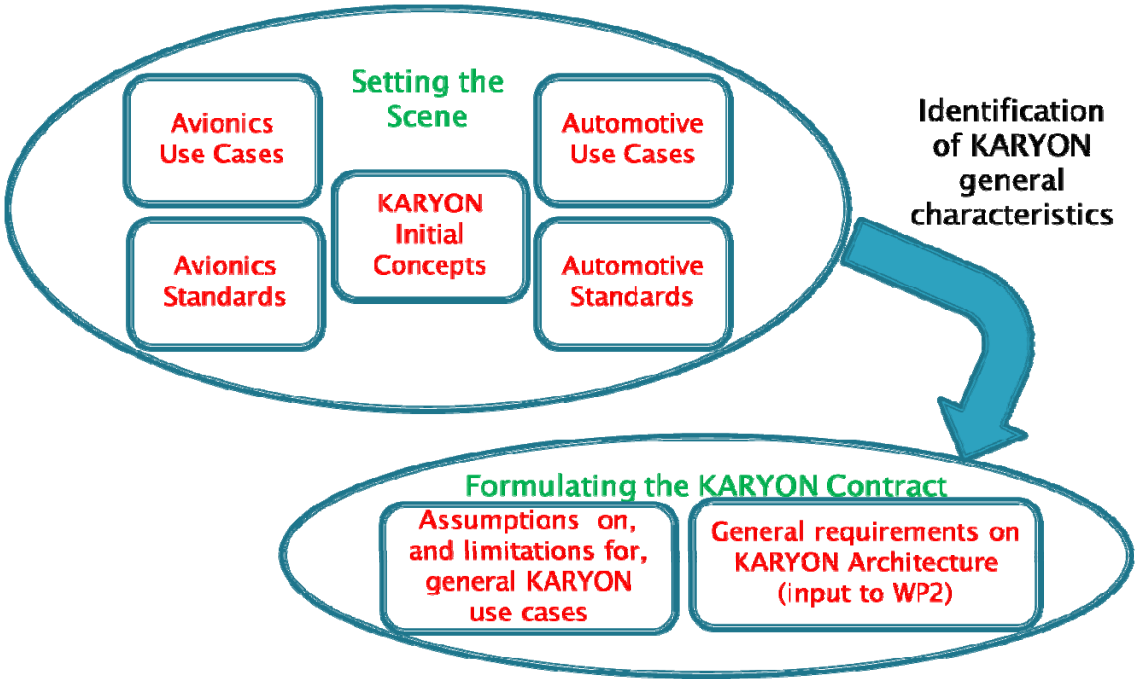

Figure 1 – KARYON characteristics

Then, the structure of the deliverable naturally derives from this work and approach. In the next section we provide some fundamental background, definitions and terminology, which are needed to clearly understand the subsequent parts of the text. This is what in the figure is summarized as KARYON initial concepts. After that we analyse and provide a detailed description of the two use cases in the avionics and automotive domains, also elaborating relevant implications from the standards on functional safety applicable to the respective domain.

Finally we extract a general definition of KARYON use cases and also the requirements this implies for any KARYON architecture to fulfil the needs in the use cases. The idea is to make possible a general exploitation of the KARYON results. The aim is to be able to claim that a system that fulfils the results of the KARYON project is sufficient for to solve any KARYON use case. Hence it is important to conclude criteria both for a general KARYON Use Case and for a general KARYON Architecture. In short: “A KARYON architecture is sufficient for every KARYON use case”.

1.2 State of the Art

The bounds for critical systems are directly linked to the domain where these systems are used. For this project the key concept is autonomous vehicles so we will focus primarily in vehicle safety critical systems, connected to the capacity of vehicles to operate autonomously.

Currently the architectures for the safety critical systems analysed are based on the level of consequences that the failure of such systems may entail. For high criticality systems, these architectures tend to be inflexible and are generally constrained using very tight bounds in terms of safety margins. This leads to a very safe condition but has performance impacts.

In automotive these systems are primarily aimed at those components or subsystems whose failure may lead to occupant death such as brakes or steering, In the avionics industry, given the potential result of an in-flight failure, most of the functional systems are of the highest criticality. To ensure this, not only the systems are subject to a very stringent certification policy, where extensive testing is conducted but also to prevent the complete failure of one of these systems, component redundancy is added. This leads to an increase on weight and power consumption onboard the aircraft but ensures that the possibility of occurrence of a catastrophic failure is negligible. The current scenarios where fully autonomous cooperative vehicles operate are very few and the operations are performed with very tight and precise safety measures factored in.

With a projected increase of vehicles in the two domains considered, the avionics and the automotive and with an ever increasing necessity of optimisation of the traveling areas, studies have been performed in the fields of improving and enhancing the vehicular loads in the roads and air space respectively. The SESAR program in avionics is one of a number of programs aimed at this objective. It is envisaged that as more and more vehicles occupy the travel lanes and with the increase in automation that more autonomous vehicles commence to appear and to be used. This leads to the need of an increase on the cooperation between these vehicles and in an improvement on the communication and decision making capabilities inside the vehicles.

1.3 Beyond State of the Art

In most cases the safety boundaries ensuring the safety of the systems are specified with tighter limits than the actual necessity. This is due to the worst case scenario approach which drives the safety architectures. As the architectures are not flexible, this leads to performance degradation, as mentioned previously. This is due that in the majority of the situations, the vehicles are in an optimal scenario which is far less stringent in terms of safety boundaries than the worst case. By taking advantage of a more flexible architecture it is possible to improve the performance of the vehicle operations without compromising the safety of the whole system.

The capability to fly UAVs in non-segregated airspace is a hot item currently in the international market. Both the FAA and EASA have been involved in the work needed to certify UAVs for this type of flights with advances expected soon. The architecture proposed is expected to increase the safety of the overall vehicle platform while reducing the certification costs associated with avionics programs. This would certainly contribute to the effort required in the certification needs and assist in the future certification standards referring to the sharing of airspace between commercial human-piloted aircrafts and UAVs.

Autonomous and cooperative capabilities are a main research and development topic for all leading automakers. Volvo, for example, is aiming for an autonomous vehicle by 2020. Several automakers, such as Scania and Volvo, have prototyped vehicle platooning and they are looking for a way to certify these innovations via the standardization bodies, see ETSI efforts on cooperative ITS. In the context of KARYON, some of the key obstacles of cooperative vehicular systems are: (1) insufficient ability to deal with a non-constant number of sensory

events under a variety of noise models, (2) insufficient ability to use timed communication among vehicles, and (3) the insufficient ability to deal with the uncertainty of complex control systems in the presence of system and communication failures. KARYON expected progress beyond the state of the art is the study of the problems above.

2. Background and Terminology

This deliverable is about the definition of use cases and general requirements for KARYON's architecture. Given that in KARYON we are concerned with dependability and safety aspects in particular, and we envisage solutions that will involve the need for some flexibility and adaptability to handle the intrinsic uncertainties affecting the operation, we first introduce the relevant definitions and terminology in these areas. The objective is to ensure that all used concepts are made clear before they are used in the remaining text. In fact, the definitions introduced in this section are relevant not only in the specific context of this deliverable, but we aim at using them consistently throughout the entire project.

In this section we also provide background on standards that are relevant in the context of KARYON. As it will be described, there are many existing and in development standards, for instance in the area of intelligent transportation systems, and therefore an important work is to identify a subset of relevant standards, from which implications might be derived when developing the KARYON architectural and system solutions.

2.1 Relevant definitions of established concepts

Dependability is an overarching concept integrating such attributes as reliability, availability, safety, integrity and maintainability [2]. The purpose of this section is to define the basic terms and their relation with respect to the objectives of KARYON.

KARYON strives for building systems that guarantee a safe behaviour in a specified operational context. The objective is that malfunctions of the electrical or electronic (E/E) components should not lead to a dangerous behaviour of the system. This is related to functional safety as e.g. defined in the ISO 26262 [1] standard as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems which controls a physical artefact like a car or an aircraft. There is a performance and a safety aspect related to the operation of a system designed for safety. The performance aspect includes all mechanisms aimed at maintaining the highest possible system functionality, i.e. preventing a fault by constructive means or maintaining correct system operation in the presence of faults by imposing the respective fault-tolerance measures. The safety aspect is concerned with preventing dangerous system behaviour. Because in KARYON we focus on fail operational systems, these systems need to maintain a certain performance level to guarantee safe behaviour. The respective performance-safety trade-off is discussed in the KARYON proposal. In the following we will briefly introduce the basic terms and notions of dependable systems relevant for KARYON as they were defined in [2] and discuss their relationship.

2.1.1 Dependability threats: Faults, errors and failures

Faults, errors and failures are the threats that affect correct component operation where a fault is the origin and potential cause of a malfunction. If it is activated e.g. by accessing or operating a faulty component, it may cause an error which represents an incorrect state. If an error remains undetected and is not corrected, it may in turn lead to a failure that occurs at the interface of a component and is defined as an incorrect service of the respective component.

It should be noted that:

1. A failure always constitutes a violation of the specified service of a component while a fault and an error may be handled by the respective means inside the component and thus are within the specified component behaviour.

2. A failure may be propagated to another component or to a higher level where it may manifest as a fault. This is expressed by the notion of the fundamental chain of dependability threats in [2].

Additionally, an informal analysis and classification of hardware faults with respect to safety is also presented in Appendix B of the ISO/DIS 26262 standard [1].

2.1.2 Dependability aspects

Dependability has multiple attributes or aspects. **Reliability** is a survival attribute and describes the probability of continuous operation. **Availability** relates the mission time to repair time and represents the probability of a correctly functioning system at some point in time. In the context of availability, **maintainability** plays an important role in that it defines the ability to undergo modifications and repair. **Safety** is defined as the absence of catastrophic consequences on the user(s) and the environment. Safety is in the focus of KARYON and therefore we deal with this attribute in more detail below. In particular, while reliability and availability are properties of the components of the E/E system, safety will be defined in an operational context and thus has a more complex and subtle relationship to the system threats introduced above. **Integrity** has a broad scope and is defined as the absence of improper system state alterations. Integrity is a prerequisite for reliability, availability and safety. However, depending on the target dependability goal, the respective countermeasures to handle failures and maintain integrity may be very different.

In the automotive area, the consequences of faults are expressed in terms of hazards and risks. A **hazard** is defined as the potential harm (physical injury or damage to the health of people) that can be caused by an artefact. A component failure, if not treated adequately, may eventually lead to a hazard. **Risk** relates the probability of occurrence and the severity of the effects of a hazard. In the context of automotive and avionics safety, hazards are classified according to their severity, their probability of occurrence and their controllability leading to the concept of *Automotive Safety Integrity Levels* (**ASIL**) or in avionics software *Design Assurance Level* (**DAL**). This is presented in more detail in the section about standards.

2.1.3 Security

Security is strongly related to dependability but has a different focus. Security is defined as the absence of unauthorized access to, or handling of, system state. This includes multiple aspects as unauthorized disclosure of information (confidentiality), unauthorized change of information (integrity) and stopping or slowing down authorized access to information (availability). The fault model for security particularly copes with faults originating from intended malicious attacks to the system. It is obvious that security threats will have a substantial impact on system safety. Although not in the main focus of KARYON, security issues will be part of the fault and threat analysis because KARYON deals with a networked system which bears the possibility of attacks from outside the system.

2.1.4 Functional safety

KARYON will measure its effectiveness mainly in what is referred to as functional safety. In general, **functional safety** limits the scope of safety to what is caused by the functionality of the system under consideration. In the automotive domain this is expressed as “absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems [1] .” In the avionics domain, safety is tightly linked to the occurrence of a failure and the potential results of such failure. It is generally defined in a five level result, from catastrophic to negligible.

For instance, one of the key safety requirements for the avionics domain, harmonized between the FAA and EASA may be described as:

"25.1309 Equipment, systems, and installations

(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed and installed so that:

(1) Each catastrophic failure condition;

(i) Is extremely improbable; and

(ii) Does not result from a single failure.

(2) Each hazardous failure condition is extremely remote; and

(3) Each major failure condition is remote.

(c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. A warning indication must be provided if immediate corrective action is required. Systems and controls, including indications and annunciations must be designed to minimize crew errors which could create additional hazards" [3]

In fact, the view of functional safety is differing between domains and safety standards. While the automotive industry has the entire functionality in scope, there are other standards like DO178B/C [4] and IEC61508 [5] that further confine the scope to safety functions. There, functional safety refers to the ability of a system to operate without failure by means of specific preventive or corrective actions. These actions are controlled and actuated by what we will refer as safety functions.

An example may be an anti-freeze detection device, which detects the possibility of a vehicle's brake to be frozen and actuates specific heating components to defrost the brakes, or a distance assurance actuator which triggers the automobile brakes if the distance to the vehicle in front is reduced drastically. Of course, triggering the brakes may also increase the likelihood of an accident if the vehicle in the rear is too near or does not break in time. Therefore, by increasing one level of safety through the use of a given safety function, we may be decreasing its safety in another function. Careful balance in these functions must be assured and will be considered in the solutions developed in KARYON.

In IEC61508, one of the concepts linked to safety functions is the **Safety Integrity Level** [SIL]. SIL is commonly described as the level of probability in the reduction of risks provided by a safety function. In the automotive domain the safety integrity levels are called ASIL (automotive safety integrity level), and they are attributes to the safety requirements. This means that for each safety requirement the ASIL levels tell how sure one has to be that that very safety requirement can be fulfilled.

ASIL is measurable in 4 levels, with level A as the lowest and therefore the one least dependable in terms of safety assurance, and D, the highest and the one with the most stringent requirements. KARYON is striving to meet ASIL D integrity level in the automotive and its equivalent in Avionics. For additional information on ASIL please refer to Section 2.2.

Although security is not considered in the scope of the project, at least for the avionics domain, some care must be taken. One of the key concepts in KARYON is a fully or near-fully automated vehicle control approach. Access to the control elements from outside sources need to be safeguarded to some degree of security in order to avoid potential hazardous situations outside the command of the legitimate ground operator.

As concerns the automotive field, security is not in the focus of KARYON, but it should be addressed because malicious attacks are a possible cause of failures. The detection of wrong information due to any cause is a key issue for the functionality of KARYON architecture.

In the Avionics domain, this security is even more paramount. The possibility of an external entity taking control and guiding the vehicles under consideration must be safeguarded. The communication and control channels must be assured to be secure at all times, with the safety kernel playing a large part in the detection of unauthorised access and rejection of invalid commands.

A brief analysis of these aspects is expected in further WPs but no detailed study is expected in the current scope of the project.

2.1.5 Level of service

The definition of Level of Service (LoS) is in general linked to a given domain or area of operation. The broader term for LoS refers to the commitment to perform an action or set of actions within a time frame in response to an external stimuli or internal trigger.

Level of Service may be measured in terms of dependability metrics, such as the ones described in Sections 2.1.2 and 2.1.3, that is, reliability, availability, integrity, safety, etc. But it can also be measured, alternatively or in addition, in terms of other attributes, namely performance ones. In KARYON we are interested in the dependability and performance dimensions, while the security dimension, although important in general, will not be the main focus of the work. We provide some concrete examples of Level of Service specifications below.

In general, the higher the Level of Service required in terms of any of its attributes, the higher the associated cost of the system. If considering safety requirements alone, the more stringent they are, or the more disastrous the result of a service failure (as in the case of the avionics domain), the costlier is the end product. Therefore the objective of any manufacturer is to provide the highest possible LoS at an acceptable cost. Many of the onboard avionics equipment are deployed with multiple redundant copies to ensure very high reliability levels, but such equipment is very costly.

The concept of level of service is today present in the automotive field mainly by the notion of so called limp-home mode. That means that when a critical functionality of the car has found itself not reliable enough, the ability to manoeuvre is reduced. In the limp-home state the intention is that the driver should be able to safely continue to a repair-shop, even though much functionality, such as achieving higher speed, is not available. In the KARYON context we are looking at different levels of service for highly automated functions.

The measurement of level of service could be an innovative approach to deal with automotive cooperative systems, because in this case the infrastructure operation and the information coming from other vehicles strongly impact on the vehicle functions.

Let us consider a “virtual traffic light” example, realized by car-to-car communication. The decision of what vehicle to pass the crossing (see Figure 2), when and at what speed, is fully done by the vehicles without involving the drivers.

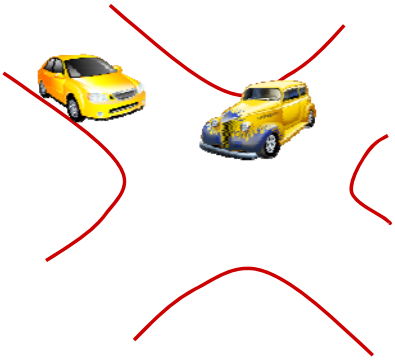

Figure 2 – VTL Road Crossing

In such an example, the level of service can be linked to two factors: speed of each vehicle and the distances between them. These two lead to a derived factor, which is the time it takes for a vehicle to cross the intersection. Level of service in this example, can therefore be linked to the average speed which a vehicle is moving when passing the crossing, compared to the average speed it could have in ideal realization of the virtual traffic light. A lower level of service here means that there are some margins, which may make sense from a safety point of view.

High LoS can be categorised as ensuring that the speed reduction for the vehicle is minimal (compared to the ideal case), as well as that the time it takes to cross the intersection is also small. Medium LoS may be represented by a significant reduction (compared to the ideal case) of traversing speed and also by taking longer to cross the intersection, while low LoS can be defined as the slowest speed for crossing and the longest time required, as depicted in Figure 3.

Figure 3 – Low LoS VTL Road Crossing

Note that the LoS here is related to the ideal realization of the functionality. This means that the average speed value that is considered as high level of service may depend on the number of other vehicles crossing the intersection. Lowering the LoS means inserting more margins than required in a perfectly ideal case where all cars have perfectly (100%) accurate data about all other cars coordinates, velocities and intended behaviours.

This implies that for delivering the highest level of service, considerations need to take into account the sensory capabilities of the vehicles, both internal and external, as well as the factored reliability of those same sensors and their data.

In the avionics domain, some of these sensors can be as diverse as GPS signal reception and processing or internal inertial guidance. Further external control communication channels may

not be accessible for a given time frame and this leads to the necessity for the system to be able to balance high performance with high safety.

In conclusion, in the use case scenarios that will be described ahead in this deliverable, the considered LoS can be linked to a set of attributes, both dependability- and performance-related, and to respective measurements. For instance, speed of vehicles, distance between vehicles, distance to objects in the overall environment, and others. For each of these measurements, a degree of assurance must be factored in. This degree of assurance will be linked to the level of service possible: the higher the degree of assurance, the higher the LoS possible.

2.2 Standards, scope and focus

This section will provide a brief description of the standards which have relevance to the KARYON concept. The two selected domains, automotive and avionics have distinct standards and we will identify those in the following sections. We will also strive to reach a common understanding between the automotive and the avionics standards.

The standards presented here will be taken into account when designing the project but it should be noted that they are only presented in a support role for the design and may not be completely followed due to time and effort constraints.

This section is also only an introduction to the standards and serves as a starting point in the analysis regarding standards which is expected in next deliverable of this Work Package.

2.2.1 Standards relevant to KARYON

On the basis of the automotive application area addressed by KARYON, the communication, information and security standards under development by ETSI, that has been committed with the EC mandate M/453 on cooperative ITS, should be considered as a reference for KARYON. In addition, functional safety is a key issue for the project, so the standards related to these subjects have been particularly examined.

ETSI EN 302 665

This standard identifies the scenario considered for ITS, and covers the communication architecture of the various stations, including the vehicle communication sub-system, which has to be taken into account as a reference for the definition of the KARYON architecture.

ETSI TR 102 638

This standard defines BSA (Basic Set of Applications) mainly focusing on V2V, V2I and I2V communications in the V2X dedicated frequency band. However, it does not exclude using other access technologies such as cell networks, e.g., 2G, 3G, 4G, and broadcasting systems, such as DAB, T-DMB, and DVB.

The Basic Set of Applications includes several applications:

- Driving assistance – Co-operative awareness
- Driving assistance – Road hazard Warning
- Speed management
- Co-operative navigation
- Location based services
- Communities services

- ITS station life cycle management

Among them, the basic applications concerning Active Road Safety are of some interest to KARYON, because they are more related to vehicle dynamics and to dynamic information exchange among vehicles and with the infrastructures.

ETSI TS 102 637-2

This standard specifies the Cooperative Awareness Basic Service, which provides by means of periodic sending of status data a cooperative awareness to neighbouring nodes. Quality requirements are also proposed for this mandatory facility in order to provide reliable component performance for application development. In particular the following quality requirements are specified:

- Timing Requirements
- General Confidence Constraints
- Message Format Specification

These requirements are of relevance to KARYON, because they provide the background for the representation of the status that will be necessary to define the functionalities of the applications considered in the project and to develop the KARYON architecture.

ETSI TS 102 868-1

This standard provides the Protocol Implementation Conformance Statement (PICS) proforma for Conformance test specification for Co-operative Awareness Messages (CAM) as defined in TS 102 637-2 in compliance with the relevant requirements and in accordance with the relevant guidance given in ISO/IEC 9646-7.

This standard is of relevance to KARYON due to its deep view of protocol implementation and of the detailed information on message contents, which allows identifying the status and the manoeuvres of the neighbouring vehicles.

ETSI TR 102 863

In co-operative Intelligent Transport Systems (ITS), the Local Dynamic Map (LDM) is a key facility element which supports various ITS applications by maintaining the information on objects influencing or being part of traffic.

The ITS architecture identifies the LDM to be a key function within the ITS station facilities layer. Co-operative Awareness Messages (CAMs) and Decentralized Environmental notification Messages (DENMs) are important sources of data for the LDM. Moreover, a Basic Set of Applications (BSA) is defined, which can be realistically deployed in a time frame of about 3 years after the end of their standardization. The applications are defined in ETSI TR 102 638 (see above).

Information held in the LDM is classified into four distinct types:

Type 1: permanent static data usually provided by a map data supplier:

- includes information about the road topography, road attributes (such as speed limits and functional road class) and points of interests. It describes static information on real world objects.

Type 2: transient static data obtained during operation:

- includes information about roadside infrastructure such as position of gantries and traffic signs. It describes information of the real world with a quasi-static behaviour.

Type 3: transient dynamic data:

- includes information about road works such as position, lane width, speed limits and incidents. It describes information of the real world with a dynamic behaviour having influence on traffic efficiency.

Type 4: highly dynamic data:

- includes information about ITS stations within the vicinity such as vehicles and dynamic traffic signs. It describes information of the real world with a highly dynamic behaviour having mainly influence on traffic safety and some influence on traffic efficiency.

Several LDM functionalities are relevant to KARYON, since they support co-operative awareness, such as:

- Emergency vehicle warning
- Slow vehicle indication
- Across traffic turn collision risk warning
- Merging Traffic Turn Collision Risk Warning
- Co-operative merging assistance
- Intersection collision warning
- Co-operative forward collision warning
- Lane Change Manoeuvre

The current status of in-range ITS stations information item in the LDM maintains the identification, position, speed and other dynamic information received from all vehicles within ITS G5 range of the host station. It comprises the following elements:

- Vehicle identifier
- Vehicle type
- Acting as emergency vehicle
- Vehicle dimensions
- Vehicle speed
- Yaw
- Acceleration control
- Ambient air temperature
- Traffic-affecting hazard cause
- External lights on
- Rout navigation advise
- Vehicle occupancy
- Traffic signal priority
- Door open indicator
- Current road curvature
- Front wiper setting

- Crash status
- Dangerous cargo

Local Dynamic Map service is relevant to KARYON, because it deals with information needed to perform several functionalities, while KARYON aims at dealing with uncertainties affecting the validity of similar information.

ETSI TR 102 893

This standard summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) operating in a fully deployed ITS.

This standard is relevant to KARYON, because the vulnerabilities of roadside ITS stations and of vehicle stations can impair vehicle safety, if proper countermeasures are not taken.

The standard recommends several countermeasures, and these can provide the background when considering in KARYON the definition of fault models.

ETSI TR 102 862 V1.1.1 (2011-12)

This report describes the use of time slotted MAC algorithms in VANETs. Two specific MAC methods, self-organizing time division multiple access (STDMA) and mobile slotted Aloha (MS-Aloha), are described in detail, not excluding other time slotted approaches. Time slotted approaches are suitable for road traffic safety applications as the maximum delay is predictable and channel access can be made fair among all participating nodes even during broadcast. However, time slotted approaches do require synchronization between nodes to build a common framing structure for transmissions, something that is not needed for non-time slotted approaches, e.g., CSMA that is used by ITS G5.

This report addresses a topic that is related to communication predictability, which is in the focus of KARYON. KARYON could give inputs for the standardization in that field of what can be achieved without the use of access to a global timing or positioning systems, as the STDMA and MS-Aloha require.

ISO 26262

As mentioned in the DoW, the new ISO standard 26262 will be taken as a reference for the research conducted in KARYON.

Since this standard covers the whole product lifecycle from the concept phase to the commissioning phase, and also the general management systems of the companies involved in product development, both OEM and suppliers, including the supporting processes, the standard is not fully applicable to KARYON, which is more focused on on-board architecture issues. For this reason only some parts of the standard can be considered as a reference for KARYON, and especially the following:

- Part 3: Concept phase
- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
- Part 10: Guideline on ISO 26262

It has to be noted the Part 4 (Product development at the system level) is touched by KARYON, and this part could be applied only for specific activities related to the safety measures that will be analysed in KARYON and to the testing activities that will be required for the verification of the results achieved.

RTCA DO-178B/C
Software Considerations in Airborne Systems and Equipment Certification

This standard defines the required conditions and steps needed to ensure safety when designing software for the avionics domain. It covers the entire lifecycle of the software development process from requirements to final certification processes. It does not cover the E/E hardware necessities.

RTCA DO-254
DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE

This standard is the companion standard to the DO-178B/C since, as 178B/C defines the safety for the software process, the DO-254 covers the E/E hardware safety considerations. With both DO-178B/C and DO-254 the software and hardware required conditions are defined for the avionics domain.

ARINC 653
AVIONICS APPLICATION SOFTWARE STANDARD INTERFACE

This standard defines the standard interfaces and expected behaviour of software functions developed under an IMA architecture. The IMA architecture is the current avionics architecture devised to reduce weight, power consumption and on-board loaded hardware processing components, as well as to increase the number and functionalities of on-board applications. This architecture has steadily replaced the previous federated architecture. A discussion on these architectures is expected in further deliverables.

2.2.2 Automotive and Avionics similarities

This section will provide a brief comparison between the automotive, ISO-26262, and the avionics, RTCA DO-178B/C and DO-254, standards considered. It is not intended to provide a definitive conclusion but to provide an introduction on the similarities and differences between the two standards.

SIL is mainly applicable to automotive domain. Avionics is not subject to SIL specifications, to our understanding. In fact, avionics usually define safety/criticality through several standards (RTCA-DO178B/C is one, DO-254 another). In pure software terms, RTCA-DO178B/C's Design Assurance Level (DAL), defines the safety level through the effect a failure will have on an aircraft. This effect is measured in what may be referred as a criticality scale, where the higher the criticality, the higher the safety requirements will be.

The five levels and its effects are defined as:

Hazard Class	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities

Figure 4 – Avionics hazards

Safety is well addressed in the automotive field. The recently introduced ISO 26262 will be the reference standard for the next years.

According to this standard, safety in defined as "the absence of **unreasonable risk**", where a risk is judged as unreasonable when it is "unacceptable in a certain context according to valid societal moral concepts".

Therefore, hazard analysis and risk assessment is the starting point to develop the automotive systems, to determine the "automotive safety integrity level" (ASIL), and the safety goals for each hazardous event.

The standard provides quantitative targets for the maximum probability of the violation of each safety goal due to random hardware failures. One of the possible sources of target data is the following:

ASIL	**Random hardware failure target values**
D	$< 10^{-8}\ h^{-1}$
C	$< 10^{-7}\ h^{-1}$
B	$< 10^{-7}\ h^{-1}$

The target shall be met over the operational life of the vehicle.

According to ISO 26262, degradation concept is implicitly considered in terms of safety goal and safe states in the case of failure, but a measure of degradation (in terms of levels) is not included in the standard, certainly because the standard is related to safety and not to performance.

The mapping of degradation of service to ASIL is not a direct task. In fact ASIL is linked to functions and to the associated risks. If the level of service is an information provided to the vehicle system and therefore it is external to the vehicle system, and if the vehicle system,

which makes use of that information, has to be ASIL D (for hypothesis), the system has to be ASIL D whatever is the information and also the information has to be provided with ASIL D.

Regarding a scale to classify the severity of the consequences of a hazard, an example is given by the ISO standard:

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 and less than 10% probability of AIS 1-6 Damage that cannot be classified safety-related	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5-6
Informative examples	Bumps with roadside infrastructure Pushing over roadside post, fence, etc. Light collision Light grazing damage Damage entering/exiting parking space Leaving the road without collision or rollover	Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with very low speed Side collision with a passenger car (e.g. intrudes upon passenger compartment) with very low speed Rear/front collision with another passenger with very low speed Collision with minimal vehicle overlap (10-20%) Front collision (e.g., rear-ending another	Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with low speed Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed Rear/front collision with another passenger car with low speed Pedestrian/bicycle accident while turning (city intersection and streets)	Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with medium speed Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed Rear/front collision with another passenger car with medium speed Pedestrian/bicycle accident (e.g., 2-lane road) Front collision (e.g., rear-ending another vehicle, semi-truck, etc.) with passenger compartment deformation

		vehicle, semi-truck, etc.) without passenger compartment deformation		

To determine the ASIL level of a safety goal, it is also necessary to consider the probability of exposure in the specific hazardous event and the controllability of the vehicle. Precise rules are given by the standard to derive ASIL from the combination of severity, probability of exposure, and controllability.

The concept of risk is generally understood as a combination of the severity of an accident and its probability. Depending on the safety standard, the exact definition may differ a bit.

By comparing ASIL and DAL definitions, similarities are noticeable. A S3 class hazard in the automotive standard is equivalent to a catastrophic hazard event in the avionics standard. Similarly S2 is similar to hazardous or major.

Both the automotive and the avionics domains require hazard/risk analysis in design time for the embedded components but with differences. The avionics requires that all the components to be analysed and certified (based on each component's criticality level) at design prior to any flights to take place, whilst the automotive takes into account that some components inside the vehicle cannot a priori interfere with the safety of the automobile and require no qualification of those components. In some sense it is similar to the DAL E certification of some components inside the aircraft, but with the notion that even though the components are DAL E they still need to have to be certified.

The concept of certification and qualification is also a difference. Automobiles, in general, require qualification (some of the components may be certified but not all need be) while aircrafts require certification (all components need be certified). Qualification is typically considered less stringent in terms of constraints than certification. Qualification of a product is linked to "it has at least this capacity" while certification is "it has exactly the capacities it states it has". Certification also requires an accredited third party (the external entity certifying the systems and platforms) while qualification is usually performed only by the manufacturer.

In Europe, the main certification body for aeronautics is EASA, and no aircraft can fly in non-segregated airspace without prior certification for flight. In the automotive field the vehicle to be driven in public roads should receive the "Type Approval" i.e. conformity statement of the product according to specific technical regulations (e.g. European regulations or ECE/ONU regulation) issued by national authority (e.g. Italian department of transport, Vehicle Certification Agency in UK). This "type Approval" is also applicable to some of the components of the automotive, such as lights, windscreen and engines. There are specific safety requirements included in the "Type Approval" specification (regulation) concerning the components internal to the vehicle (e.g. Crash, Electronic Stability Control, other ADAS systems). This "type Approval" is the exception to the qualification mentioned previously when referring to automotive.

Automobile's qualification is somewhat less stringent and therefore some of the activities performed in qualification of an automobile may prove insufficient when applied to an avionics program. Regarding the functional safety the application of ISO26262 requirement for the automotive is voluntary (although important to reduce the risk of issues of product liability) while the application of DO-178 or DO-254 requirements for safety of software or hardware is mandatory for the aircraft.

3. Use Cases

This section will define the two scenarios used to prove the concept of KARYON. These scenarios will be primarily based on a set of range scale considerations, given the nature of each scenario (vehicle based). The first subsection provides an introduction to the unit values and spatial/temporal definitions which will drive the use case scenarios.

The second subsection will define the two scenarios used to prove the concept of KARYON. The domains selected for this proof are the automotive and the avionics domains. Each of these scenarios will be composed of four separate sections:

- A high level description of the use case, including a description of the vehicle in question, a tentative identification of the type of sensors, both internal and external that can be used and a brief depiction of the surrounding environment.
- A preliminary identification of the main functionalities required. These will serve in the identification of relevant requirements.
- Based on the two sections above, identification of the safe and unsafe conditions possible as well as the means through which those conditions may be met.
- The fourth and final section strives to define requirements specific for each use case.

The two scenario use cases will be the basis for the test case definitions used in the proof of concept of the KARYON project. From each of the scenarios it is expected to be extracted the various test case needed to validate the concept behind KARYON. Section 5 will provide a brief description in the validation methods employed for the validation of the concept.

3.1 Scale considerations

As mentioned in Section 2.1.5, one of the factors used in Level of Service determination is the distance between vehicles. This refers to a given spatial scale and will be further described in the next section. However, distance per se, is not a sufficient factor to ascertain if a hazardous situation may occur. We need to consider the predictability of such a hazard to happen and factor it, not only in preventive functions but also in corrective functions. This leads to the necessity to define a temporal scale of events and from it deriving the recommended and minimum allowed time to reactive functionalities. These times and the associated hazard analysis are mainly connected to the level of service of each situation.

In automotive, a time scale has been traditionally considered, e.g. milliseconds scale for real time control, fractions of seconds scale for manoeuvring, higher scale for planning. However when introducing functionalities where the level of autonomy is varying, as may be the case when Level of Service varies, the time scale for requested driver reaction may also vary a lot. Onboard systems traditionally comply with these scales in terms of requirements regarding processing speeds, control cycles, OS, etc. To give an idea, a typical automotive real-time control loop of chassis systems is scheduled with 1 ms period, while engine control is based on engine revolution time base. 50 ms can be an acceptable reaction time for functions involving driver interfacing and can be directly perceived by him/her.

In avionics the temporal scale considered for safety purposes is variable. Usually the time units “increase” the further away from the ground and other aircraft each aircraft is and “decreases” otherwise. This is generally associated with time to reaction purposes on the part of the pilot manning the aircraft where if the aircraft is at high altitude, it is considered to have more slack for corrective measures, while at lower altitude, the risk of crashing the airplane increases and therefore corrective measures must be taken faster. Although these time constraints are not

standardised, generically, main control loops for secure functions run in times between 5 and 30 milliseconds with less critical functions allowed to execute every minute.

Distance between vehicles is a key measurement when discussing level of service and safety. Time to react is directly linked to the relative speed of the vehicles and to the distance between them if we consider them to be in the same path.

The following figure describes a typical avionics minimum distance separation area for a given aircraft. Should another aerial vehicle breach this distance it is considered a potential safety hazard and corrective actions need to take place. Considering a manned vehicle, these actions are subject and approved by an air traffic controller on the ground as well as by the pilot in the aircraft.

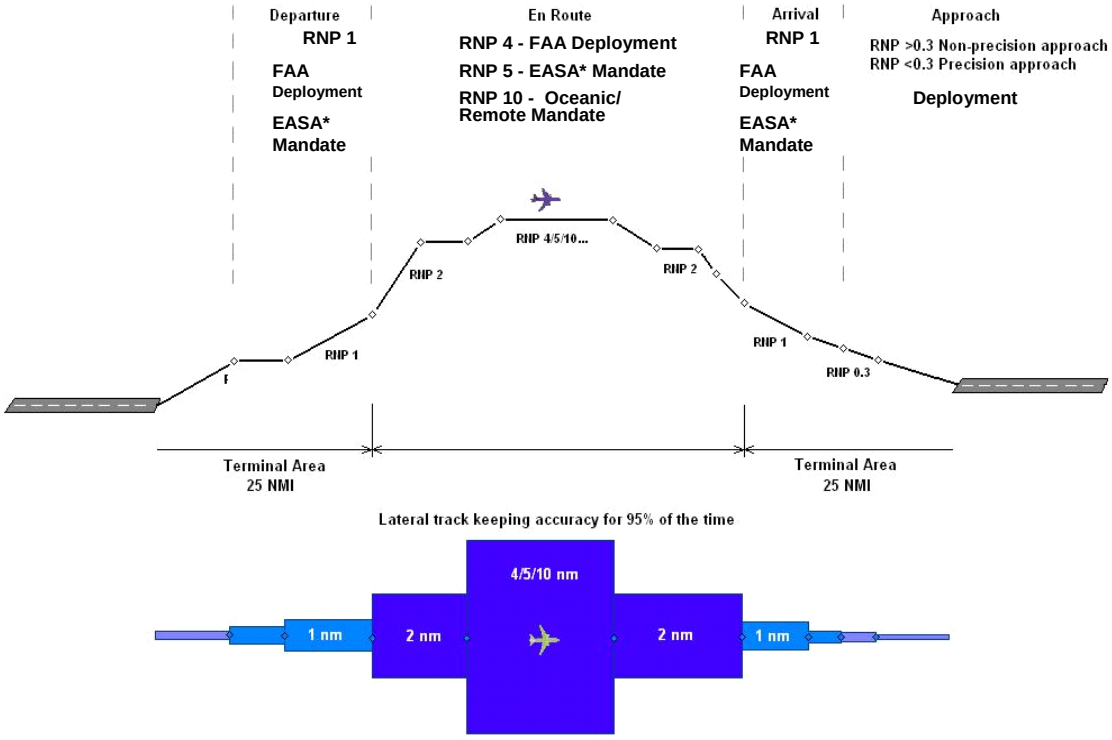

Figure 5 – Avionics safety separation standards

As can be seen for the avionics domain, the minimum separation distance is not a fixed value throughout all the flight phases.

For adaptive cruise control (ACC) the reasoning is rather similar. For a typical ACC the driver sets both the preferred speed and the safety distance to the vehicle in front expressed as number of seconds. In the general case, the minimum safety distance between cars is defined as the minimum distance where the vehicle can safely stop itself without endangering anyone or impacting in other vehicle. Of course this is very subjective and very dependent on the whole environment. An example is, when the road is wet from rain, this minimum safety distance increases in value due to the necessity of a longer breaking space. Additionally, speed is also a factor to take into consideration. The higher the speed, the larger the space needed to safely stop the vehicle.

These considerations will be taken into account in the use case definitions as well as in the definition of the generic concept validation.

The possibility of hazards occurring in vehicular domains, are based in various conditions. Distance between vehicles, relative path and direction of vehicles, time needed for each vehicle to reach given points based on the relative speed of the vehicles…

These factors can be determined with more or less accuracy a priori given a certain scenario. The determination of these factors is based on external and internal sensor capabilities, communication channels and data merging capabilities on-board the vehicles. In addition to this, estimation of how trustworthy is each of these measurements is also of paramount importance.

The surrounding environment will affect the determination of how safe is the vehicle and how swiftly preventive or corrective actions can be decided and taken.

In the automotive domain, this will be based on the number of other vehicles surrounding a given automobile, relative speed and direction, and distance between all of them. Similarly changes of direction, additional impediments in the road, such as road blocks, fallen debris or just potholes can and will make decision making more complex.

For the avionics domain, some of these factors are not taken into consideration as we do not anticipate having physical barriers in the air. However, as the relative speed of vehicles in the air is generally higher than in the ground, a shorter decision time or longer detection distances need to be determined in order to ensure a similar degree of safety.

As noted above, one factor to take into consideration is the accuracy of the position determination for all the vehicles. In a perfect world the position of any vehicle can be determined instantly and with an absolute accuracy and therefore it does not have an impact on the safety considerations needed for calculating the overall safety of a scenario.

However when considering actual operating scenarios we need to take into consideration the error factor associated with determining a vehicle's position. This error will add an uncertainty factor to the position of each vehicle. One of the roles required of the safety mechanisms is to ensure that this uncertainty is kept to a minimum and based on the determination of this uncertainty, to specify the Level of Service for each vehicle.

To determine the Level of Service, external and internal sensors as well as communication channels are considered. Through the merging of the information collected by the sensors and the data received through the communication channels, calculating the position of a vehicle as well as a rough estimation of the error factor associated to that position (how trustworthy is the data) can be accomplished and a Level of Service specified for the vehicle.

3.2 Automobile use case definitions

3.2.1 Description

Safety-related failures of vehicles can lead directly to accidents involving to the loss of human life and property. Contemporary vehicles include more than 70 microprocessors that regulate many safety critical actuators. The flexibility afforded by the microprocessors has led to increased functionality at the cost of greater complexity. Analysing the system's safety-related properties is correspondingly more demanding. Even a basic control procedure can have a large state space that hide important errors and limit the opportunity for formal verification. Drive-by-wire (DbW) technology can possibly improve safety at the cost of greater complexity and redundancy requirements. Such systems include more microprocessors than the contemporary vehicles. A key problem with DbW is that their large complex software is hard to verify, which may lead to a runaway vehicle. Since not all unsafe states can be discovered during the system development, it is imperative to assert the safety-related properties during the vehicle operation.

The automotive industry seeks to enhance vehicle functionality, in addition to transportation. Future vehicles will communicate with each other and form networks that will provide useful safety information, guidance through traffic congestions, reduce energy consumption and CO2 omission, as well as social entertainment and business advertisement.

In order to sustain these functionalities, vehicles will have thousands times more the computing power that they have today. Computer chips will cost pennies and they will be embedded everywhere; on the road, inside the vehicles and all around us. With this prospect technology, the automotive industry is the next place to be revolutionized. For example, collision avoidance systems will use sensors to feel and see the road and give the driver heads up advanced notice that there is arriving object. The right-decision-making processes will occur on-board within a fraction of a second. The safety of these processes will depend on the system ability to coherently perceive its surrounding environment and the wellbeing of its subsystems.

The automotive scenario considered in KARYON is referred to the general one as the ITS environment addressed by the recent EU projects and also the scope of standardization by ETSI, as represented in Figure 6.

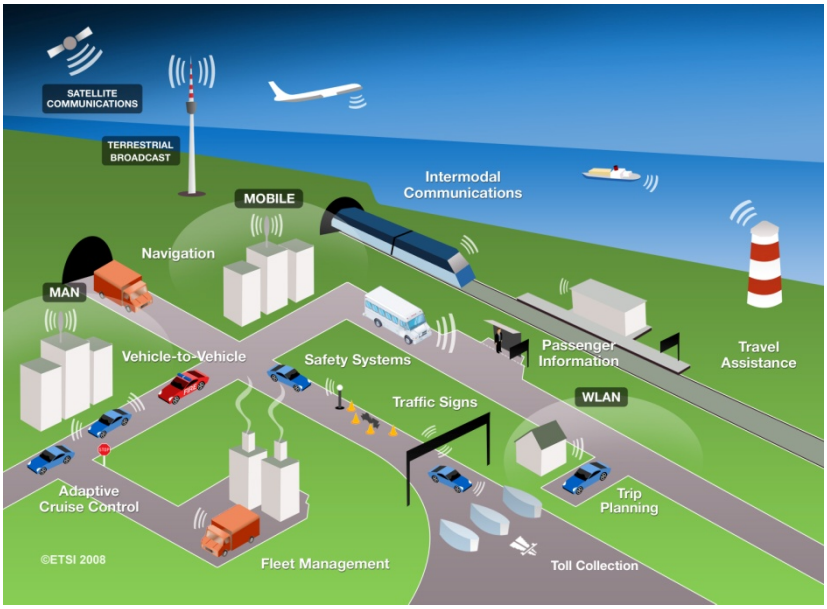

Figure 6 – The ITS environment (source: ETSI)

In particular, several communication, information and sensing systems are included, but without any limitation to specific technologies. However, at least the facilities and the equipment to provide cooperative driving functionalities are assumed to be available, in particular:

- V2V communication: ITS-G5, 60 GHz, IR
- Roadside stations: V2I and I2V ITS-G5
- On-board 77 GHz RADAR or/and LIDAR systems
- LDM service

As concerns LDM, it is supposed that the status in a certain area is provided to vehicles, according to the Local Dynamic Map concept reported in ETSI TR 102 863 (see the specific paragraph of this deliverable for the data provided by LDM).

Since the DoW of KARYON includes the study of automatic driving associated to Intelligent Traffic Light, a prerequisite of this use case is the availability of the complete and correct information about the presence of all vehicles in the intersection area, including those without any V2V or V2I communication system. For this reason, Collision Risk Warning RSU (Road Side Unit) is assumed available to detect the potential obstacles approaching the intersection area.

The communication architecture of the territory's ITS stations (roadside stations, central ITS stations) is assumed to be compliant with ETSI standards. Similarly, the onboard

communication architecture complies with ETSI standards, even if several implementations are possible, depending on the complexity of the onboard applications.

We plan to study a set of Advanced Driver Assistance Systems (ADASs) for coordinating vehicles and propose a set of solutions that increase their safety. In particular, we examine scenarios in which vehicles cooperate while: (1) going on the road and keeping their distance from other vehicles, (2) cruising in their lanes and coordinating when lane changes are needed and (3) crossing intersections in a coordinated way.

In addition to the three demonstrative use cases considered, we need to take into account the notion of Level of Service, discussed in section 2.1.5, and its effects in these use cases. Three scenarios are considered:

- Ideal conditions, with good communication capabilities, all vehicles cooperating and no faults occurring. This would be the optimal Level of Service.
- Fault conditions, where one or more of the sensor and communication capabilities are functioning sub-optimally or in failure. This would lead to a lowering of the Level of Service thus forcing the system to increase the safety measures needed to ensure a safe environment.
- Fault recovery conditions, where the failures occurring in the previous scenario are solved and the level of uncertainty raised by the faults is lowered. This would permit the raising of the Level of Service back into the optimal level, thus reducing the safety measures in effect, without compromising the overall vehicle safety.

The set of studied ADASs covers basic operations that allow the drivers to safely pilot their vehicles on the road:

Adaptive Cruise Control Systems

ACCs allow vehicles to slow when approaching other vehicle and to accelerate to their cruising speed when possible. These systems are important for accident prevention as well as for reducing energy consumption, because they smoothly adjust the vehicle speed and by that reduce the stop-and-go phenomena when the traffic contention is high. ACCs often incorporate with several other subsystems, such as Lane Keep Assist Systems (LKASs), Lane Change Assistance Mechanisms, Electronic Stability Control (ESC) and Real-time Traffic Information Systems (RTISs). Each of these subsystems relies on other subsystems and enabling technologies, such as Global Positioning System (GPS) and Vehicle-to-Vehicle Communication (V2V). In such a complex system of systems, the ability for monitoring the system wellbeing is essential.

The level of service for this use case is mainly the needed time margin between vehicles for meeting the safety goals. Higher level of service means a lower time margin between vehicles. For each level of service, and for each speed interval, the safety goals are different with respect their attributes of Automotive Software Integrity Levels (ASIL). This means that depending on the vehicles judgement of the integrity level possible to guarantee at a certain moment, the level of service can be determined. The integrity includes health status of sensors both on the actual vehicle and the vehicles in front as well as communication channels and computing resources.

The following three figures depict the situations explained.

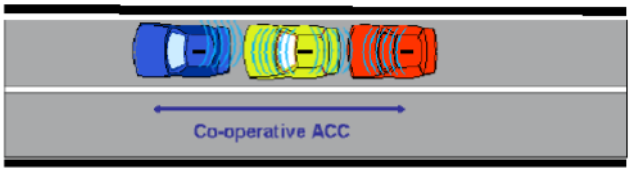

Figure 7 – Adaptive Cruise Control system

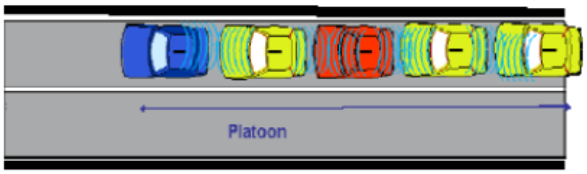

Figure 8 – Platoon driving using ACC

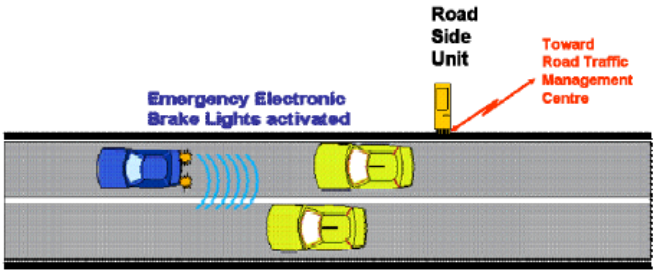

Figure 9 – Road side emergency signalling

A basic scenario implies several vehicles moving as a whole, based on each vehicles ascertaining its position and then broadcasting it to the other vehicles around it. The more accurate this position determination and the faster the communication, the higher the level of service are possible, without compromising the safety of the scenario. Of course this also must take into consideration the number of vehicles around it. The more vehicles, the more time will be needed to process the data and the lesser the LoS will be. One key factor will be a balance between the number of vehicles, or the radius of detection, and the distance between each vehicle.

In addition to each vehicle transmitting its position to the other vehicles in a radius around it, it must also be taken into consideration, the placement of sensors in the surrounding road. These may be detection based, in order to supplement each vehicles position broadcast or transmission based, to ensure that one vehicles broadcast covers a wider radius than the vehicle based transmitter is capable or prepared. This will help with future hazard predictions, such as a traffic accident a few kilometres up the road.

As described above the platooning manoeuvers will be based upon the Level of Service of each vehicle in the platoon. This LoS may not be homogeneous, i.e., there may be different Levels of Service in the various cars, given that not all the cars may have similar sensor capabilities, data merging capabilities or communication capabilities. This leads to a localised degradation of the Level of Service but it does not ensure that all cars have the same LoS.

Preliminary two Levels of Service can be specified for the ACC, one of true platooning where the higher assurance of the position estimation of each car along with the good communication capabilities between the cooperative systems, allows for a shorter distance between cars. The second Level of Service corresponds to worst communication capabilities which lead to what we may call cruise control, where distance between each car is increased. This increase is proportional to the factor of uncertainty in ascertaining the position of each car.

In order to validate the assumptions for this scenario, as well as the safety architecture correct operation, some validation criteria shall be used. Following are high level descriptions of the validation criteria:

In ideal conditions the vehicles will operate in the first level of service, maintaining similar speeds and a short separation distance between them.

In failure conditions, due to injected faults, the separation between vehicles should increase proportionally to the degree of confidence loss resulting of those faults. Additionally the traveling speed may be reduced to ensure greater safety, in case of total communication loss.

Recovery conditions, resulting from the removal of the faults injected into the system, shall lead to a reduction of the separation distance to values similar to the ideal conditions, over a period of time, and, if the overall speed had decreased, to an increase also back to the original values.

The means to validate the above criteria will be briefly expanded in section 5 and refined in the following WPs, particularly in WP 5.

Crossing road intersections using ITSs' traffic lights

One of the most fundamental components in contemporary Intelligent Transport Systems (ITSs) are the traffic lights that coordinate and monitor the crossing of intersections. When a traffic light system detects a critical failure in its components, it signals to the arriving vehicles that it is in an inoperative mode (i.e., blinking the orange light). While the traffic light is in failure mode, the drivers coordinate the crossing of the intersection by themselves. Future traffic light systems will periodically broadcast I-am-alive messages to the arriving vehicles. The arriving vehicles will monitor the reception of the I-am-alive messages. When the traffic light system is in an inoperative mode, the vehicles will switch to the use of a backup system: a virtual traffic light that relies on vehicle-to-vehicle communications for coordinating the intersection crossing. It is unclear whether a virtual traffic light that relies entirely on mobile ad hoc networking can provide the same dependability level as a traffic light system that uses stationary infrastructure. However, virtual traffic light can be literally deployed anywhere without the need for stationary infrastructure. Therefore, virtual traffic lights are likely to emerge as an important ITS technology. The KARYON project will develop a means that would facilitate the assertion of safety constraints that are related to virtual traffic lights.

The following figures depict the situations explained.

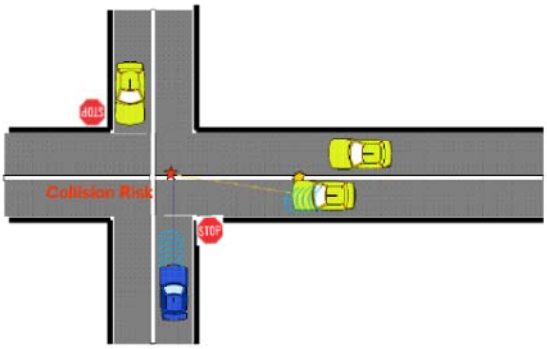

Figure 10 – Road Crossing collision risk

Figure 10 depicts a possible collision risk if no action is taken by any of the two vehicles. Each vehicle is merely checking for other vehicles in front as per the platooning rules in previous use case and is not aware of other vehicles crossing the intersection. Figure 11 depicts a warning forward transmission by a road side assistance component informing one vehicle of another approaching vehicle to the crossing.

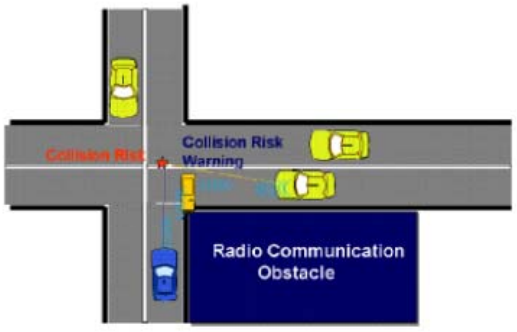

Figure 11 – Road Crossing collision detection

Figure 12 and Figure 13 provide a more complete view of the underlying logic with the use of virtual traffic lights to signal, which vehicles should cross and in which sequence.

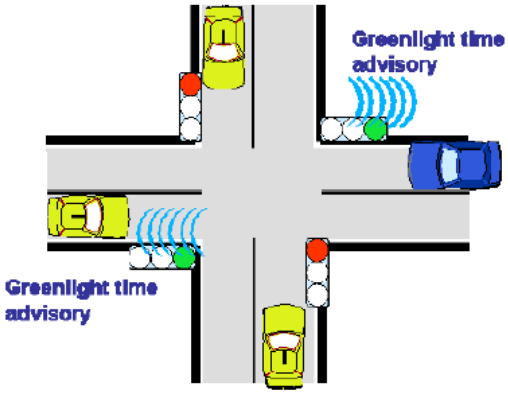

Figure 12 – Green light crossing signal

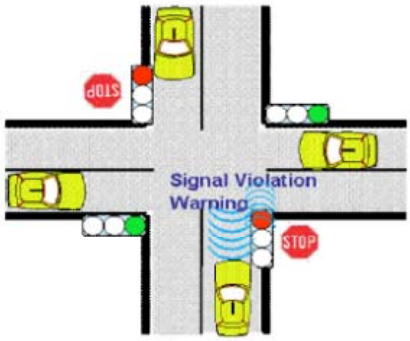

Figure 13 – Red light road crossing violation warning

The road crossing intersection scenario is based on communication primarily, as the sensor capabilities of each car are not sufficient on their own to ensure a safe crossing. These sensors are mainly aimed to detect other cars or obstacles in front or behind the car and not to the side from where a crossing vehicle may appear. In addition, cooperation is needed in case of direction change which forces a crossing in front of the car such as a car in front coming towards the vehicle intending to turn left on the crossing.

Two levels of service are specified for the crossing. The first is based on good communication capabilities which allow for the cooperative systems to agree with adequate advance on the approach each vehicle is to take when approaching the crossing. This leads to the lesser disruption and is expected that the difference in relative speeds and time is kept to the bare minimums, i.e., no discernible differences are expected in each vehicle driving patterns.

The second LoS, is based on lesser communication capabilities, which increases the uncertainty in determining each vehicles relative position and speed, as well as the intentions of the vehicle. Two vehicles crossing the intersection with no change of directions when they were originally in opposite directions, poses no unsafe situation even with poor coordination, but if one intends to change direction this may lead to a collision risk and thus to unsafe condition.

In order to validate the assumptions for this scenario, as well as the safety architecture correct operation, some validation criteria shall be used. Following are high level descriptions of the validation criteria:

- In ideal conditions the vehicles will approach the crossing, adapting their approach to cross without discernible changes in the traveling patterns. The rule to follow is a yield to the right approach where the vehicle presenting itself from the right has priority over the one

from the left. The cooperation efforts will ensure that the increase or decrease of speed of each vehicle is minor when performing the crossing.

- In failure conditions, due to injected faults, the uncertainty concerning the relative speed and position forces the reduction of the speed when approaching the intersection noticeably, with the ultimate consequence of the vehicle stopping near the intersection in case of total failure to use indirect sensory information. This would be the equivalent to a stop sign in order to collect additional sensor data from the environment in order to safely proceed into the intersection.
- Recovery conditions, resulting from the removal of the faults injected into the system, shall lead to an increase back to the original levels of the approach speed to the intersection.

The means to validate the above criteria will be briefly expanded in section 5 and refined in the following WPs, particularly in WP 5.

Coordinated lane change manoeuvres on highways and roundabouts for individual vehicles and platoons

Unintentional lane departure is one of the highest risk factor on the road. The idea here it to provide a distributed mechanism for assuring that at any time and any region there is at most one vehicle that is changing its lane and that the nearby vehicles allow it to safely complete the manoeuvre. This concept can be, of course, extended to platoons of cars that can change lanes in a coordinated manner.

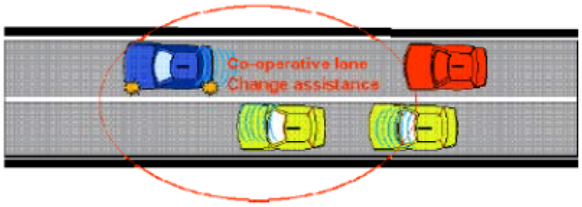

Figure 14 – Proximity detection warning when changing lanes

Each vehicle emits its position to the surrounding vehicles. By extrapolating all of these positions it is possible to visualise a safety “bubble” around each vehicle as seen in Figure 14, and not just what is ahead and what is behind the vehicle and thus to facilitate the changing of lanes in a safer manner. A similar approach can be applied to vehicles entering new lanes as shown in Figure 15, and when joining to vehicle platoon. Therefore, we focus on one of them; lane change.

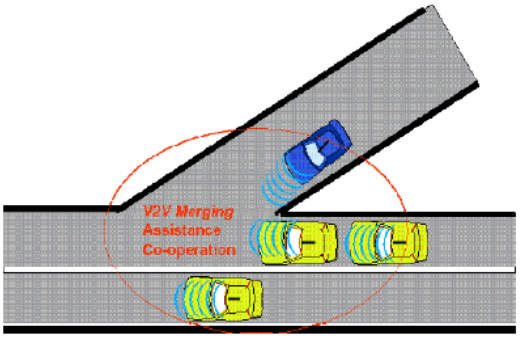

Figure 15 – Proximity warning when entering new lanes

Coordinated lane change in a similar manner to the intersection crossing depends highly on the communication channels to ensure that the intentions of all the vehicles are understood and agreed upon before the actual change can take place. In this scenario however, the sensors do

help in the determination of unsafe conditions and may prevent the change in an unsafe situation.

The Level of Services considered as minimum for the determination of the safety architecture in this scenario are based on the accuracy of the information concerning relative position and speed of the vehicles. This accuracy may be greater than the crossing intersection due to additional data from the sensors and thus allows for shorter manoeuvers. If good communication and thus cooperation is possible, with data accuracy augmentation and merging from sensors the lane change is possible into a relative short slot between vehicles. If the accuracy is lower the distance between vehicles needs to be greater as well as the speed at which the lane change is performed also needs to be extended to ensure that the safety mechanisms can assure the safe change.

In order to validate the assumptions for this scenario, as well as the safety architecture correct operation, some validation criteria shall be used. Following are high level descriptions of the validation criteria:

- In ideal conditions the vehicle distance will be equal to the length of the vehicle changing lane plus a small gap in front and behind the other vehicles. In addition the speed at which the lane change occurs shall not change noticeably.
- In failure conditions, due to injected faults, the uncertainty concerning the relative speed and position forces the increase of the gap between vehicles and it may force a reduction of the speed of the involved vehicles. The front vehicle may be forced to accelerate whilst the trailing vehicle may have to slow down. This change in speed will be linked to the quality of the communication mechanisms.
- Recovery conditions, resulting from the removal of the faults injected into the system, shall lead to a decrease in the car distance back to the original as well as a stabilisation of speed if the other cards speed has been changed due to reduction of communications.

The means to validate the above criteria will be briefly expanded in section 5 and refined in the following WPs, particularly in WP 5.

Given that platooning is a function considered important to improve traffic flow, and consequently, fuel efficiency, also reducing the risk of collisions, thanks to the coordinated control of the vehicles, roundabout merging is an interesting possible application of KARYON's use cases, for the following reasons:

- Interaction with other vehicles includes not only the vehicles that can be detected with on-board sensors (as it happens, for instance, on a straight road) but also vehicles out of sight, coming from different directions. Communication, vehicle location are key prerequisites, therefore the support of cooperative control and, eventually of the infrastructures, are necessary.
- A relevant number of vehicles are involved, and information exchange among several vehicles is necessary to coordinate each of them. The communication channel is heavily loaded by this application, which therefore can represent a significant study case.
- A complete vehicle control requires steering, propulsion and braking actuations, therefore includes all most important vehicle functions.
- In terms of safety, the case is also significant, because failures can cause severe damages, due to foreseeable lateral impacts.

3.2.2 Functionalities

The functions considered in KARYON include some of those already defined in ETSI (ETSI TR 102 638) as Cooperative Awareness Basic Service, and especially those related to road safety and traffic efficiency.

In addition, more advanced functions are considered, which covers the area of co-operative driving including automatic driving. Some of them are derived from the above said ETSI standard, other from European projects dealing with automatic driving (e.g. Cybercars2).

A summary of the functions relevant to KARYON are listed Table 1.

Cooperative Awareness Basic Service	A) Intersection collision warning
	B) Signal violation warning
	C) Lane Change Manoeuvre
	D) Co-operative adaptive cruise control D1) Emergency brake lights D2) Stationary vehicle warning
	E) Intersection management E1) Traffic light optimal speed advisory E2) Collision Risk Warning from RSU E2) Signal violation warning
Automatic driving	F) Co-operative vehicle-highway automation system (Platoon) F1) Co-operative side merging F2) Co-operative roundabout merging
	G) Intersection control

Table 1 – ITS and co-operative driving functions relevant to KARYON

The vehicle functionalities foreseeable to perform the above functions are described in the following:

Propulsion control

By wire control of the propulsion force by means of engine torque control and gearbox management to produce the desired acceleration

Braking control

A wired control braking system can produce the desired deceleration. This functionality includes the interaction with other braking sub-functions, e.g. ABS, or with yow rate control.

Steering torque control

This functionality consists of the superimposition of a steering torque on the steering wheel, in order to implement automatic vehicle steering, allowing at the same way any action by the driver in the case of need.

Collision avoidance

This functionality is based on the detection of moving obstacles on the vehicle trajectory, by means of RADAR systems with an obstacle detection range of at least 150 m. This functionality can usually require also short range LIDAR or ultrasonic systems to detect obstacles in vehicle proximity (up to few meters) covering also a lateral area, as it is necessary to avoid dangerous situations for pedestrians and other road users moving with lateral relative speed.

V2X Communication

Communication is a two way function to supply data and to receive information from other vehicles and infrastructures, according to the services standardized by ETSI. Communication includes firewall functions, recognition of wrong messages, and countermeasures against malicious attacks.

Cooperative awareness

Cooperative awareness functionality regarding road safety is a warning service based on the information about the status of the neighbouring vehicles and of the road conditions, intended to alert the driver and safely anticipate the needed manoeuvres. The information provided is standardized by ETSI.

Cooperative automatic driving

Cooperative automatic driving includes many possible functions, based on the available information about the neighbouring vehicles and ranging from only longitudinal control to the complete vehicle control including lateral control. In general and in the complete functionality, automatic driving do not require any driving action by the driver, but usually the driver performs a surveillance task and should be ready to take the control in the case of risky situations or whenever the road conditions do not allow automatic driving (e.g. in complex traffic scenarios).

The main functions that compose cooperative driving are:

- Overtaking manoeuvre
- Platooning (normal mode, joining mode, leaving mode, cutting mode)
- Roundabout
- Intersection (with priority or without any priority)

3.2.3 Safety conditions

In order to identify the safety requirements of the control systems, a hazard analysis and risk assessment has been conducted. According to the safety lifecycle of ISO 26262, before the execution of the hazard analysis, it is required to define the item, which is the system or the group of systems under development. In KARYON, only a part of a system is addressed, in the sense compliant with ISO 26262, which defines a system as a "set of elements that relates at least a sensor, controller, and actuator with each other".

According to the use case functionalities, the control systems are interfaced to a communication channel providing:

- for co-operative awareness services: warning information, and also
- for co-operative driving: control signals produced by the on-board co-operative driving applications and addressing the on-board equipment for vehicle control.

As a preliminary risk assessment, only the hazards produced by the communication channel are considered. Two separate hazard analyses and risk assessment have been conducted, with reference to the two categories of applications and, presumably, of consequent architectural constraints, as follows.

In the different use cases considered, the common functionality of the communication system with the external environment is to provide warning information to the driver, allowing him/her to approach the hazardous situation in the right way.

The different malfunctions that have been selected in the attached risk assessment are limited to the unavailability of the warning signalling or to the communication of incomplete or false information, specific for each use case. All the on-board EE systems (like ACC, ESP, etc.) that can be eventually used as external measures to mitigate or directly cover the hazardous events are considered perfectly functioning and, in any case, are not considered source of fault/failure/malfunction.

For each use case one typical scenario has been defined, on which the related malfunction has been applied. This preliminary analysis, that it is not exhaustive, can give an indication on the risky situation that can occur in case of failure. A complete analysis should include a complete set of situations, as well as the malfunctions of the safety kernel (in terms of functionalities), such as providing wrong information to driver or routing wrong control signal for some applications (e.g. ACC).

In the following table the outcomes of the analysis are summarized. Annex A provides the detailed information regarding:

- Locality (location, road condition, environmental and driving situations, traffic situation)
- Dynamic driving status (speed, accelerations, manoeuvres)
- User conditions (actor, location, careful level)
- Vehicle condition (ignition key status, engine status, etc.)
- Persons at risk
- Controllability level and justification
- Accidental scenario if controllability task will fail
- Severity level of Loss and damage, and justification
- Probability level and justification.

Ref. use case	Failure/ malfunction/ (effects in terms of functional outputs)	Hazard		ASIL	Safety goal ID	Safety goal	Safe state
		ID	Description				
A - Intersection collision warning	M1 = intersection collision warning unavailable/false negative	H1	Collision with the overtaking vehicle	A	SG1	To alert the driver that the warning information is unavailable	Warning function turned off
B - Signal violation warning	M2 = Signal violation warning unavailable/false negative	H2	Collision with the vehicle coming from the crossing road	B	SG2	To alert the driver that the warning information is unavailable	Warning function turned off
C - Lane Change Manoeuvre	M3 = Lane change warning unavailable/false negative	H3	Collision with the vehicle running on the other lane	A	SG3	To alert the driver that the warning information is unavailable	Warning function turned off
ACC: D1 - Emergency brake lights D2 - Stationary vehicle warning	M4 = Emergency electronic "brake lights" warning unavailable/false negative	H4	Bumping into the front vehicle due to an excessive deceleration whitout adequate recovery with ACC	B	SG4	To increase the safety distance of ACC control and alert the driver that the warning information is unavailable.	Warning function turned off. ACC control in safe distance mode.
Intersection management E1 - Traffic light optimal speed advisory	M5 = Incorrect information of traffic light status	H5	Collision with the overcoming vehicle	QM	SG5		
Intersection management E2 - Collision Risk Warning from RSU	M6 = Signal of collision risk warning unavailable/false negative	H6	Collision with the vehicle coming from the crossing road	B	SG6	To alert the driver that the warning information is unavailable	Warning function turned off

Table 2 – Summary of the outcomes of the hazard analysis and risk assessment concerning co-operative awareness services

From this preliminary analysis the conclusion is that, for co-operative awareness services, the information provided to drivers shall comply with ASIL B requirements (maximum, depending on the cases), and that the control mechanisms shall recognize the unavailability of warning information and shall detect false negative information.

Furthermore, in the case of ACC, the control parameters shall be adapted if the considered malfunctions occur.

Concerning automatic driving, the following use cases have been considered linked to the use case scenarios and Levels of Service described previously.

F1 - Co-operative merging in highways, for a car coming from the acceleration lane and merging into a platoon, in a quite normal situation in terms of visibility, road surface, and considering a quite high speed due to the on purpose lane for this manoeuvre, but expecting a medium-low careful level of the driver, due to his/her confidence in the system functionality, at least after a certain period of usage.

F2 - Co-operative merging in a roundabout in an urban road, at variable speed, and in normal environmental conditions, but again with a quite low careful level of the driver, due to the same reasons as for the above use case, with the addition of the confidence due to low speed.

G - Automatic driving in an intersection of an urban road, at variable speed, as it may be required to safely manage complex manoeuvres involving more vehicles, possibly in the presence of pedestrians.

The only malfunction considered in the above use case is missing information of the presence of the other vehicles or wrong information on their position and speed. For an exhaustive analysis other malfunctions shall be included, but at this preliminary stage the actuation systems (propulsion, braking and steering) are assumed to be properly working.

The result is that in the above situations the required integrity level ranges from ASIL D to ASIL B. However, due to the similarities of the different use cases as concerns the malfunctions, an ASIL D is probably the unique that should be identified as the general requirement.

In the same way, the safety goals and the safety states are similar in the above use cases. In all cases, the driver shall be alerted well before the hazardous event occurs and the automatic control shall be turned off, keeping a moderate engine braking, so as to allow the driver to recover by stopping or accelerating the vehicle depending on his/her evaluation.

A consideration has to be taken into account in favour of the feasibility of the above safety goals, even in the case that the malfunctions occur just before the hazardous events, i.e. leaving a short time to diagnose the malfunction and to enable the driver to take safe recovery actions. In fact, in this case, it can be expected that the automatic driving has worked properly up to the time the malfunction occurs, so that the car would be in quite correct and safe conditions in terms, for instance, of distance from the other cars and speed.

In the following table the results of the analysis are summarized. The complete data used for the analysis are reported in Annex A - Preliminary hazard analysis and risk assessment of the automotive use cases .

Ref. use case	Failure/ malfunction/ (effects in terms of functional outputs)	Hazard		ASIL	Safety goal ID	Safety goal	Safe state
		ID	Description				
Automatic driving F1 - Co-operative side merging	M7 = Signal of presence of vehicles for co-operative side merging unavailable/false negative	H7	Collision with the vehicle coming from the main roadway	**D**	**SG7**	**To alert the driver that the control function is unavailable**	**Control function turned off, leaving the engine brake**
Automatic driving F2 - Co-operative roundabout merging	M8 = Signal of presence of vehicles for co-operative roundabout merging unavailable/false negative	H8	Collision with the vehicle coming from the roundabout	**C**	**SG8**	**To alert the driver that the control function is unavailable**	**Control function turned off, leaving the engine brake**
Automatic driving G- Intersection control	M9 = intersection control collision warning unavailable/false negative	H9	Collision with the vehicles coming from the crossing roads	**B**	**SG9**	**To alert the driver that the control function is unavailable**	**Control function turned off, leaving the engine brake**

Table 3 – Summary of the outcomes of the hazard analysis and risk assessment concerning co-operative driving

3.2.4 Requirements

Each requirement is numbered as follows: R.x.z; or, R.x.y.z. “x” and “y” are numbers which correspond to the section and subsection where the requirement is contained. Z is a serial number, unique within the section where the requirement is defined. The numeric sequence formed by either “x.y” or “x.y.z” is unique throughout this document and, as so, identifies the requirement to which it corresponds.

R.3.2.10

The information for the cooperative functions shall be determined in terms of quality and quantity in order to specify the level of service for the vehicle.

Rationale: The information quality and quantity is the key item which impacts the Level of Service determination.

R.3.2.20

In cooperative awareness functions, missing information relevant to vehicle shall be detected and the level of service is lowered in TBD seconds.

Rationale: In the case that the communication is unreliable, this must be detected and based on the uncertainty of the vehicles positions, the level of service should be lowered in a bounded time frame.

R.3.2.30

In cooperative driving, missing information relevant to vehicle operation shall be detected and, if the missing information cannot be reconstructed, the vehicle shall slow down and even stop (according to traffic rules and the safety analysis).

Rationale: In the case the missing information cannot be reconstructed, automatic driving could be unsafe operation.

R.3.2.40

In cooperative driving, missing information relevant to vehicle operation shall be detected and, if the missing information can be reconstructed without faults, automatic driving shall be maintained at the highest level of service, compatible with safety requirements.

Rationale: In the case the missing information can be reconstructed without failure and in a timely manner, automatic driving is resumed at higher vehicle performance still ensuring adequate safety level.

R.3.2.50

The system architecture supporting cooperative functions shall be devised in order to take into account the hazards identified in the preliminary hazard analysis.

Rationale: Based on the preliminary hazard analysis detailed previously.

R.3.2.60

In the lowest LoS, the safety and control functions will insure that the speed of each vehicle shall not exceed TBD km/h.

Rationale: In case of higher collision risk, the action to take is to reduce vehicular speed. Identification of the value for the maximum safe speed is to be determined in the safety mechanisms specification.

R.3.2.70

In the lowest LoS, the safety and control functions will insure that the distance between each vehicle shall not exceed TBD meters.

Rationale: In case of higher collision risk, the action to take is to increase vehicular distance. Identification of the value for the minimum safe distance is to be determined in the safety mechanisms specification.

R.3.2.80

The system architecture supporting cooperative functions shall be an extension of autonomous driving.

Rationale: The autonomous driving refers to a single vehicle. Extension to it is required to ensure cooperation.

R.3.2.90

The system architecture supporting cooperative functions shall be based on a set of functionalities that allow autonomous driving.

Rationale: Extension to R3.2.80, refining the requirement to include the set of functionalities.

R.3.2.100

The system architecture supporting cooperative functions allows the use of external infrastructures following the European standards under way.

Rationale: Current external infrastructures already provide a base architecture which account for a modicum of cooperative information to be disseminated to various vehicles.

R.3.2.110

The system architecture supporting cooperative functions shall ensure safety according to ISO 26262.

Rationale: as ISO 26262 is currently considered the standard to follow for this project. NOTE: This requirement may not be fully validated due to effort and timing considerations.

R.3.2.120

On board architecture for cooperative driving shall comply with ISO 26262.

Rationale: The applications of these standards are intended to be focused on Part 3 (only focus on Functional Concept) and Part 4 limited to verification of the functional concept.

The architecture shall be clearly identified in terms of boundary, and exhaustive assumptions shall be defined at the item level, so as to be able to facilitate architecture elements such as SEooC and to make easer their application.

R.3.2.130

Cooperative driving shall be based on V2V requirements defined by ETSI standards or consider possible direction for progress in these areas.

Rationale: as per 3.2.80.

R.3.2.140

Functional safety of cooperative driving shall be ensured. Failures to be considered include those related to communication.

Rationale: as per R3.2.10, R3.2.20 and R3.2.30.

R.3.2.150

The reference use case can be chosen from the following list:

- adaptive course control
- lane changing
- crossing of road intersection

Rationale: as per the chosen use cases presented previously.

R.3.2.160

The architecture can be based on automotive state of the art technologies or in line with the expected trends.

For exemplum, automotive busses can be considered (CAN, LIN, Flexray), Autosar approach could be a solution for software architecture, dynamic task allocation shall be avoided, etc.

Rationale: n/a

R.3.2.170

Cooperative driving shall be based on autonomous decisions performed by each vehicle, and not taken by external supervisors.

Rationale: It is not envisaged traffic control mechanisms to completely replace autonomous cooperative driving, as this relates to the purpose of the use cases.

3.3 Avionics use case definition

3.3.1 Description

The avionics domain considered will be comprised of an unmanned aerial vehicle (UAS) performing a given operational scenario in a non-segregated air space.

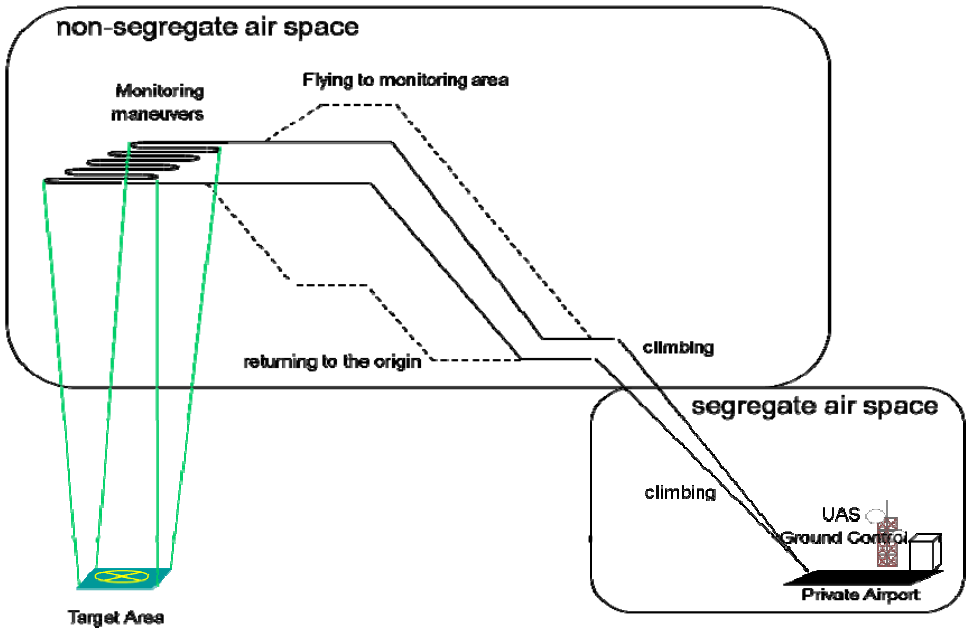

Figure 16 – Avionics base scenario

The main requirement considered is the capability of performing the operational scenario following a pre-authorized 4D trajectory without failure or path deviation. For this scenario three main situations may occur:

- 4D Trajectory Navigation Control based on external and internal sensors
- 4D Trajectory Navigation Control based on external sensors
- 4D Trajectory Navigation Control based on internal sensors

The system under consideration will have internal and external sensor capabilities. Some of the sensors to be considered are:

- External sensors
    - GPS (Global Positioning System) (assumption: sampling rate = 10 samples/sec)
    - GBAS (Ground Based Augmentation System)
    - ADS-B (Automatic Dependent Surveillance – Broadcast) (assumption: sampling rate = 100 samples/sec)
    - DME (Distance Measurement Equipment)
- Embedded sensors
    - INS (Inertial System)
    - Radio-Altimeter
    - ADS (Air-Data System)
    - Video Camera

The current considered pattern is for the UAS to begin a controlled climb into the boundary of non-segregated air space and take safety measures and a final 4D navigation plan. It will then commence its ascent to the target altitude and space, perform the scanning of the targeted area through a grid sweep pattern and then descend to the previously referred boundary. Once

ground control has been reasserted at the boundary, the UAS will then proceed to the selected landing space and finalise its operation.

A “safety state” for an aerial vehicle can be considered as a spatial volume around the vehicle where the possibility of entrance of others objects is minimal. The approach or the eventual entrance of some other vehicle into this volume is defined as an “air traffic conflict”. Usually this spatial volume is described in terms of a vertical and a lateral distance, called “separation minima”.

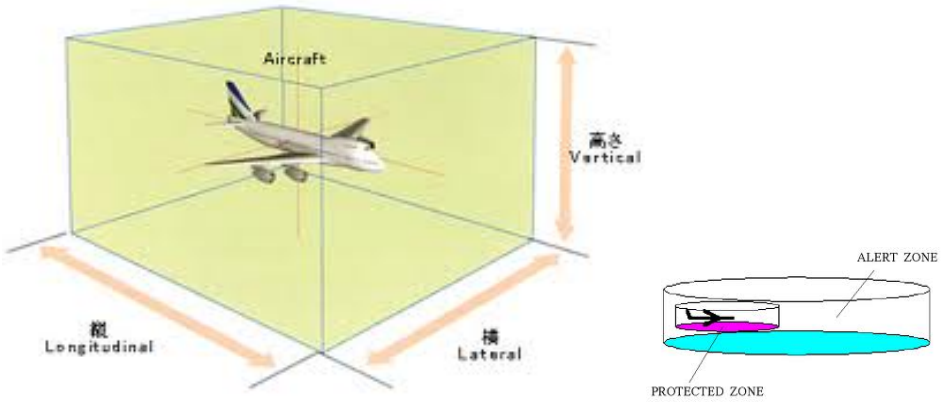

Figure 17 – Aerial Vehicle Safe State

Different safety levels can be defined and applied for different flight situations. As example, for an airplane flying on route monitored by a radar system, a used separation minima is 1000 feet in the vertical direction and 3 nautical miles (NM) as lateral separation. These values are used if the airplane is at a distance up to 40 NM from the radar antenna. Far than 40 NM from the radar antenna, the lateral separation distance increases to 5 NM.

Typically, the safety separation distance is large for aerial vehicles flying in high altitudes and high speeds, decreasing for climbing and descending flight phases, reaching small values at final approach and landing, where the traffic density is higher.

Based on this safety separation concept, the fundamental information required to control the air traffic safely is the knowledge of all vehicles position in a common time base.

Currently, the mainly sensors and electronic devices used by the air traffic control systems (ATC) to monitor and support the operation of the aerial vehicles in the airspace are based on the ground, as radar systems, very high frequency omni-directional range (VOR), distance measurement equipment (DME) and others.

In the future air traffic management systems (ATM), each aerial vehicle will sense its position and time clock based on satellite navigation information, sending its position information to the ATM on the ground and to other aerial vehicles flying in the same airspace. This way, the air traffic mapping of all vehicles will be available to the ATM and also to each vehicle flying in that region.

The dissemination of vehicle position information based on satellite technology shall allow the development of a collaborative air traffic management. It is expected that direct flights following optimal trajectories, the called 4D-Trajectories, shall be authorized. Complex flight procedures executed for safety purposes shall be eliminated and, mainly, it shall allow the integration of remote piloted vehicles (UAS) into the airspace shared by others piloted vehicles.

Aiming to perform a safety analysis of a shared airspace traffic including UAS it is convenient to consider two special traffic scenarios involving a:

- UAS and a collaborative aerial vehicle ;

- UAS and a non-collaborative aerial vehicle.

A collaborative vehicle here means an aerial vehicle that knows its position and is able to diffuse it to others vehicles, as well as to the ATM center, see figure below. A non-collaborative vehicle, i.e., not using ADS-B satellite based information, has a much less accurate estimative of its actual position, and only can transmit it to the ATM center by a voice channel.

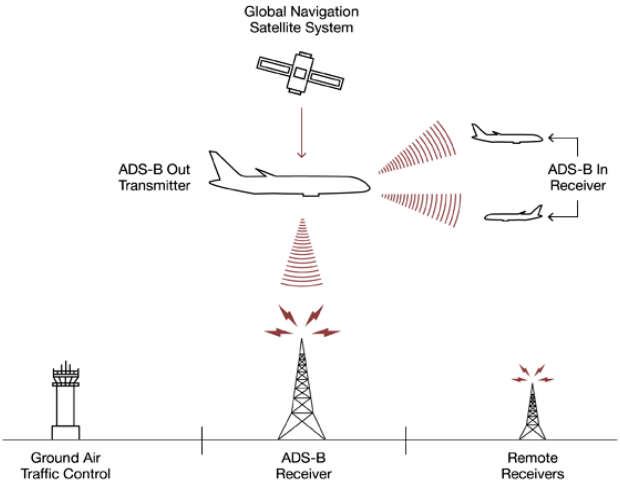

Figure 18 – Collaborative aerial vehicle

From this point forward, when we refer to aircraft it may be an actual aircraft or an UAV. The concept is to have autonomous cooperative vehicles. This may be achieved through the use of UAVs, airplanes flying on autopilot and a mixed scenario where the airplanes collaborate with the UAVs in a given region of airspace. This collaboration may not involve all vehicles performing the same cooperative activities. Some UAVs may be mapping a region of terrain, while commercial airplanes are in their regular flight paths between destinations and other set of UAVs may be performing aerial surveillance. The key issue here is to ensure that all these sets of cooperative vehicles successfully perform their respective tasks and with the appropriate degrees of safety.

To ensure this, and taking into account the automotive use case scenarios described above, three potentially conflicting scenario are described below for discussion:

Common trajectory traffic in the same direction

This is an aerial traffic situation analogous to the road traffic scenario with cars running Adaptive Cruise Control Systems (ACCS).

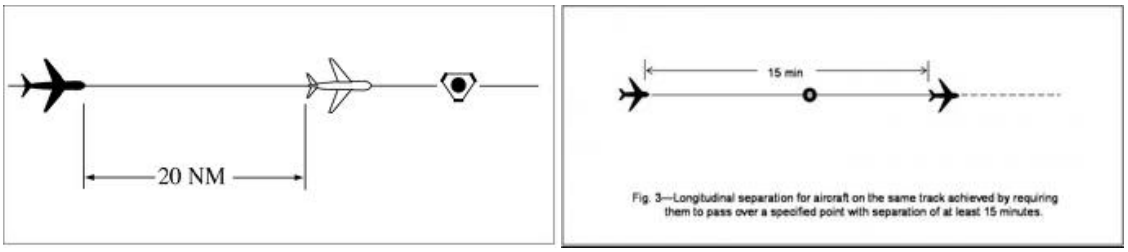

Figure 19 – Common trajectory traffic

Two aerial vehicles fly a common optimal trajectory that connects a common origin and destiny location. A traffic conflict may appear when the rear vehicle is faster than the front one, or when

both vehicles fly in the same speed. A similar and more frequently situation occurs between two aerial vehicles during the climbing flight phase after departing from the same airport.

- UAS and collaborative aerial vehicle: a safety separation can be obtained controlling the relative position between the vehicles;
- UAS and non-collaborative aerial vehicle: this can be considered an unsafe condition where the separation minima needs to be increased. Safety can be assured applying traditional separation methods.

Convergence path in final approach: even that this scenario is out of the UAS scope, this situation represents a typical problem for the 4D-Trajectory analysis. A solution can be proposed in two steps, first aligning all the vehicles into a queue and then, keeping a safety separation between the vehicles approaching in a common speed.

In this case, special care is required with the wake of turbulence produced by the front vehicle that might represent a threat to the stability of the rear vehicle.

Leveled crossing trajectories

This is an aerial traffic situation analogous to a crossing road intersection. It is a conflict situation of frequent occurrence, where two aerial vehicles with similar performance would have optimal trajectories that cross in some airspace point.

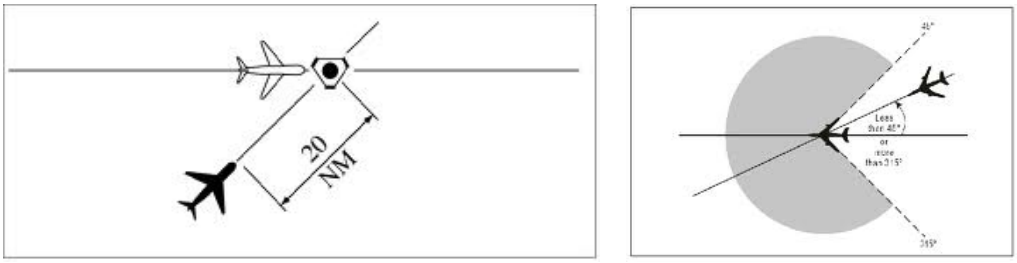

Figure 20 – Levelled crossing trajectories

- UAS and collaborative aerial vehicle: the separation minima can be assured controlling the estimated crossing time, based on the speed and distance to the crossing point of the vehicles;
- UAS and non-collaborative aerial vehicle: this can be considered an unsafe condition where the separation minima needs to be increased. Safety can be assured applying traditional separation methods.

Remark: an altitude crossing trajectory is another potential conflicting situation similar to the leveled crossing trajectories. The difficulties associated and possible procedures to assure safety are also similar to the leveled case.

Coordinated flight level change manoeuvres

This scenario considers flight level change for an UAS where it intersects the flight altitude of other vehicles. Difference between this scenario and the previous is that the cross is not directly in a collision path.

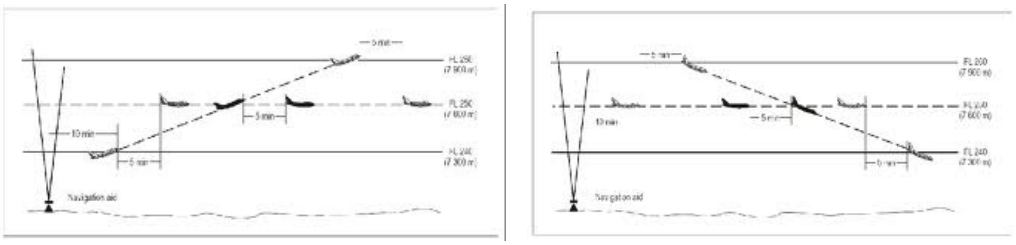

Figure 21 – Coordinated flight level change

The reasoning behind these 3 use cases is related to the automotive domain use cases. Although requiring somewhat different safety conditions and having different control options, the scenarios are similar in nature in a form that allow us to extrapolate safety and performance measures in a confident nature.

3.3.2 Functionalities

In the aeronautical industry, there is currently a reasonable consensus applying two basic documents as guides for the development of new aircraft or complex system: SAE-Aerospace Recommended Practices – 4754A "Guidelines for Development of Civil Aircraft and Systems" - ARP4754A and SAE-Aerospace Recommended Practices – 4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"- ARP4761

The SAE ARP-4754A, basically, presents a development process, applicable for aircraft/systems of highly complex and integrated nature, where development errors can be introduced and contribute to identified failures conditions.

The Development Assurance process, as it is called, is a top down process, starting from the top-level aircraft safety requirements, descending to system items level requirements, when a safety assessment process is used in conjunction with the development assurance process.

From the performance and operational aircraft requirements, failure conditions and the correspondent severity are identified and are used to establish the level of rigor required for the development of the systems and its components, the so called Development Assurance Level, as presented on section 2.2. The controlled process used for the development of software and hardware items are, respectively, DO-178B/ED-12B and DO-254/ED-80.

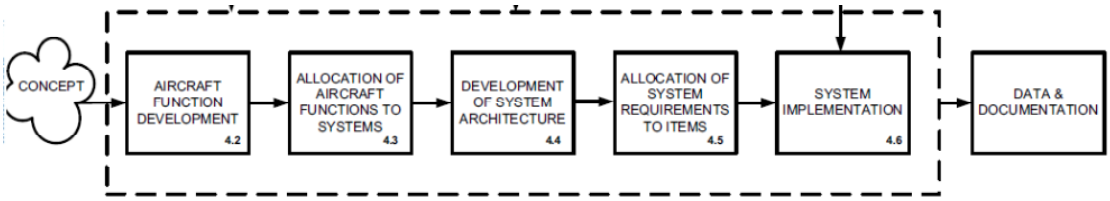

Figure 22 – Development Assurance Process

The SAE ARP-4761, basically presents a safety assessment process used to show compliance with certification requirements. The primary processes are listed below:

- Functional Hazard Assessment (FHA): examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific conditions. The FHA is developed early in the development process and is updated as new functions or failures conditions are identified.

- Preliminary Aircraft Safety Assessment/Preliminary System Safety Assessment (PASA/PSSA): establish the aircraft/system safety requirements for an initial architecture indicating if this architecture can meet those requirements.
- Aircraft Safety Assessment / System Safety Assessment
- Common Cause Analysis

Of particular interest for the present activities of KARYON Project, following the ARP-4761, is to develop a Functional Hazard Analysis for the UAS, the first step being the definition of the top-level vehicles function to be analyzed. Four vehicle level functions were then selected that can reveal safety aspects, features or desired behavior.

The selected vehicle level functions are: Remote Pilot Function, 4DT Navigation Function, Position Estimator Function, Communication Function, Conflict Manager and Collision Avoidance Function. This first list presented below in a block format, should be reviewed during the project development.

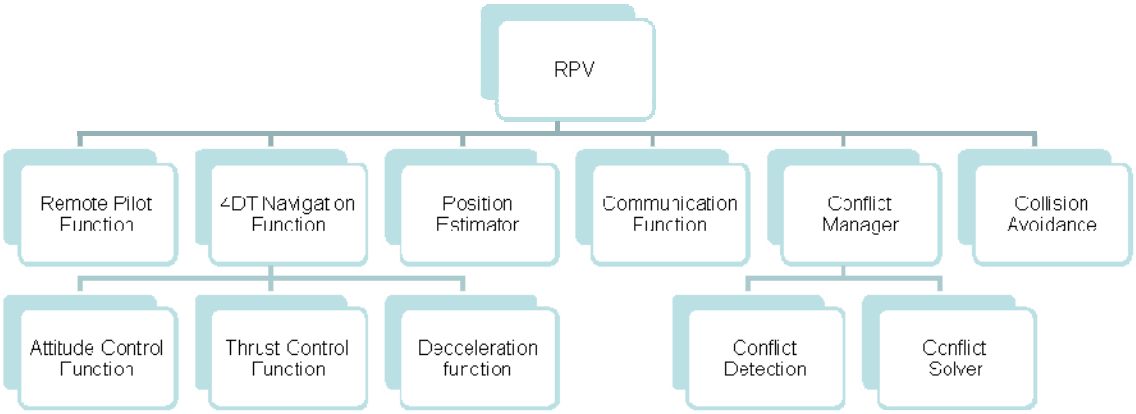

Figure 23 – UAV functionalities

The Remote Pilot Function:

The remote control function is the RPV ability to transfer the flight control command to the RPV control centre. Under remote control, the RPV receives command inputs control coming from ground control centre.

4-D trajectory Navigation

The 4D-Trajectory function can be described as the aircraft ability to follow a specific spatial trajectory, in a prescribed timing and within a limited and controllable deviation to a nominal value.

To perform such function it is required that the aircraft be able to control its attitude and accelerations over the 3 main aircraft axes. In a schematic way, these abilities can be described as sub functions executed by systems as indicated below:

Sub function	System implementation
Longitudinal control function	Wheel - elevator system
Roll control function	Wheel – aileron system
Yaw control function	Pedal – rudder system
Thrust control function	Throat engine system
Navigation function	GPS + INS navigation system
Navigation function	GPS navigation system
Navigation function	INS navigation system

Once the 4D-Trajectory function is implemented and supported by a combination of systems, as listed above, those systems must be designed with the appropriated reliability required by the 4D-T function.

In this way, a Preliminary Safety System Assessment (PSSA) is performed aiming to determine the severity of the injuries produced in case of fault or malfunction of each one of the systems, sub-system and components, that support the 4D-T functionality. It is not acceptable the existence of single failure able to produce a total loss of the 4D-T function.

The Position Estimator

The position estimator function aims to estimate the position, speed and direction of the movement of a vehicle. The function collects information from different sensors, onboard or external to the vehicle, generates the best estimative of position, speed and heading of the vehicle and the estimative of the related uncertainties.

The inputs for the position estimator are sensor measurement information, as GPS, Inertial System, Radar, Lidar, etc. The outputs of the function are the position, speed, heading and the associated uncertainties of the vehicle.

Communications

The communication function can be described as the UAS capability to exchange digital data with others entities. It is composed by the following sub functions:

- Communication RPV to RPV control centre described as the capability of the UAS to receive instructions and send information to the UAS ground control centre. Usually this function is available in a limited airspace distance range around some grounded antenna.
- Communication RPV to ATM control centre described as the capability of the UAS to receive instructions and send information to the ATM ground control centre. This function should be available through a large ground based radio-frequency network.
- Communication RPV to aircraft described as the capability of the UAS to send its position and time clock to other aircrafts sharing a common airspace, in a broadcast way.

The Conflict Manager Function:

The conflict manager function is composed by two sub-functions aiming to identify potential traffic conflict with others aircraft and to propose a collision avoidance strategy to be followed by the RPV.

The inputs of the conflict manager function are the position information from others aircraft and a map of the position of the vehicles provided by the ATM. The outputs are traffic conflicts identified and collision avoidance strategy for each one.

Collision Avoidance Function

The collision avoidance function is basically composed by the capability of the aircraft perform two sub-functions, sense and avoid:

1. Sensing function described as the RPV capability to recognize others vehicles near itself. The RPV carries a radar system onboard able to detect other vehicle in a short vicinity.

2. Avoidance function is the RPV ability to change abruptly its trajectory in an emergency or conflict situation with others vehicles

3.3.3 Safety conditions

The definition of a safety state for an aerial vehicle as a spatial volume around the vehicle where the possibility of entrance of others objects is minimal, can be useful and enough for many purposes. However, for the safety questions addressed in the KARYON project, there is interest in going deeply into this concept.

Keeping the same basic idea of a safe state around a vehicle, it would be possible defining a protection sphere around the vehicle, centered at its Center of Gravity (CG), for example, with radius 'Rv', that isolates and protects the vehicle from outside objects. In this case, the trajectory of the vehicle through the airspace could be defined in terms of the CG trajectory, and the ultimate radius of protection, preventing any kind of contact with external objects, would be the distance from the CG to the farthest physical point of the vehicle (see the figure below).

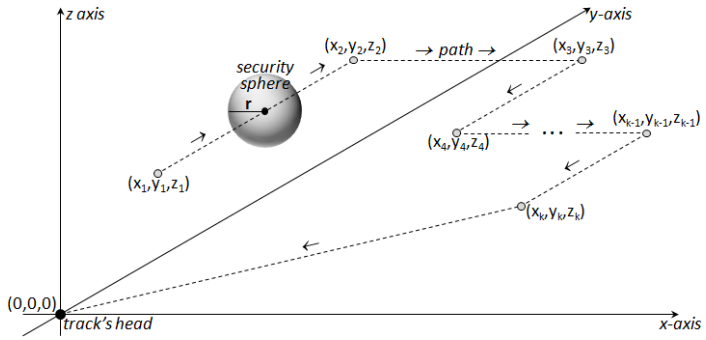

Figure 24 – Security sphere

A "safety level of reference" could also be quantitatively defined, expressing the expected number of entrance of foreign objects into the safe sphere, of radius Rs, based on statistical possibilities, for example, one possible invasion on the secure sphere in 10Exp(9) hours of flight.

Considering these definitions, the determination of the aerial vehicles position as a function of time inside airspace, an air traffic 'mapping', would be the necessary and sufficient condition to design a deterministic and automatic separation control system, able to guarantee a safe air traffic control within a required safety level.

However, different uncertainty factors can contribute for the vehicle position determination. In case of a satellite based positioning, for example, sample renovation occurs each second. An aerial vehicle flying at a speed of 500km/h, moves 140 meters, approximately, in that second. During this interval, the most probable vehicle position would be in the middle of that 140m distance. Many others factors can contribute to the position uncertainty, as delays or noise on communication channels, flight turbulence, vehicle dynamic, control system malfunctions, sensors and actuators quality and others.

From a safety perspective, the uncertainty of vehicle position is graphically expressed as an increased protection sphere, inside which the vehicle can be anywhere, with radius Rs = Rv + dR, where dR represents a delta radius due to the uncertainty of CG position.

Uncertainty models could be defined and applied for each particular aerial vehicle, considering its system configuration and health, flight conditions and other relevant factors. Part of the uncertainty model information could also be provided by the ATM center, as atmospheric conditions, satellites ephemerides, ground radar redundant position, etc.

The utilization of an uncertainty model would allow the determination of aerial vehicle time and position. Based on this model and information, a stochastic and automatic separation control system might be design assuring a desired level of safety.

The idea of the increased protection sphere resulting from the uncertainty on position determination can be far extended toward an "alert sphere", defined as a multiple of the uncertainty protected sphere.

This alert sphere is dependent, as briefly referred above, on the quality of the information used to determine the actual position and speed of the vehicle. The more sensor data and communication information is gathered, the less this uncertainty is expected to be. This allows for the determination of the Level of Services linked to the aircrafts flying in the non-segregated area, both in terms of a more globalized view in a given detection area, as well as for each aircraft in the mentioned area. It may not be possible, and indeed, it is not expected, that all air vehicles agree every second they are in the surrounding area in a common Level of Service but as long as communication is possible between all of them and with the ground infrastructures, the global Level of Service is something that may be determined over a period of time.

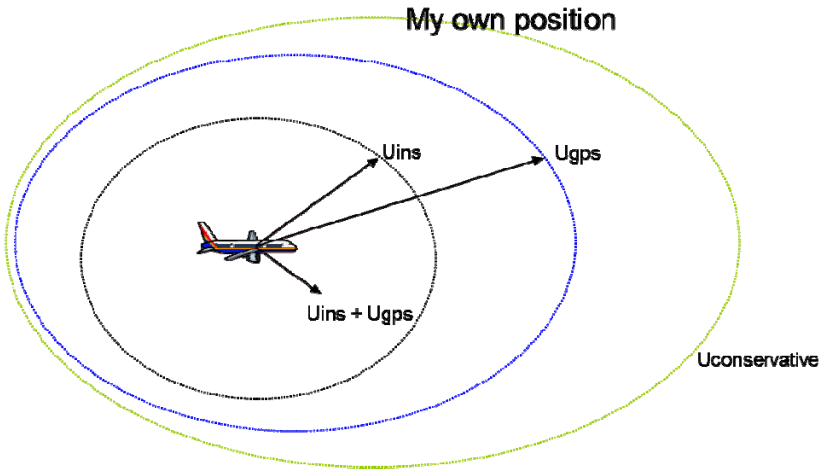

Figure 25 – Uncertainty safety radius

Figure 25 provides a good example of the uncertainty safety radius associated with the quality of information when determining the aircraft's position. If the sensors, GPS readings and communication channels are of good quality the uncertainty is reduced to a minimum. This allows for a greater degree of service and permits to reduce the separation distance by a known factor.

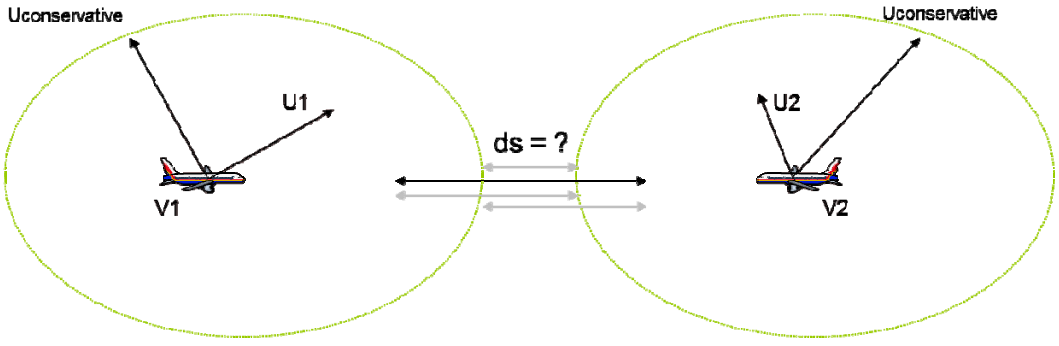

Figure 26 – Separation Distance considerations

Figure 26 provides an example of the separation distance (ds) connected to the uncertainty regarding the relative position and speed determination of the vehicles. The lower the uncertainty, i.e., the higher the confidence on the position, speed and intentions of the vehicles, the lower that separation needs to be allowing for a greater Level of Service. If the uncertainty is high, all vehicles need to consider a very high separation distance to maintain safety, thus reducing the Level of Service and the efficiency of flight.

Breaches of that separation distance leads to conflict situation, with a potential mid-air collision worst case scenario and thus a safety hazard. To avoid this, modifications to the 4DT trajectory is required. The safety mechanisms will ensure that the modifications performed autonomously will not endanger the aircraft or any surrounding aircrafts. These modifications will comprise the deviation from the previously defined 4D trajectory, the keeping of these modifications and a return to the original trajectory when the conflict situation has been removed. Of course the efficiency and speed of these course changes will be greater, the higher is the Level of Service.

Preliminary Aircraft Safety Assessment/Preliminary System Safety Assessment (PASA/PSSA)

This section presents a first trail establishing the aircraft/system safety requirements for an initial architecture, verifying and indicating if this architecture can meet those requirements.

In a general mode, failures on RPV systems implementing the 4DTrajectory function, as the rudder, navigation or propulsion system, could produce a deviation of the vehicle from the authorized 4DT, demanding track corrections.

Failures conditions are analysed for some particular system architecture. For example, it has been considered two communication channels, one for transmission and another independent channel for reception.

Failures on the UAS communication system could generate tree kinds of impacts:

- In case of a missed reception capability, the RPV would be able only to send information data. The safe procedure in such situation would be keeping the RPV in the last authorized 4DTrajectory;
- In case of missed transmission capability, the RPV would be able only to receive data information, becoming a non-collaborative vehicle in the traffic airspace, but it can still be remotely controlled;
- In case of missed reception and transmission capabilities, the expectation is that the UAS will keep the last authorized 4DTrajectory, in autonomous mode. This situation must be identifiable by the RPV that must start some pre-programmed safety procedure.
-

Combined failures on the 4D-T and communication systems could produce potentially high unsafe situations:

- Failures on 4DT system combined to reception incapability can result in deviation of the authorized trajectory, but if the UAS is able to transmit its position, traffic safety can still be achieved. This situation must be identifiable by the RPV that must start some pre-programmed safety procedure;
- Failures on 4DT system combined to transmission incapability can result in deviation of the authorized trajectory, but if the UAS is able to receive data information, it is also possible to command its trajectory, depending on the distance to the RPV control centre. In such situation, the RPV becomes a non-collaborative vehicle;
- Failures on 4DT system combined to transmission and reception incapability should transform the RPV in an ‘intruder’ or ‘unknown’ inside the airspace. Only a radar based sensor would be able to detect it. This situation must be identifiable by the RPV that must start some pre-programmed safety procedure.

Different pre-programmed safety procedure may be adopted. This subject is not treated here.

A final critical unsafe situation would occur, even if not frequently, when a non-collaborative aerial vehicle (piloted or not), without communication with the ATM centre, an ‘unknown’ or ‘intruder’, comes into the shared airspace. In this case, only a primary radar sensor would be able to prevent a conflict. ATM ground radar could detect the intruder and send some

instruction to the RPV, or the RPV could carry primary radar onboard able to detect the intruder within a safety distance and perform a deviation manoeuvre, refers to the Collision Avoidance function.

The preliminary hazard analysis of the functionalities defined in Section 3.3.2, is described in Annex B - Preliminary hazard analysis and risk assessment of the avionics use cases. One of the differences between the automotive and the avionics use cases is that the analysis performed in the automotive is done at the system level, while the one performed at the avionics is at the functionality level.

3.3.4 Requirements

R.3.3.10

The system solution shall provide means for cooperative vehicles establish a minimum separation distance (Rs) between them correspondingly to a desirable safety level.

Rationale: KARYON provides innovative system solutions to enable the safe and efficient coordination of smart vehicles that interact and cooperate in uncertain environments.

R.3.3.20

The system solution shall be applicable for any traffic situation, environment condition, sensor availability or quality of distributed state information

Rationale: KARYON solutions mitigate the risks to safety that are implicit in cooperative scenarios and originate from uncertainties affecting the quality of distributed state information and sensor data.

R.3.3.30

Each vehicle shall be able to determine its own position and the related position uncertainty.

Rationale: the minimal information required to identify and solve traffic conflict between vehicles is their position on the space and the associated uncertainty. Necessary and complementary information are the speed and the direction of movement of each vehicle.

R.3.3.40

UAS shall periodically report its position to other vehicles in surrounding area.

Rationale: This leads to an increase in positional awareness of surrounding environment.

R.3.3.50

The UAS shall include a positioning function that is based on position uncertainty models.

Rationale: uncertainties may occur when independent vehicle actuate in collaborative mode. Such uncertainties may arise on each vehicle, on the interfaces or on the environment. The amplitude of the uncertainties scope offers a challenge to KARYON solutions.

R.3.3.60

The position uncertainty models shall contain the uncertainty related to each specific vehicle and the uncertainty related to the environment external to the vehicle.

Rationale: each vehicle generates its own uncertainties depending on the health of its sensors, components, flight conditions, etc, increased by the uncertainties generated outside the vehicle, as communication channels, external sensors and others.

R.3.3.70

The position uncertainty model shall consider uncertainties of locally obtained data (due to sensor faults, local component faults) as well as uncertainties of remotely obtained data (due to communication faults, external sensor faults).

Rationale: each system generates its own uncertainties depending on the health of its sensors, components, flight conditions, etc, increased by the uncertainties generated outside the vehicle, as communication channels, external sensors and others.

R.3.3.80

Each cooperative aerial vehicle shall apply the uncertainty model, fitted to its own characteristics, for the position uncertainty determination

Rationale: the position of a specific vehicle is equal to a estimated position added to the uncertainty calculated by the model applied to that specific vehicle.

R.3.3.90

The positioning function shall update the environment uncertainty periodically, including, if possible, data from the ATM.

Rationale: in the assembly of systems actuating in collaborative mode, the ATM is the entity which has best conditions to manage the environment uncertainties.

R.3.3.100

The Position Estimator functionality shall provide information of the UAS actual position to other functionalities.

Rationale: position information is an input required by other RPV functionalities.

R.3.3.110

4DT Navigation functionality shall provide means to follow a trajectory prescribed in position and time.

Rationale: the RPV must follow a commanded trajectory defined by its spatial position in a given time.

R.3.3.120

Communication functionality shall provide means to the RPV send and receive data information to/from others aircraft, the ATM and the RPV control centre.

Rationale: the exchange of digital data is the basic mean of interaction between the vehicles.

R.3.3.130

The Conflict Manager functionality shall provide ability to identify traffic conflict with other aircraft and determine a collision avoidance procedure to be executed by the RPV.

Rationale: real operating flight conditions may produce traffic conflict between aircraft. The RPV must be able to anticipate potential conflicts and to define strategies to avoid collisions.

R.3.3.140

The Conflict Detection functionality shall provide ability to identify traffic conflict with others aircraft flying in the same local scenario.

Rationale: real operating flight conditions may produce traffic conflict between aircraft. The RPV must be able to anticipate potential conflicts.

R.3.3.150

The Conflict Solver functionality shall provide ability to determine a collision avoidance procedure to be executed by the RPV.

Rationale: real operating flight conditions may produce traffic conflict between aircraft. The RPV must be able to define strategies to avoid collisions.

R.3.3.160

UAS shall ascertain flight conditions prior to entering non-segregated air space.

Rationale: by analysing sensor and communication data when entering non-segregated air space is will be possible for the RPV to determine actual Level of Service and operate accordingly.

R.3.3.170

In the lowest LoS, ~~the safety control will insure that~~ the horizontal distance separation between each vehicle shall not ~~exceed~~ be less than TBD NM.

Rationale: In case of higher collision risk, the action to take is to increase vehicular separation distance.

R.3.3.180

There will be a minimum of TBD seconds between Level of Service modifications.

Rationale: The system should stabilize between LoS changes in order to avoid communication inconsistencies between avionics components.

R.3.3.190

RPV shall be able to recognize communication failure

Rationale: the ability to recognize communication failure allows the RPV to start-up different pre-programmed safety procedures.

R.3.3.200

RPV shall keep track on the last authorized 4DT after reception communication failure detection

Rationale: after a reception communication failure the RPV will no longer be able receive commands and to modify its authorized 4DTrajectory, it has to keep the last valid trajectory. Thereafter it has to have priority over other aerial traffic.

R.3.3.210

RPV shall keep track on the last authorized 4DT after transmission communication failure detection

Rationale: after a transmission communication failure the RPV will no longer be able transmit its position, but it can be remotely commanded by the RPV control centre. Thereafter it has to have priority over other aerial traffic.

R.3.3.220

RPV navigation control system shall be able to compensate for deviation from the 4D-Trajectory, produced by the attitude control system

Rationale: failures on the attitude control system, like elevator or rudder trim, can produce small deviations from the 4D-Trajectory. The navigation control system needs to correct such deviations.

R.3.3.230

RPV shall start a pre-programmed safety procedure in case of a combined failure of 4DT Navigation and Communication functions;

Rationale: In case of a combined Communication and 4DT Navigation functionalities failure, the UAS will deviate of the authorized 4DTrajectory, with no capability to inform its position or to identify the position of other vehicles. It must begin a start a pre-programmed procedure descending to some segregated air space.

R.3.3.240

ATM shall apply the uncertainty model to each collaborative aerial vehicle in airspace for the position uncertainty determination

Rationale: each vehicle calculates its own uncertainties. The ATM, independently, calculates the uncertainties of each vehicle.

R.3.3.250

The ATM shall provide the environment uncertainty

Rationale: in the assembly of vehicles actuating in collaborative mode, the ATM is the entity which has best conditions to access environment information.

R.3.3.260

The ATM shall update the environment uncertainty periodically

Rationale: the environment conditions change continuously with the time. The uncertainty related to the environment shall reflect that dynamics.

R.3.3.270

The ATM and each collaborative vehicle shall execute uncertainty consistency crosscheck periodically

Rationale: different systems may have different sensors and moreover redundant information may be introduced in a collaborative scenario. The consistency checks aim to harmonize the information between the entities.

4. The KARYON Contract

As mentioned in the introduction, the ambition is to identify general criteria for both the KARYON use cases and the KARYON system implementations. We can call this the KARYON contract: “A KARYON architecture is sufficient for every KARYON use case”. In this section we list these criteria and hence define what we mean by KARYON use case and what requirements that implies when defining the general KARYON architecture. As input to these all what has been described in the previous sections of this report apply.

4.1 A General KARYON Use Case

This section will describe a generic environment and operation of autonomous vehicles taking into account the KARYON concept. It is not devised to be linked directly to any domain but is kept general enough to be expanded into any such particular domain.

Fully intelligent vehicles with decision operation capabilities are still years into the future and are not the short term objective of KARYON. Since no artificial intelligence is considered in the scope of KARYON, autonomously operating a vehicle requires that the vehicle has a-priori knowledge of the route to take to fulfil such an operation, knowledge of static obstacles in the projected path, expected “problematic” conditions as well as safety features that allow for the vehicle to detect “not-known” obstacles during the journey and take avoidance decisions to increment the safety of the vehicle. The initial route may of course be subject to alterations and corrections due in most part to the before mentioned “not-known” obstacles and the avoidance decisions taken during detection of those obstacles.

These not-known obstacles may be other vehicles or actors, mobile obstacles not represented/known at route start or other undetermined conditions.

To achieve this detection, internal sensory capabilities is needed, to accurately determine the position of the vehicle as well as to “foresee” its position a given time frame in the future as well as external sensor capabilities to actually detect the obstacles. The nature of these sensors is domain specific and will be described further in detail in each scenario. Detection is not sufficient however if the vehicle is unable to process the sensor data in an acceptable time frame or if actions to be taken to avoid the hazard is not actuated also in an acceptable time frame.

The amount of sensor data to be processed has a direct impact on the time needed to obtain a “trustable” understanding of the surrounding environment. The more data available, the more time needed to ensure the correctness of the perceived environment or actions need be taken to maintain the same level of safety while constructing the surrounding state in a timely manner.

From the scenario described above the following assumptions can be taken:

- The vehicle will be capable of operating without human control safely.
- Control of the vehicle may be overwritten by a human controller under specific conditions to be defined.
- The vehicle will be capable of moving from a starting point to an end point passing through several “waypoints”.
- The vehicle will be capable of detecting external obstacles in a given time frame and distance radius, to be defined.
- The vehicle will be capable of operation outside the projected path in response to an outside perceived threat in a given time frame, to be defined.

- The vehicle will be capable to detect internal failures and no single failure will result in a catastrophic failure.
- The vehicle will be capable to communicate with other vehicles/actors in the surrounding environment.
- If a failure occurs and human control is unavailable, preventive actions must be taken to ensure the safety of the vehicle and of any other surrounding vehicles or actors.

In order to be able to generalize the KARYON results, we should know the limits for their applicability. As said before the idea is that for every use case fulfilling the general KARYON use case criteria, the criteria is assumed to be valid for all KARYON use cases. That means that if any of these assumptions are found not to hold, it is not a KARYON Use Case. Below is first the complete list, and then follows the rationale in a discussion.

- A functionality (service) involves cooperative vehicles
- Each functionality has several levels of service
- The level of integrity w.r.t. to all relevant failures, by each level of service for each functionality to behave safely, shall be determinable
- Different levels of service require different levels of integrity, at least w.r.t. some of the failures

For each level of service there is a well-defined transition to a higher and/or a lower level of service

4.1.1 Criteria rationale

This section provides the rationale for the use case criteria described previously, rationale which will be used for the definition to the general requirements defined in the subsequent section.

- **A functionality involves cooperative vehicles**

This is a core assumption on the scope of KARYON initial concepts. This implies that the use case enables at least communication between vehicles. Use cases excluding vehicle to vehicle communication are outside the scope of the KARYON architecture.

- **Each functionality has several levels of service**

Even if not defined by other reasons, different levels of service shall be able to be identified to match different levels of required integrity (see further the assumptions below)

- **The level of integrity w.r.t. to all relevant failures, by each level of service for each functionality to behave safely, shall be determinable**

A complete hazard analysis shall be able to be done for any use case KARYON addresses safety-critical functionalities, and hence the assumption that a complete hazard analysis can be done. If this is not the case we are outside the scope of KARYON.

- **Different levels of service require different levels of integrity, at least w.r.t. some of the failures**

There needs to be an advantage of adjusting the level of service to match available levels of integrity. This is a major assumption within the KARYON initial concepts. If the level of available integrity is found too low for the current functionality, there should be means to stay fail-operational. In the KARYON general assumptions the means for staying fail-operational is by lowering the level of service. If no such possibility exists in a use case, it is outside the KARYON scope.

- **For each level of service there is a well-defined transition to a higher and/or a lower level of service**

For any decision to go up or to go down one level of service, there is a defined transition, including constraints on the time to fulfil the transition. In the fail-operational assumptions is included that not only the level of services themselves but also the transitions between them can be considered as part of the fail-operational concept. This includes definitions on the timeliness for changing level of service still being considered as a safe behaviour. If the transitions between the levels of services are not well-defined, we are outside the scope of KARYON.

4.2 General KARYON Requirements

In this section extracts a set of requirements serving as input for the rest of the KARYON project. In particular this can be seen as a specification for the architecture work package (WP2) of KARYON, i.e., requirements that should be fulfilled by any KARYON architecture.

Below is the complete list with the rationale.

R.4.2.10

Each vehicle shall be able to perform several functionalities (services) simultaneously

Rationale: It is assumed that there are several functionalities of the vehicle of interest. This is the case for all vehicles of today, and also assumed in the vehicles we study in the use cases. This implies that when defining a KARYON system/architecture it cannot be enough only assuming to implement a single functionality. Much of the complexity making the solution general is that it should be able to handle all functionalities at the same time.

R.4.2.20

The set of functionalities shall be extendable

Rationale: This requirement is important for any architectural pattern to be exploitable for a real vehicle developer. We assume that incremental product development must be supported in such a way that addition of a single functionality should not require a completely new architecture.

R.4.2.30

We consider functionalities that involve sensing, actuating, and communicating with other vehicles or infrastructure

Rationale: This requirement is a direct consequence of the use case criteria that we are looking at cooperative vehicles. The implication on the architecture is that for the realization of every functionality, sharing resources with actors outside the vehicles (other vehicles and infrastructure) shall be possible.

R.4.2.40

Some resources for sensing, actuating and communication shall be able to be shared among several functionalities

Rationale: When adding a new functionality to a vehicle, it should be able to take advantage of that some sensing and/or some actuating from other functionalities also can be used in the new one. A general KARYON architecture must give the possibility for several functionalities to share some resources.

R.4.2.50

Functionalities shall always behave safely independently of level of service

Rationale: If the available level of integrity becomes too low for the actual level of service, a transition to a lower level of service shall be done immediately (the time to initiate the transition shall be much shorter than the time for the transition itself).

R.4.2.60

Functionalities shall always operate in the highest possible level of service

Rationale: If the available level of integrity becomes high enough for a higher level of service than the actual one, a transition to a higher level of service shall be done immediately (the time to initiate the transition shall be much shorter than the time for the transition itself).

R.4.2.70

KARYON's architecture shall be able to express on different levels of abstraction

Rationale: This is to match a break-down of safety-requirements, and different phases in a safety standard reference life-cycle.

R.4.2.80

On each level of abstraction and for each architectural element, the level of integrity shall be possible to express w.r.t. each applicable failure.

Rationale: This means a capability to express safety requirements having safety integrity levels (SIL) and being allocatable to any failure of any architectural element. This requirement implies that we need failure models of the architectural elements we use.

R.4.2.90

There shall be a known set of rules how to determine the level of integrity for avoiding each possible resulting failure when composing architectural elements.

Rationale: This implies rules for SIL inheritance and for SIL decomposition (effects of redundancy)

R.4.2.100

There shall be a known set of rules how to determine the level of integrity for avoiding each possible resulting output failure of an architectural element, given the integrity levels of avoiding the applicable input faults and internal faults

Rationale: This implies a requirement on models for failure behaviour of all architectural elements.

R.4.2.110

There shall be known rules how the amount of, and the quality of, relevant information determines the level of integrity for each relevant failure.

Rationale: This requirement asks for transformation rules from the "quality of information" domain to the "integrity level" domain. The previous domain is what can be measured by the system itself and the latter domain is where the use case requirements are set. In order to understand when to up and down in levels of service, such transformation rules have to be established that are applicable for the architecture and its elements.

R.4.2.120

The amount of relevant information shall be measurable.

Rationale: There shall be a way for a KAYON system to dynamically extract what is needed to determine the available levels of integrity. Given the requirement on a transformation rule to determine integrity of level is fulfilled, then the amount of relevant information should be measurable by the system itself as an input to that transformation.

R.4.2.130

The quality of relevant information shall be measurable.

Rationale: There shall be a way for a KARYON system to dynamically extract what is needed to determine the available levels of integrity. Given the requirement on a transformation rule to determine integrity of level is fulfilled, then the quality of relevant information should be measurable by the system itself as an input to that transformation.

R. 4.2.140

The cooperative driving architecture shall be exploitable in the near future.

Rationale: n/a

R. 4.2.150

Karyon shall define the functional safety requirements in order to allow the definition of the functional safety concept.

Rationale: n/a

R. 4.2.160

Clear assumptions shall be defined at the item level, as concerns any element external to Karyon architecture and interacting with it.

Rationale: n/a

R. 4.2.170

Karyon architecture shall be demonstrated to be compliant with functional safety requirements. The demonstration shall be based on the methods recommended by the ISO standard, such as fault injection and back-to-back simulation.

Rationale: n/a

R. 4.2.180

The architecture shall be able to support significant use cases in terms of:

number of involved vehicles

potential risks in case of failure

relevance of communication in addition to autonomous sensing

Rationale: n/a

R. 4.2.190

The selected use cases shall be clearly defined in order to be useful test cases for the verification of the Karyon architecture.

Rationale: n/a

R. 4.2.200

Each use case shall be dealt with a description of the scenario, including information on operational condition, so as to allow good risk analysis.

Rationale: n/a

R. 4.2.210

Each use case shall be dealt with a description of the operation and vehicle interactions, so as to allow good risk analysis.

Rationale: n/a

5. Method of validation

5.1 General validation goals and scope

Validation in KARYON will in the first line provide evidence that the elaborated safety architecture is appropriate for the functional safety goals as expressed by the safety requirements [cf. ISO26262-9]. Further, because KARYON strives for adaptive system behaviour in response to faults and environment uncertainties, we will show the gracefully degrading functionality in the presence of faults while always meeting the demands specified by to the overall safety goals.

The high-level safety goals addressing the vehicle behaviour in an operational context will be derived from the analysis of the two specific use cases from the avionics and the automotive fields. The use cases are providing the basis for validating the main achievements from KARYON particularly:

- The fulfilment of specified safety goals in the specific operational context.
- The benefits for complex control exploiting sensor-based perception and the improved environmental awareness and coordination through a wireless communication network.
- The gracefully degrading functionality while maintaining the required safety level

Based on the use cases and analysis of the requirements provided in this deliverable, test cases will be elaborated. Specifying these test cases is essential initial work in WP5 (Milestone M5.1 and M5.2 month 19). The test cases will cover essential characteristics of the environment, the situational context and the system conditions to prove that the KARYON architecture fulfils the functional safety goals. Based on the objective of KARYON to explore the fundamental performance-safety trade-off, evaluation will assess the graceful degradation of performance under internal fault conditions and external uncertainties while always maintaining the intended safety level.

5.2 Methods for validation

System evaluation and validation is the main objective of WP5 (Prototyping and Evaluation), however, KARYON will investigate dedicated techniques and provide the respective system and evaluation components throughout the project. KARYON will extensively exploit simulators to model the environment, the communication network and the sensor/actuator system. WP3 will explicitly address these issues by building middleware specifically dealing with the cooperation between simulated and real components allowing mixed reality systems and hardware- and software-in-the-loop experiments. This will establish the experimental basis generating critical environmental situations and excessive load, latency and connectivity conditions for the communication system. Further it will arrange the floor for fault injection experiments. Again, this is considered early in the project in WP3 by developing tools for experimental evaluation of safety assurance according to the ISO26262 safety standard.

The starting points for validation are the test cases that are developed in WP5. Derived from a careful analysis of the requirements specified in this document they will set the respective operational context, the environment situations and system conditions to exercise the KARYON safety concepts and mechanisms. A significant aspect of adopting a simulation-based approach is that systems can be tested in extreme conditions and with a large number of items to evaluate the safety properties without incurring in any real risks. As an outcome of these simulations we expect clear evidence that the safety requirements specified in this document will be met under

the test conditions. The respective use cases and the simulation and fault injection components are detailed in the WP5 description.

Table 4 depicts the requirements verification matrix, indicating the projected method of verification. Design represents written report without physical demonstration of the requirement detailing the means through which the requirement is fulfilled while demonstration is indicative that the requirement will be validate in WP5 through means of physical or simulated components.

Requirements				
Section	**ID**	**RID**	**Detail**	**Validation**
3.2	10	1	The information for the cooperative functions shall be determined in terms of quality and quantity in order to specify the level of service for the vehicle.	Design
3.2	20	2	In cooperative awareness functions, missing information relevant to vehicle shall be detected and the level of service is lowered within TBD seconds.	Demonstration
3.2	30	3	In cooperative driving, missing information relevant to vehicle operation shall be detected and, if the missing information cannot be reconstructed, the vehicle shall slow down and even stop (according to traffic rules and the safety analysis).	Demonstration
3.2	40	4	In cooperative driving, missing information relevant to vehicle operation shall be detected and, if the missing information can be reconstructed without faults, automatic driving shall be maintained at the highest level of service, compatible with safety requirements.	Demonstration
3.2	50	5	The system architecture supporting cooperative functions shall be devised in order to take into account the hazards identified in the preliminary hazard analysis.	Design
3.2	60	6	In the lowest LoS, the safety and control functions will insure that the speed of each vehicle shall not exceed TBD km/h.	Demonstration
3.2	70	7	In the lowest LoS, the safety and control functions will insure that the distance between each vehicle shall not exceed TBD meters.	Demonstration
3.2	80	8	The system architecture supporting cooperative functions shall be an extension of autonomous driving.	Design
3.2	90	9	The system architecture for cooperative driving shall be based on a set of functionalities that allow autonomous driving.	Design

Requirements				
Section	**ID**	**RID**	**Detail**	**Validation**
3.2	100	10	The system architecture supporting cooperative functions allows the use of external infrastructures following the European standards under way.	Design Demonstration
3.2	110	11	The system architecture supporting cooperative functions shall ensure safety according to ISO 26262. The architecture for cooperative driving shall be based on a set of functionalities that allow autonomous driving.	Design
3.2	120	12	On board architecture for cooperative driving shall comply with ISO 26262.	Design Demonstration
3.2	130	13	Cooperative driving shall be based on V2V requirements defined by ETSI standards or consider possible direction for progress in these areas.	Design
3.2	140	14	Functional safety of cooperative driving shall be ensured. Failures to be considered include those related to communication.	Design Demonstration
3.2	150	15	The reference use case can be chosen from the following list: • adaptive course control • lane changing • crossing of road intersection	Demonstration
3.2	160	16	The architecture can be based on automotive state of the art technologies or in line with the expected trends. For exemplum, automotive busses can be considered (CAN, LIN, Flexray), Autosar approach could be a solution for software architecture, dynamic task allocation shall be avoided, etc.	Design
3.2	170	17	Cooperative driving shall be based on autonomous decisions performed by each vehicle, and not taken by external supervisors.	Demonstration
3.3	10	18	The system solution shall provide means for cooperative vehicles establish a minimum separation distance (Rs) between them correspondingly to a desirable safety level.	Demonstration
3.3	20	19	The system solution shall be applicable for any traffic situation, environment condition, sensor availability or	Demonstration

Requirements				
Section	**ID**	**RID**	**Detail**	**Validation**
			quality of distributed state information	
3.3	30	20	Each vehicle shall be able to determine its own position and the related position uncertainty.	Demonstration
3.3	40	21	UAS shall periodically report its position to other vehicles in surrounding area.	Demonstration
3.3	50	22	The UAS shall include a positioning function that is based on position uncertainty models.	Demonstration
3.3	60	23	The position uncertainty models shall contain the uncertainty related to each specific vehicle and the uncertainty related to the environment external to the vehicle.	Demonstration
3.3	70	24	The position uncertainty model shall consider uncertainties of locally obtained data (due to sensor faults, local component faults) as well as uncertainties of remotely obtained data (due to communication faults, external sensor faults).	Demonstration
3.3	80	25	Each cooperative aerial vehicle shall apply the uncertainty model, fitted to its own characteristics, for the position uncertainty determination	Demonstration
3.3	90	26	The positioning function shall update the environment uncertainty periodically, including, if possible, data from the ATM.	Design
3.3	100	27	The Position Estimator functionality shall provide information of the UAS actual position to other functionalities.	Design Demonstration
3.3	110	28	4DT Navigation functionality shall provide means to follow a trajectory prescribed in position and time.	Design Demonstration
3.3	120	29	Communication functionality shall provide means to the RPV send and receive data information to/from others aircraft, the ATM and the RPV control centre.	Design Demonstration
3.3	130	30	The Conflict Manager functionality shall provide ability to identify traffic conflict with other aircraft and determine a collision avoidance procedure to be executed by the RPV.	Design
3.3	140	31	The Conflict Detection functionality shall provide ability to identify traffic conflict with others aircraft	Demonstration

Requirements				
Section	ID	RID	Detail	Validation
			flying in the same local scenario.	
3.3	150	32	The Conflict Solver functionality shall provide ability to determine a collision avoidance procedure to be executed by the RPV.	Demonstration
3.3	160	33	UAS shall ascertain flight conditions prior to entering non-segregated air space.	Demonstration
3.3	170	34	In the lowest LoS, the safety control will insure that the horizontal distance separation between each vehicle shall not exceed be less than TBD NM.	Demonstration
3.3	180	35	There will be a minimum of TBD seconds between Level of Service modifications.	Demonstration
3.3	190	36	RPV shall be able to recognize communication failure	Demonstration
3.3	200	37	RPV shall keep track on the last authorized 4DT after reception communication failure detection	Demonstration
3.3	210	38	RPV shall keep track on the last authorized 4DT after transmission communication failure detection	Demonstration
3.3	220	39	RPV navigation control system shall be able to compensate for deviation from the 4D-Trajectory, produced by the attitude control system	Demonstration
3.3	230	40	RPV shall start a pre-programmed safety procedure in case of a combined failure of 4DT Navigation and Communication functions;	Demonstration
3.3	240	41	ATM shall apply the uncertainty model to each collaborative aerial vehicle in airspace for the position uncertainty determination	Demonstration
3.3	250	42	The ATM shall provide the environment uncertainty	Demonstration
3.3	260	43	The ATM shall update the environment uncertainty periodically	Demonstration
3.3	270	44	The ATM and each collaborative vehicle shall execute uncertainty consistency crosscheck periodically	Demonstration
4.2	10	45	Each vehicle shall be able to perform several functionalities (services) simultaneously	Design Demonstration

Requirements				
Section	ID	RID	Detail	Validation
4.2	20	46	The set of functionalities shall be extendable	Design
4.2	30	47	We consider functionalities that involve sensing, actuating, and communicating with other vehicles or infrastructure	Design
4.2	40	48	Some resources for sensing, actuating and communication shall be able to be shared among several functionalities	Design Demonstration
4.2	50	49	Functionalities shall always behave safely independently of level of service	Design Demonstration
4.2	60	50	Functionalities shall always operate in the highest possible level of service	Design
4.2	70	51	KARYON's architecture shall be able to express on different levels of abstraction	Design
4.2	80	52	On each level of abstraction and for each architectural element, the level of integrity shall be possible to express w.r.t. each applicable failure.	Design
4.2	90	53	There shall be a known set of rules how to determine the level of integrity for avoiding each possible resulting failure when composing architectural elements.	Design
4.2	100	54	There shall be a known set of rules how to determine the level of integrity for avoiding each possible resulting output failure of an architectural element, given the integrity levels of avoiding the applicable input faults and internal faults	Design
4.2	110	55	There shall be known rules how the amount of, and the quality of, relevant information determines the level of integrity for each relevant failure.	Design
4.2	120	56	The amount of relevant information shall be measurable.	Design Demonstration
4.2	130	57	The quality of relevant information shall be measurable.	Demonstration
4.2	140	58	The cooperative driving architecture shall be exploitable in the near future.	Design
4.2	150	59	Karyon shall define the functional safety requirements in order to allow the definition of the functional safety	Design

Requirements				
Section	**ID**	**RID**	**Detail**	**Validation**
			concept.	
4.2	160	60	Clear assumptions shall be defined at the item level, as concerns any element external to Karyon architecture and interacting with it.	Design
4.2	170	61	Karyon architecture shall be demonstrated to be compliant with functional safety requirements. The demonstration shall be based on the methods recommended by the ISO standard, such as fault injection and back-to-back simulation.	Design Demonstration
4.2	180	62	The architecture shall be able to support significant use cases in terms of: • number of involved vehicles • potential risks in case of failure • relevance of communication in addition to autonomous sensing	Demonstration
4.2	190	63	The selected use cases shall be clearly defined in order to be useful test cases for the verification of the Karyon architecture.	Design
4.2	200	64	Each use case shall be dealt with a description of the scenario, including information on operational condition, so as to allow good risk analysis.	Design
4.2	210	65	Each use case shall be dealt with a description of the operation and vehicle interactions, so as to allow good risk analysis.	Design

Table 4 - Requirements verification matrix

References

[1] ISO26262, first edition 2011-11-15

[2] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable Secur. Comput.* 1, 1 (January 2004), 11-33.

[3] FAR 25 Regulations – sec. 25.1309

[4] RTCA DO-178B/C, Software Considerations in Airborne Systems and Equipment Certification

[5] IEC61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.

Annex A Preliminary hazard analysis and risk assessment of the automotive use cases

Ref. use case	Scenario (safety relevant situation)								
	Locality								
	Location	Road condition					Environmental driving situation	Traffic Situation	Other characteristics
		Adherence	Road Surface	Slope	Route	Regulated priority			
A - Intersection collision warning	Urban road	High µ	Normal	No slope	Crossing	Stop signal	Poor Visibility on the right	A vehicle is overtaking coming from right road on the left lane	None
B - Signal violation warning	Urban road	High µ	Normal	No slope	Crossing	Green light	Poor visibility of the crossing road	Another vehicle is coming from right/left way whitout respecting the red light	None
C - Lane Change Manoeuvre	Urban road	High µ	Normal	No slope	Straigh road	Overcoming vehicle has priority	Poor visibility (blind spot)	Another vehicle is running on the other lane	Dashed line
ACC: D1 - Emergency brake lights D2 - Stationary vehicle warning	Highway	High µ	Normal	No slope	Straigh road	--	Poor visibility of the preceding braking/stationary vehicles	Many preceeding vehicles	--
Intersection management E1 - Traffic light optimal speed advisory	Urban road	High µ	Normal	No slope	Crossing	Green light	Poor visibility of the crossing road	Another vehicle is approaching the crossing from the crossing road	None
Intersection management E2 - Collision Risk Warning from RSU	Urban road	High µ	Normal	No slope	Crossing	Right hand vehicles have priority	Very poor visibility of the crossing road	Another vehicle is approaching the crossing from the crossing road (rigt way)	None
Automatic driving F1 - Co-operative side merging	Highway	High µ	Normal	No slope	Acceleration lane to enter a highway	Main roadway	Very poor visibility of the crossing road	Other vehicles coming from the principal roadway	None
Automatic driving F2 - Co-operative roundabout merging	Urban road	High µ	Normal	No slope	Intersection in roundabout	Priority on roundabout	Normal visibility of the roundabout	Other vehicles in roundabout	None
Automatic driving G- Intersection control	Urban road	High µ	Normal	No slope	Crossing	Priority on the right hand	Poor visibility of the left and right roads	Other vehicles on the crossing roads	None

Figure 27 – Operational conditions

Scenario (safety relevant situation)													
Driver/vehicle [status before failure]													Persons at risk
Dynamic Driving State				Users condition			Vehicle Condition					Other charact.s	
Speed	Long. accel./ decel.	Lateral accel.	Manoeuvres	Actor	Located	Careful level	Key status	Engine status	Brake status	Clutch status	Other conditions		
Very low speed [v < 20 kph]	Low	Negligible	Proceeding straight	Driver	On-board	High	On	On	Off	On	None	None	Driver, passengers, occupants of other vehicle
Medium speed [v < 70 kph]	Low	Low	Proceeding straight	Driver	On-board	Medium	On	On	Off	On	None	None	Driver, passengers, occupants of the other vehicle
Medium speed [v < 70 kph]	Low	Low	Lane change	Driver	On-board	Medium	On	On	Off	On	None	None	Driver, passengers, occupants of other vehicle
High speed [v < 130 kph]	Low	Negligible	Proceeding straight	Driver	On-board	Low	On	On	Off	On	ACC engaged	None	Driver, passengers, occupants of other vehicle
Medium speed [v < 70 kph]	Low	Negligible	Proceeding straight	Driver	On-board	High	On	On	Off	On	None	None	Driver, passengers, occupants of other vehicle
Medium speed [v < 70 kph]	Low	Low	Proceeding straight	Driver	On-board	Medium	On	On	Off	On	None	None	Driver, passengers, occupants of other vehicle
Medium Speed [V < 110 kph]	High	Low	Automatic insertion in principal roadway	Driver	On Board	Low	On	On	Off	On	Automatic driving engaged	None	Driver, passengers, occupants of the other vehicle
Low Speed [V < 40kph]	Low	Low	Insertion in roundabout	Driver	On Board	Low	On	On	Off	On	Automatic driving engaged	None	Driver, passengers, occupants of other vehicle
Very Low Speed [V < 30kph]	Low	Negligible	Proceeding straight	Driver	On Board	Low	On	On	Off	On	Automatic driving engaged	None	Driver, passengers, occupants of other vehicle

Figure 28 – Operating modes

Ref. use case	Failure/ malfunction/ (effects in terms of functional outputs)	Hazard		External measures	Expected task of persons for averting danger
		ID	Description		
A - Intersection collision warning	M1 = intersection collision warning unavailable/false negative	**H1**	Collision with the overtaking vehicle	None	Driver can try to stop the vehicle
B - Signal violation warning	M2 = Signal violation warning unavailable/false negative	**H2**	Collision with the vehicle coming from the crossing road	None	Driver can try to stop the vehicle
C - Lane Change Manoeuvre	M3 = Lane change warning unavailable/false negative	**H3**	Collision with the vehicle running on the other lane	External rear mirror. Honking by the other vehicle	Driver can try to stop the manouver
ACC: D1 - Emergency brake lights D2 - Stationary vehicle warning	M4 = Emergency electronic "brake lights" warning unavailable/false negative	**H4**	Bumping into the front vehicle due to an excessive deceleration whitout adequate recovery with ACC	ACC	Driver can try to stop the vehicle
Intersection management E1 - Traffic light optimal speed advisory	M5 = Incorrect information of traffic light status	**H5**	Collision with the overcoming vehicle	Traffic light	Driver can try to stop the vehicle
Intersection management E2 - Collision Risk Warning from RSU	M6 = Signal of collision risk warning unavailable/false negative	**H6**	Collision with the vehicle coming from the crossing road	None	Driver can try to stop the vehicle
Automatic driving F1 - Co-operative side merging	M7 = Signal of presence of vehicles for co-operative side merging unavailable/false negative	**H7**	Collision with the vehicle coming from the main roadway	External rear mirror. Honking by the other vehicle	Driver can try to stop/decelerate the vehicle, but due to low careful level it should be expected that the reaction is too late or missing.
Automatic driving F2 - Co-operative roundabout merging	M8 = Signal of presence of vehicles for co-operative roundabout merging unavailable/false negative	**H8**	Collision with the vehicle coming from the roundabout	none	Driver can try to stop/decelerate the vehicle, but due to low careful level it should be expected that the reaction is too late or missing.
Automatic driving G- Intersection control	M9 = intersection control collision warning unavailable/false negative	**H9**	Collision with the vehicles coming from the crossing roads	none	Driver can try to stop/decelerate the vehicle, but due to low careful level it should be expected that the reaction is too late or missing.

Figure 29 – Hazards and expected tasks for averting danger

Ref. use case	Controllability		Accidential scenario if controllability task will fail		Loss and damage		Probability of exposition		ASIL
	C	Comment	State changes	Consequence	S	Comment	E	Comment	
A - Intersection collision warning	C2	The visibility is low, the vehicle speed is quite low to allow stopping but the driver expects to receive the right information and therefore he could not be ready to stop the vehicle in time.	Vehicle halted in the middle of the cross	The overtaking vehicle at medium speed (50 kph) collides with the vehicle	S3	Severe injuries could be expected due to lateral impact, in particular for the occupants of the right side.	E2	Not so often. Probability of being in a cross with an other vehicle in overtaking coming from an intersection	A
B - Signal violation warning	C3	The visibility is low and the vehicle speed is medium. It is difficult to stop the vehicle before the collision	Vehicle halted in the middle of the cross	The other vehicle coming from the intersection collides with the vehicle	S3	Severe injuries could be expected, due to lateral impact	E2	Not so often	B
C - Lane Change Manoeuvre	C2	The visibility is low and the vehicle speed is medium. It is difficult to stop the manouver before the collision. In many case the *External Measures* can make the controllability easier.	Vehicle changes lane. Vehicle stays on lane.	The other vehicle coming from the other lane collides with the left/right side vehicle. The vehicle bumps the front	S2	Injuries could be expected, due to the impact	E3	Normal driving	A
ACC: D1 - Emergency brake lights D2 - Stationary vehicle warning	C3	The hazardous situation is shaded by the preceding front vehicles, the speed is high, the careful level is quite low and delays the human intervention. Moreover, in any case, the ACC cannot react in time.	ACC intervention with an automatic braking	Bumping due to an excessive deceleration the front vehicle whitout adequate recovery with ACC	S3	Severe injuries could be expected, due to the impact	E2	Normal driving	B
Intersection management E1 - Traffic light optimal speed advisory	C0	The driver respects the traffic light that passes from green to yellow	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	QM
Intersection management E2 - Collision Risk Warning from RSU	C3	The visibility is low and the vehicle speed is medium. It is difficult to stop the vehicle before the collision	Vehicle halted in the middle of the cross	The other vehicle coming from the crossing road collides with the vehicle	S3	Severe injuries could be expected, due to lateral impact	E2	Not so often.	B
Automatic driving F1 - Co-operative side merging	C3	The visibility is low (blind spot), the vehicle speed is high and the driver expects that the automatic driving system manages the situation.	Vehicle enters the main road	The other vehicle coming from the other lane collides with the vehicle, causing an accident involving two or more cars	S3	Severe injuries could be expected, due the impact at high speed, involving many persons	E4	Often	D
Automatic driving F2 - Co-operative roundabout merging	C3	The visibility is medium and the vehicle speed is low. It is quite difficult to stop the vehicle before the collision, because the driver is able to recognize the hazardous situation too late	Vehicle enters the roundabout	The other vehicle coming from the roundabout collides with the vehicle	S2	Severe injuries could be expected, due to lateral impact	E4	Often	C
Automatic driving G- Intersection control	C3	The visibility is low, the vehicle speed is low and the driver expects that the automatic driving system manages the situation.	Vehicle halted in the middle of the crossing	The other vehicles coming from the crossing roads collides with the vehicle	S1	Light injuries could be expected due to lateral impact at very low speed.	E4	Often	B

Figure 30 – Controllability, severity and probability of exposure and consequent ASILs

Ref. use case	Safety goal ID	Safety goal	Safe state
A - Intersection collision warning	SG1	To alert the driver that the warning information is unavailable	Warning function turned off
B - Signal violation warning	SG2	To alert the driver that the warning information is unavailable	Warning function turned off
C - Lane Change Manoeuvre	SG3	To alert the driver that the warning information is unavailable	Warning function turned off
ACC: D1 - Emergency brake lights D2 - Stationary vehicle warning	SG4	To increase the safety distance of ACC control and alert the driver that the warning information is unavailable.	Warning function turned off. ACC control in safe distance mode.
Intersection management E1 - Traffic light optimal speed advisory	SG5		
Intersection management E2 - Collision Risk Warning from RSU	SG6	To alert the driver that the warning information is unavailable	Warning function turned off
Automatic driving F1 - Co-operative side merging	SG7	To alert the driver that the control function is unavailable	Control function turned off, leaving the engine brake
Automatic driving F2 - Co-operative roundabout merging	SG8	To alert the driver that the control function is unavailable	Control function turned off, leaving the engine brake
Automatic driving G- Intersection control	SG9	To alert the driver that the control function is unavailable	Control function turned off, leaving the engine brake

Figure 31 – Safety goals and safe states

Annex B Preliminary hazard analysis and risk assessment of the avionics use cases

1. The 4-Dimensional Trajectory function (1)	
Function description	Aerial vehicle ability to follow a specific spatial trajectory in a prescribed timing and within a limited deviation to a nominal value.
Failure condition	Total loss of UAS capability to follow a 4D-T
Phase operation	On route with reference to the UAS monitoring use case.
Effect	The UAS departs from the authorized 4D-Trajectory and interferes with other aircraft in-flight or assets/people on the ground.
Classification	Catastrophic
Functional requirement	1. UAS needs to recognize the failure, and 2. UAS needs to activate an emergency procedure
Verification methods	Simulation

1. The 4-Dimensional Trajectory function (2)	
Function description	Aerial vehicle ability to follow a specific spatial trajectory in a prescribed timing and within a limited deviation to a nominal value.
Failure condition	Malfunction: partial loss or intermittent loss of a sub-function, see below;
Phase operation	On route with reference to the UAS monitoring use case.
Effect	Significant deviation from the authorized 4D-T in a systematic mode.
Classification	Major
Functional requirement	1. UAS needs to detect the deviation outside the limit, and 2. UAS needs to recovery the authorized 4D-T
Verification methods	Simulation

1.2 Attitude control function	
Function description	This function controls the UAS angles and movements around the longitudinal, lateral and vertical axis.
Failure condition	1. Total loss of movements control around 1 axis, or 2. Malfunction of movements control around 1 axis
Phase operation	On route with reference to the UAS monitoring use case.
Effect	Small deviation from the authorized 4D-T in a systematic mode.
Classification	Minor
Functional requirement	1. UAS needs to detect the deviation outside the limit, and 2. the navigation control needs to compensate the deviation to the limits.
Verification methods	Simulation

1.3 Thrust control function (1)	
Function description	Thrust function controls UAS longitudinal acceleration.
Failure condition	Total loss of thrust function (engine out)
Phase operation	On route with reference to the UAS monitoring use case.
Effect	The UAS departs from the authorized 4D-Trajectory and interferes with other aircraft in-flight or assets/people on the ground.
Classification	Catastrophic
Functional requirement	1. UAS needs to recognize the failure and 2. UAS needs to activate an emergency procedure.
Verification methods	Simulation

1.3 Thrust control function (2)	
Function description	Thrust function controls UAS longitudinal acceleration.
Failure condition	Malfunction: partial or intermittent loss of thrust function
Phase operation	On route with reference to the UAS monitoring use case.
Effect	Significant deviation from the authorized 4D-Trajectory in a systematic mode.
Classification	Hazardous
Functional requirement	1. UAS needs to detect the deviation outside the limit, and 2. the navigation control needs to compensate the deviation to the limits.
Verification methods	Simulation

1.4 Navigation control function (1)	
Function description	Aerial vehicle ability to follow a specific spatial trajectory within a limited deviation to a nominal value. The observed flown position can be calculated from GPS, INS or GPS and INS information.
Failure condition	Total loss of UAS capability to follow a spatial trajectory
Phase operation	On route with reference to the UAS monitoring use case.
Effect	The UAS departs from the authorized 4D-Trajectory and interferes with other aircraft in-flight or assets/people on the ground.
Classification	Catastrophic
Functional requirement	1. UAS needs to recognize the failure, and 2. UAS needs to activate an emergency procedure
Verification methods	Simulation

1.4 Navigation control function (2)	
Function description	Aerial vehicle ability to follow a specific spatial trajectory within a limited deviation to a nominal value. The observed flown position can be calculated from GPS, INS or GPS and INS information.
Failure condition	Malfunction or degraded function to follow a spatial trajectory based uniquely on GPS, INS or GPS+INS information.
Phase operation	On route with reference to the UAS monitoring use case.
Effect	Small deviation from the authorized 4D-T in a systematic mode.
Classification	Minor
Functional requirement	
Verification methods	Simulation

1. The 4-Dimensional Trajectory function (3)	
Function description	Aerial vehicle ability to follow a specific spatial trajectory in a prescribed timing and within a limited deviation to a nominal value.
Failure condition	Total loss of Attitude and Navigation control function
Phase operation	On route with reference to the UAS monitoring use case.
Effect	The UAS departs from the authorized 4D-Trajectory and interferes with other aircraft in-flight or assets/people on the ground.
Classification	Catastrophic
Functional requirement	1. UAS needs to recognize the failure, and 2. UAS needs to activate an emergency procedure
Verification methods	Simulation

1. Communication function	
Function description	UAS capability to exchange digital data with others entities.
Failure condition	1. Total loss of communication, or 2. malfunction: corrupted or intermittent signal

Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**UAS is unable to inform its position and receive information or commands to/from external entities**
Classification	**Major**
Functional requirement	**UAS need to recognize the failure and to keep track on the last authorized 4D-T**
Verification methods	**Simulation**

1.1 UAS x UAS control centre communication function	
Function description	**UAS capability to receive commands and send information to the UAS ground control centre. Usually this function is available in a limited airspace distance range around some grounded antenna.**
Failure condition	**1. Total loss of communication, or 2. malfunction: corrupted or intermittent signal**
Phase operation	**On route**
Effect	**UAS is unable to inform its position and receive information or commands to/from external entities**
Classification	**Major**
Functional requirement	**UAS need to recognize the failure, keeping the last authorized 4D-T**
Verification methods	**Simulation**

1.2 Communication UAS x ATM control centre function	
Function description	**UAS capability to receive and send information to the ATM control centre. This function should be available through a large ground based radio-frequency network.**
Failure condition	**1. Total loss of communication, or 2. malfunction: corrupted or intermittent signal**
Phase operation	**On route**
Effect	**UAS is unable to inform its position and receive information or commands to/from external entities**
Classification	**Major**
Functional requirement	**UAS need to recognize the failure, keeping the last authorized 4D-T**
Verification methods	**Simulation**

1.3 Communication UAS x aircraft function	
Function description	**UAS capability to send its position and time clock to other aircrafts sharing a common airspace in a broadcasting mode.**
Failure condition	**1. Total loss of communication, or 2. malfunction: corrupted or intermittent signal**
Phase operation	**On route**
Effect	**UAS is unable to inform its position and receive information or commands to/from external entities**
Classification	**Major**
Functional requirement	**UAS need to recognize the failure, keeping the last authorized 4D-T**
Verification methods	**Simulation**

3. Sense & Avoid function	
Function description	**UAS is able to recognize others vehicles flying in the airspace around itself and to perform a quick manoeuvre deviating to the traffic;**
Failure condition	**Total loss of sense capacity**
Phase operation	**On route**
Effect	**UAS is unable to recognize any object around itself**
Classification	**No safety hazards**
Functional requirement	

Verification methods	**Simulation**

3.1 Sense function	
Function description	**UAS is able to recognize others vehicles flying in the airspace by a mapping received from the ATM, a mapping composed from ADS-B or an on-board radar system;**
Failure condition	**Total loss of sense capacity**
Phase operation	**On route**
Effect	**UAS is unable to recognize any object around itself**
Classification	**No safety hazards**
Functional requirement	
Verification methods	**Simulation**

3.2 Avoid function	
Function description	**UAS ability to perform a quick manoeuvre deviating from a conflict situation with others vehicles.**
Failure condition	**Total loss of sense capacity**
Phase operation	**On route**
Effect	**UAS is unable to recognize any object around itself**
Classification	**No safety hazards**
Functional requirement	
Verification methods	**Simulation**

4. Remote control function	
Function description	**UAS capability to transfer the flight control command to the UAS control centre.**
Failure condition	**Total loss of sense capacity**
Phase operation	**On route**
Effect	**UAS is unable to recognize any object around itself**
Classification	**No safety hazards**
Functional requirement	
Verification methods	**Simulation**

5. Communication system (1)	
System description	**The communication system is composed by two independent digital data channels, transmission and reception channels.**
Failure condition	**1. Total loss of reception channel, and/or 2. malfunction: corrupted or intermittent signal on reception channel**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**UAS is able only to transmit information data**
Classification	**Minor**
Functional requirement	**UAS need to recognize the reception failure and to keep track on the last authorized 4D-T**
Verification methods	**Simulation**

5. Communication system (2)	
System description	**The communication system is composed by two independent digital data channels, transmission and reception channels.**
Failure condition	**1. Total loss of transmission channel, and/or 2. malfunction: corrupted or intermittent signal on transmission channel**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**UAS is only able to receive data information, becoming a non-collaborative vehicle in the traffic airspace.**

Classification	**Major**
Functional requirement	
Verification methods	**Simulation**

5. Communication system (3)	
System description	**The communication system is composed by two independent digital data channels, transmission and reception channels.**
Failure condition	**Total loss of reception & transmission channel**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**UAS is able only to transmit information data**
Classification	**Catastrophic**
Functional requirement	**UAS need to recognize the communication failure loss and to start some pre-defined procedure in autonomous mode.**
Verification methods	**Simulation**

5. Communication system (4)	
System description	**The communication system is composed by two independent digital data channels, transmission and reception channels.**
Failure condition	**Malfunction: corrupted or intermittent signal on reception & transmission channels**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**UAS is able only to transmit information data**
Classification	**Major**
Functional requirement	
Verification methods	**Simulation**

5. Longitudinal control system	
System description	**System composed by a logical unit, command wheel and elevator control surface**
Failure condition	**1. Total loss of longitudinal control system 2. malfunction of longitudinal control system**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**Deviation of the authorized 4D-Trajectory**
Classification	**Minor**
Functional requirement	**UAS navigation control system needs to compensate the deviation recovering the track**
Verification methods	**Simulation**

5. Combined Failure: 4D-Trajectory system & Communication system (1)	
System description	**1. 4D-Trajectory System: attitude, thrust and control systems 2. Communication system: transmission and reception channels**
Failure condition	**1. Total loss of the 4D-Trajectory system, combined with 2. corrupted or intermittent reception channel**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**The UAS departs from the authorized 4D-Trajectory, but is still observable by the ATM. It requires traffic priority, or it may interfere with other aircraft in-flight or assets/people on the ground.**
Classification	**Hazards**
Functional requirement	**UAS must be able to detect and identify the combined failure. UAS must start emergency procedure**
Verification methods	**Simulation**

5. Combined Failure: 4D-Trajectory system & Communication system (2)	
System description	**1. 4D-Trajectory System: attitude, thrust and control systems**

	2. Communication system: transmission and reception channels
Failure condition	**1. Total loss of the 4D-Trajectory system, combined with 2. corrupted or intermittent transmission channel**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**The UAS departs from the authorized 4D-Trajectory but may be remote controlled. It becomes a non-collaborative traffic.**
Classification	**Hazards**
Functional requirement	**UAS control center must activate remote control. UAS must be able to detect and identify the combined failure UAS. If UAS centre do not engage remote control UAS, must start emergency procedure**
Verification methods	**Simulation**

5. Combined Failure: 4D-Trajectory system & Communication system (3)	
System description	**1. 4D-Trajectory System: attitude, thrust and control systems 2. Communication system: transmission and reception channels**
Failure condition	**1. Total loss of the 4D-Trajectory system, combined with 2. Total loss of communication system**
Phase operation	**On route with reference to the UAS monitoring use case.**
Effect	**The UAS departs from the authorized 4D-Trajectory and interferes with other aircraft in-flight or assets/people on the ground.**
Classification	**Catastrophic**
Functional requirement	**UAS must be able to detect and identify the combined failure. UAS must start emergency procedure**
Verification methods	**Simulation**

End of Document

