Kernel-based ARchitecture for safetY-critical cONtrol

KARYON

FP7-288195

D1.3 – Standards Analysis Report

Work Package	WP1		
Due Date	M18	Submission Date	2013-06-17
Main Author(s)	Pedro Costa (GMV)		
Contributors	Rolf Johansen (SP) José Parizi (EMB) Renato Librino (4SG) Siavash Aslanihajiabadi (4SG) Jeferson Souza (FFCUL)		
Version	V1.0	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Automotive standards, Avionics standards		
Reviewers	José Parizi (EMB) Siavash Aslanihajiabadi (4SG)		

Part of the Seventh

Framework Programme

Funded by the EC - DG INFSO

Version history

Rev	Date	Author	Comments
V0.1	2013-05-03	Pedro Costa (GMV)	Document release for revision
V0.2	2013-05-07	Pedro Costa (GMV)	Updated according to SVN Template changes.
V0.3	2013-06-03	Pedro Costa (GMV)	Update following partner revision.
V0.4	2013-06-07	Pedro Costa (GMV)	Updated following revision by Embraer and 4SG.
V1.0	2013-06-17	António Casimiro (FFCUL)	Final review and submission.

Glossary of Acronyms

ACARS	Aircraft Communications Addressing and Reporting System
ACC	Adaptive Cruise Control
ADS	Automatic Dependent Surveillance
ADSF	Automatic Dependent Surveillance Function
ADSU	Automatic Dependent Surveillance Unit
ADS-B	Automatic Dependence Surveillance – Broadcast
AFDX	Avionics Full-Duplex Switched Ethernet
AOA	ACARS Over AVLC
APEX	APplication Executive
ASIC	Application Specific Integrated Circuits
ASIL	Automotive Safety Integrity Level
ATC	Air Traffic Control systems
ATN	Aeronautical Telecommunications Network
AVLC	Aviation VHF link control
BSA	Basic Set of Applications
CAM	Co-operative Awareness Messages
CCA	Common Cause Analysis
CMA	Common Mode Analysis
CPDLC	Control to Pilot Data Link Communication
CPM	Core Processing Module
CPIOM	Core Processing Module Input/Output
DAB	Digital Audio Broadcasting
DENM	Decentralized Environmental notification Messages
DoW	Description of Work
DSRC	Dedicated Short Range Communications
DVB	Digital Video Broadcasting
Dx.y	Deliverable belonging to work package x, with serial number y
EASA	European Aviation Safety Agency
ES	Extended Squitter
ETSI	European Telecommunications Standards Institute
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FIS-B	Flight Information Service - Broadcast
FMEA	Failure Mode and Effects Analysis

FMES	Failure Modes and Effects Summary
FPGA	Field Programmable Gate Arrays
FTA	Fault Tree Analysis
G5	5 GHz communication for ITS
HAS	Hardware Accomplishment Summary
HFDL	HF Data Link
HMI	Human Machine Interface
HVP	Hardware Verification Plan
I2V	Infrastructure to Vehicle
IMA	Integrated Modular Avionics
ISM	Industrial, Scientific , and Medical
ITS	Intelligent Transport System
KARYON	Kernel-based ARchitecture for safetY-critical cONtrol
LDM	Local Dynamic Map
LIDAR	Light Detection And Ranging
LRM	Line Replaceable Module
LRU	Line Replaceable Unit
MAC	Medium Access Control
MASPS	Minimum Aviation System Performance Standards
PHAC	Plan for Hardware Aspects of Certification
PHY	Physical Layer
PICS	Protocol Implementation Conformance Statement
PLD	Programmable Logic Devices
PRA	Particular Risks Analysis
QoS	Quality of Service
RCP	Required Communication Performance
RMS	Rate Monotonic Schedule
RSU	Road Side Unit
SAE	Society of Automotive Engineers
SATCOM	Satellite Communication
SDO	Standards Development Organizations
SEooC	Safety element out of the context
SSR	Secondary Surveillance Radar
STDMA	Self-Organizing Time Division Multiple Access
TCAS	Traffic Collision Avoidance System
TDMA	Time Division Multiple Access
TIS-B	Traffic Information Service – Broadcast

TVRA	Threat, Vulnerability and Risk Analysis
T-DMB	Terrestrial Digital Multimedia Broadcasting
Tx.y	Task belonging to work package x, with serial number y
UAT	Universal Access Transceiver
V2I	Vehicle to Infrastructure
V2X	Vehicle to Infrastructure or Vehicle
V2V	Vehicle to Vehicle
VANET	Vehicular Ad Hoc Network
VDL	Very High Frequency Data Link
VDR	VHF Digital Radio
VHF/HF	Very High Frequency/High Frequency
VLC	Visible Light Communication
WAVE	Wireless Access in Vehicular Environments
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Network
WPx	Work Package with serial number x
ZSA	Zonal Safety Analysis

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 the standards currently enforced in the two selected domains, the automotive and the avionics, and providing a study result on the commonalities and dissimilarities of them. From this it may be possible to establish a roadmap of how to standardise in the future the KARYON solution as well as how to transpose its concept into other autonomous vehicles domains. As stated in the DoW:

"One secondary objective of the two tasks is the study of the standards being considered for the project in the avionics and the automotive industry and the assessment of how the requirements being defined and the use cases may contribute to those standards."

Therefore, the present deliverable is devoted to the analysis of the standards enforced in the two domains under study, concluding about the similarities and roadblocks between them.

The deliverable is divided into five separate sections:

- Introduction – This section will provide the introduction to the KARYON concept
- Standards – This section will describe the standards under analysis and provide an analysis concerning those standards.
- Roadmap for KARYON – This section will define a roadmap for the future standardisation KARYON concept.
- Conclusions – This section will provide the conclusion taken at the time this deliverable was written based on the analysis of the standards and the requirements.

Table of Contents

1. Introduction 9
1.1 Context and Problems 9
2. Standards 10
2.1 Introduction 10
2.2 Automotive 10
2.2.1 ISO 26262 11
2.2.2 AUTOSAR 14
2.2.3 802.15 15
2.2.4 ETSI EN 302 665 Intelligent Transport Systems (ITS); Communications Architecture 16
2.2.5 ETSI TR 102 638 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions 18
2.3 Avionics 18
2.3.1 RTCA DO-178B/ED-12B 18
2.3.2 RTCA DO-254/ED-80 22
2.3.3 ARINC 653 25
2.3.4 Additional Protocols and Guidelines 28
2.3.5 Communication technologies 28
2.4 Analysis 32
2.5 Other Domains 35
3. Roadmap for KARYON 37
3.1 Objective 37
3.2 Requirements 37
4. Conclusions 39
References 40

List of Figures

Figure 1: Safety Standards 10
Figure 2: Sequence of Events for a Software Error to lead to a Failure Condition. 19
Figure 3: Hazard Condition Categorization. 20
Figure 4: System Development Assurance Levels. 23
Figure 5: Detailed System Development Assurance Levels. 23
Figure 6: Federated Architecture (example). 25
Figure 7: Federated Architecture to IMA. 26
Figure 8: ARINC 653 Ports. 27
Figure 9: ASIL Risk Decomposition. 32
Figure 10: IEC 61508 Risk Matrix. 32
Figure 11: ARP4754 Risk Matrix. 33

List of Tables

Table 1: KARYON Terminology. 12

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 improves 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 (in the provision of some 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.

2. Standards

2.1 Introduction

This section will provide a description of the standards relevant to KARYON, an analysis of how those standards affect the KARYON concept as well as a comparison between the standards if they refer to different domains. The objective is to provide a comprehensive analysis of the commonalities of the standards, extract if possible additional requirements applicable to KARYON and attempt to expand the concept into other transportation domains.

The two domains targeted by the KARYON concept are the automotive and the avionics. The key standards considered for these domains are the ISO26262 and AUTOSAR for the automotive and the RTCA DO-178B/C and RTCA DO-254 for the avionics. One other standard to be considered for support of the ISO 26262 in the automotive domain is AUTOSAR. An analysis of the standards will be detailed in the following sections. It should be noted that many of the standards have proprietary clauses in them and that although a comprehensible analysis can be performed it cannot be openly written containing information present in those standards.

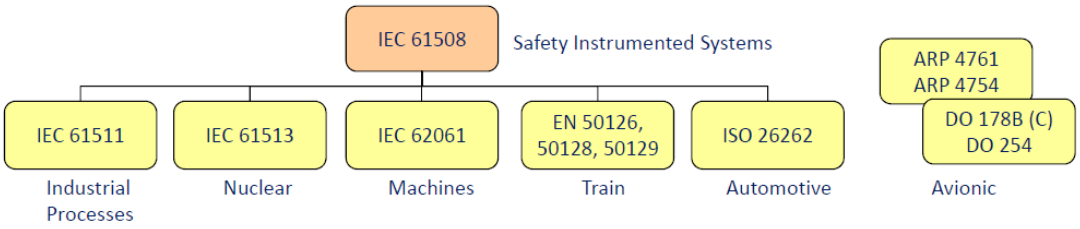

Figure 1: Safety Standards.

Figure 1 provides a description of the key safety standards currently considered in the industry. Although there are others, and we will name them in following sections, this picture describes the connection between safety standards. Note the separation between the avionics and the remaining domains in the figure above. Indeed the safety standards for avionics appear to be fully separate from the remaining domains. We will perform an analysis on the differences and similarities between the two domains and strive to reach conclusions if the KARYON concept can begin the closing of the gaps between them.

We will not analyze IEC 61508 in this document, apart from a brief mention here.

2.2 Automotive

From a KARYON perspective we can regard the standard on functional safety for road vehicles (ISO26262) as guiding in the following steps:

- Determining the safety goals and their ASIL attributes for a given functionality.
- Break-down of safety goals to functional safety concept.
- Allocated functional safety requirements having ASIL attributes.
- Break down of functional safety concept to technical safety concept.
- Allocated technical safety requirements having ASIL attributes.
- Implications on system design and verification methods from technical safety concept.

- Tables prescribing different methods depending on ASIL.
- Break down of technical safety concept to hardware and software allocated safety requirements
- Allocated hardware safety requirements having ASIL attributes.
- Allocated software safety requirements having ASIL attributes.
- Implications on hardware design and verification methods from allocated hardware safety requirements.
- Tables prescribing different methods depending on ASIL
- Implications on software design and verification methods from allocated hardware safety requirements.
- Tables prescribing different methods depending on ASIL.

We note that the ISO26262 standard includes also, for example, prescriptions on how to manage development, how to interact between customer and supplier, how to perform assessments, etc. KARYON point of view focuses on guidance in the following ways:

- How to perform the hazard and risk analysis for any functionality (or for any level of service for a given functionality).
- How to identify applicable safety requirements that apply on architectural elements of different levels of abstraction, and also how redundancy strategies have an impact on the integrity level attributes (ASIL).
- Implications on design and verification processes as a consequence of what safety integrity levels (ASIL attributes of safety requirements) that are allocated to a given part of a design.

2.2.1 ISO 26262

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

In D1.1 an introductory description of the main concepts of this standard was given. In the following the results of the analysis of this standard are reported, in relation to KARYON.

Since this ISO 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. In order to identify the requirements applicable to KARYON, some considerations are reported hereafter for each of the 10 parts which the standard is composed of.

2.2.1.1 Part 1: Vocabulary

The terminology defined in the ISO standard contains some specific meanings not widely used in other domains. Some effort is needed to have a common terminology. The table hereafter is a tentative to establish a link between the terminology used in Kayon, which addresses both avionics and automotive domains and is more general, and the terminology used in automotive according to the standard.

KARYON Terminology	ISO 26262 Terminology	Note
Safety constraint	Functional safety requirement Technical safety requirement	
Level of service	Vehicle operating mode	
Safety kernel	N.A. However, the Safety kernel is an *Element* (to be considered as a SEooC)	The Safety Kernel developed by KARYON is a generic element not designed for a specific vehicle model
Integrity	Automotive safety integrity level	
Quality of information	N.A.	ISO 26262 does not consider quality of information, but considers faults and different failure modes
Safety argument	Safety case	The safety case includes the requirements, the arguments that prove that the item is safe and the evidence of that
Use case	Vehicle function & Situation	The situation is the combination of the operational conditions and of the operating modes
Vehicle system	Item	The item can be composed of one or more systems (which includes sensors, processing units and actuators)
Validation	Verification	The verification is the demonstration of the compliance with the requirements at the nearest high level
N.A.	Validation	Validation proves item's safety. Validation is a phase only applicable to an item, at vehicle level and for a specific vehicle model.
Redundancy	ASIL decomposition	

Table 1: KARYON Terminology.

2.2.1.2 Part 2: Management of functional safety

Management of functional safety requires suitable organization and running supporting processes. Some requirements specify what has to be implemented independently from any specific project, for instance the safety culture, the competence management, the quality management during the safety lifecycle, and the tailoring of the safety lifecycle to the company processes. Other requirements are related to the specific projects and include the assignment of the roles and the responsibilities, the planning and the coordination of the safety activities, the progression of the safety lifecycle, the safety case, the safety measures, the audits, and the functional safety assessment.

However, the requirements concerning the safety case can be applied, and only partially, for the activities conducted.

In addition, the approach required to develop generic elements, i.e., elements not specifically designed for a specific item and a vehicle model, shall be applied. These elements are called SEooC (Safety element out of the context).

2.2.1.3 Part 3: Concept phase

The requirements of this phase cannot be fully applied, because they have to be applied in the development of an item, and the objective of KARYON is only to develop the Safety Kernel. On the other side, since the Safety Kernel should be considered as a SEooC, all the activities required to develop a SEooC should be carried out. These activities include the definition of the assumptions; therefore also the concept phase shall be conducted, not as a development activity but as the definition of the assumptions regarding the entire item in which the Safety Kernel is assumed to be integrated and part of it.

2.2.1.4 Part 4: Product development at the system level

Similar considerations as for Part 3 can be done. This phase goes deeply in the design of the system, by defining and allocating the various functional requirements to the system elements. The final result is the definition of the technical requirements of each element (component) and the technical safety concept. Of course not all the components of the system need to be fully specified, but all the safety mechanisms (including diagnostics and recovery functions) involving the Safety Kernel and the other parts of the system shall fully be defined.

Furthermore, the ascending part of the V-cycle requires the availability of the real components, in order to start the integration activities at the different levels (hardware-software level, system level and vehicle level) and to validate the item to ensure the achievement of the safety goal. This ascending part is absolutely outside the perimeter of KARYON.

2.2.1.5 Parts 5 and 6: Product development: hardware level and software level

These parts concern the development of the components (not prototypes) and are outside the perimeter of KARYON.

2.2.1.6 Part 7: Production and operation

These parts are outside the perimeter of KARYON.

2.2.1.7 Part 8: Supporting processes

This part covers processes that are not usually performed in research activities, but only in product development, such as documentation, change management, configuration control, qualification of software and hardware. However, if the Safety kernel will include some software or hardware elements already available, they should be qualified according to the requirements of the Part 8, or at least the requirements that cannot be verified should be pointed out.

2.2.1.8 Part 9: ASIL-oriented and safety-oriented analyses

This part is fundamental for KARYON, because it concerns redundancy concepts and the requirements to apply redundancy to achieve the necessary ASIL. Furthermore, the analysis of dependent failures is another key issue, in order to identify single events or single causes that violate a safety requirement or a safety goal. The safety analysis play a key role to verify the

correctness of the solutions, and several qualitative and quantitative safety analyses methods are recommended, both deductive and inductive methods.

2.2.1.9 Part 10: Guideline on ISO 26262

This part is a guideline and contains useful information to conduct the safety activities. In particular, the parts dealing with SEooC and its development (see use cases), and the diagnostic coverage of sensor data, are of special interest for KARYON.

The following requirements are derived and should be applied to KARYON concept and activities:

- The Safety kernel should comply with ISO 26262, but the application of the standard is limited to some of the requirements contained in the following parts and (as specified in the subsequent KARYON requirements):
  - Part 2: Management of functional safety
  - Part 3: Concept phase
  - Part 4: Product development at the system level
  - Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
  - Part 10: Guideline on ISO 26262
- The sequence of the KARYON activities shall follow the phases required by the standard from the concept phase to the product development phase (only the descending phases of the V-cycle)
- The definition of the KARYON architecture shall be the result of the following phases (as concerns functional safety)
  - Item definition (to identify the vehicle system that KARYON is addressing and its interfaces, and to define the system functionalities)
  - Hazard analysis and risk assessment. It includes the definition of the safety goals and of the safety states
  - Functional safety concept
  - Product development at the system level (up the definition of the technical safety concept, limited to the Safety kernel, as a SEooC, see the next requirement)
- The Safety Kernel should be dealt as a generic element (i.e., not designed for a specific vehicle model). Therefore the definition and the development of the Safety Kernel should meet the requirements related to SEooC.
  - The Safety kernel shall be developed as a part of the item
  - Assumptions shall be defined at the item level, covering the architecture and the interactions between the Safety Kernel and the other architecture elements

The safety case shall be provided by KARYON project, in order to demonstrate that the safety of the item is achieved, at least considering the KARYON perimeter in terms of activities and architecture elements.

2.2.2 AUTOSAR

AUTOSAR is a de facto standard in the automotive domain. It is defined by the AUTOSAR consortium consisting of a large number of companies being vehicle OEMs and suppliers of different tiers. AUTOSAR can be described as providing definitions in three areas.

Firstly, it defines a standardized interface for application software components (SWC). This implies that SWCs can be developed independent of the underlying hardware platform. Furthermore it means that one SWC can communicate with other SWC in a standardized way abstracting whether they are allocated on the same electronic control unit (ECU) or not.

Secondly, AUTOSAR defines middleware architecture of so called basic software modules (BSW). This layered architecture is the enabler of the standardized interface. In this architecture are specified a large number of BSW modules in the areas of services, communication framework, operating system, and microcontroller abstraction.

Last but not least, AUTOSAR specifies a methodology with a number of templates in xml format for exchanging information between companies or for import/export to tools.

At least the following AUTOSAR concepts are identified as relevant for KARYON.

- The Run-Time Environment (RTE). The RTE realizes the concept of the virtual functional bus (VFB). This implies that each SWC only has to know about its port interface, including signals, but nothing about how the signals are communicated to other SWC, may it be over one or several buses or just by shared memory on the same ECU.
- Diagnosis services. Provides generic logging and tracing functionality. Especially can be noted a capability of tracing VFB communication. This means that all signals communicated between SWC can be traced in the RTE and may act as a trigger for a diagnostic trace message.
- The modular basic software architecture. The modular approach with well-defined interfaces in the layered BSW architecture is an enabler for adding more services and concepts without need to changing most of the standard. In later versions of AUTOSAR the scope of the BSW architecture has been extended compared to the pearlier ones. Because of the modular approach, it may be possible to further extend the scope in common versions as well.
- A Mode concept implementing a coordinated switching of modes affecting BSW modules and application software components. There are three different mode levels: vehicle modes, application modes and BSW modes. The mode concept is well integrated with the RTE, implying for example that mode requests can originate from as well local as remote ECUs, in a transparent way from an application component perspective.

Service mechanisms for assuring what in safety context may be called ‘freedom of interference’, such as memory management and watchdog management.

The following requirements are derived and should be applied to KARYON concept and activities:

The general KARYON architecture pattern shall be possible to be instantiated as an extension to AUTOSAR. As per the requirements document, this requirement will be validated only partially as the effort needed to prove this is beyond the capabilities of the project.

2.2.3 802.15

The IEEE 802.15 working group defines a family of standards which specifies the rules and norms that govern wireless short range networks or personal area networks (WPANs). This family of standards describes among other characteristics:

Part 15.1 – It defines the physical layer (PHY) and medium access control (MAC) sub-layer for WPANs based on the Bluetooth standard protocol.

Part 15.2 – It defines mechanisms to facilitate the coexistence of WPANs and wireless local area networks (WLANs), i.e., IEEE 802.11 networks. Both WPANs and WLANs use of the same industrial, scientific, and medical (ISM) frequency band, which is the 2.4 GHz.

Part 15.3 – It defines the specification of high rate WPANs, which may be utilized to transmit traffic with different quality of service (QoS) requirements.

Part 15.4 – It defines the PHY and MAC sub-layer for WPANs that are known as wireless sensors networks (WSNs), which include wireless sensors and actuators networks (WSANs). It provides a time division multiple access (TDMA) mechanism to support the transmission of traffic with real-time restrictions.

Part 15.5 – It defines the rules and mechanisms that must be followed to create WPANs using mesh topologies.

Part 15.6 – It defines a communication standard suitable for medical and personal entertainment domains, which involve the creation of networks around the human body, but not limited to humans.

Part 15.7 – It defines the PHY and MAC sub-layer for visible light communication (VLC), which comprises the use of "visible light" to perform networked communications.

The parts we will focus this study in are 15.1, 15.2, 15.3, 15.4, and 15.5, which special interest in 15.4. As the communication capabilities relate to the automotive domain, the necessity of having standardized wireless communication means and formats is required. Additionally as a future goal of the project is to devise mechanisms through which autonomous cooperative vehicles operate in the real world, how these communication means operate in close proximity with other wireless networks must be taken into account. Although part 15.7 has automotive and avionic as possible target domains, we will not discuss this emergent part in details.

2.2.4 ETSI EN 302 665 Intelligent Transport Systems (ITS); Communications Architecture

Scope: Definition of ITS Communications Architecture for Europe includes the following views:

- Scenario description;
- Functional View and Information View;
- OSI reference model view including:
- Application View,
- Security View,
- Network and Transport View,
- Interface View, Management view;
- Engineering view to support Implementation Guidelines for Interoperability;
- Enterprise/Organizational/Operational view.

Any entity connected to the communication network is considered as a station. Communication architecture of these various stations, including vehicle communication sub-system is covered by the standard.

At different protocol layers, protocols indications are provided. Dedicating amendments to ITS, functionalities from various OSI layers are supplied as facilities.

This standard defines a vehicle communication system which shall be considered as the reference for the development of the Safety Kernel investigated by KARYON. It also presents informative on-board architectures which can be implied in the KARYON.

Focusing on applications more relevant to KARYON project, the standard is analyzed and a brief summary of the identified concepts are provided:

- The concept of Application Priority for communication channel access: The aim is to support the contention management in a single station or in a physical communication channel.
- Facilities, especially:
    - Local Dynamic Maps

      Digital maps supply cooperative systems with many advantages for road safety critical applications. Such maps used in ITS may contain some local information which could be lane-specific (e.g. curbs, pedestrian walking and bicycle paths) or in concern of road furniture (e.g. traffic signs a traffic lines). On the other hand, they may contain the information regarding dynamic objects which are sensed directly or indirectly; identified and reported by other road users. Such map is referred as a Local Dynamic Map (LDM). In order to reference the objects in LDM, spatial queries are made and natural features of objects are implied to determine their dependencies and relations. Additionally the dynamic information corresponding to each object is required to be time-stamped. To the vehicles which are not equipped with digital maps, the LDM containing the location of dynamic objects might also be provided.
    - Support for relevance checking

      This is a facility based on LDM and location referencing. Generic HMI also invokes this facility to present a relevant view to the driver.
- Support for common message management for data exchange between ITS-S applications. In particular:
    - Periodic messages as CAMs (Co-operative Awareness Messages)
- On-board communication architecture (informative), in order to identify the communication interfaces with external stations and with on-board networks, which will be considered in KARYON architecture.

  Note: To identify the on-board architecture and its interfaces with the safety kernel all the mentioned information above should be considered as assumptions. In the case that some of them be proved to be incompatible with cooperative functionalities and their safety operation, advices must be provided and reported to the standardization committees so that the improve of the standard will be possible. KARYON should assume the availability of the following infrastructures and services:
    - V2V communication: ITS-G5, 60 GHz, IR.
    - Roadside stations: V2I and I2V ITS-G5.
    - Collision Risk Warning RSU[1] (Road Side Unit).
- KARYON should assume that vehicles are equipped with 77 GHz RADAR or/and LIDAR systems.

[1] 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.

- KARYON should assume that the cooperative vehicles communicate with the ITS, whose architecture complies with the specifications of ETSI EN 302 665.
- KARYON should assume that the facilities provided by ITS, in particular LDM and support for relevance checking, are available and used to perform the required functionalities envisaged in KARYON use cases.
- KARYON should assume that the support provided by ITS stations to manage Cooperative Awareness Messages is provided by ITS.

KARYON should adopt one of the (informative) on-board communication architectures provided by the standard.

2.2.5 ETSI TR 102 638 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions

Scope: Definition of a V2V / V2I-Communication Basic Set of Applications as a basis for the specification of the basic system.

Defining BSA (Basic Set of Application), this standard mainly focuses on V2V, V2I and I2V communications on the V2X dedicated frequency band but not excluding other access technologies as cell networks (e.g. 2G, 3G, 4G), and / or broadcasting systems (DAB, T-DMB, 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

The basic applications concerning active road safety and cooperative traffic efficiency are more related to vehicle dynamics and to dynamic information exchange among vehicles and also with the infrastructures. Hence these applications are of particular interest for KARYON.

No additional requirements can be derived, because those reported in D1.1 as use cases already cover some of the most significant services defined by the standards and comply with the purpose of KARYON.

2.3 Avionics

2.3.1 RTCA DO-178B/ED-12B

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.

One of the key aspects of the DO-178B standard is that instead of defining very strict requirements concerning the software safety assurance and certification process, it provides a set of guidelines which, when followed, provide sufficient accreditation of the software development process to ease the certification process. This in turn allows the designers and

system engineers to select the best approach, based on the overall system requirements to perform the task. One of the shortcomings of other standards are the strict nature of the requirements, which may be quite adequate for some domains but are sorely lacking in others if followed to the letter of the standard.

The standard is defined in the following major sections:

- System Aspects relating to Software Development
- Software Life Cycle
- Software Planning Process
- Software Development Processes
- Software Verification Processes
- Software Configuration Management Process
- Software Quality Assurance Process
- Certification Liaison Process

2.3.1.1 System Aspects relating to Software Development

This section provides a vision of the system life cycle processes needed to better understand the software related life cycle processes. It covers several topics, of which the following is of particular interest to the KARYON concept: System safety assessment process and software level.

This topic gives an insight into the relationship between software errors and failure conditions, a categorization of those failure conditions and, based on that categorization, a definition and determination of the software level necessary to eliminate or reduce the probability of those conditions occur and the foreseen impact of the failures.

The standard defines the software level of a software component as the designation that is assigned to that component based on the determination of the system safety assessment process. This level is based on the contribution of the software to the potential failure conditions according to the system safety assessment process. This is performed by establishing how an error in one software component relates to the system failure condition(s) and the associated severity of that failure.

According to this standard, only software components in Partitions can be assigned individual software levels by the system safety assessment process. Regarding the concept of Partitions, this will be further detailed in Section 3.3.3.

Figure 2 depicts a sequence of events leading from a software error up to a failure condition at the aircraft level. This is a simplified example, as some errors may have multiple fault scenarios and lead to far more complex and hard to quantify failure conditions.

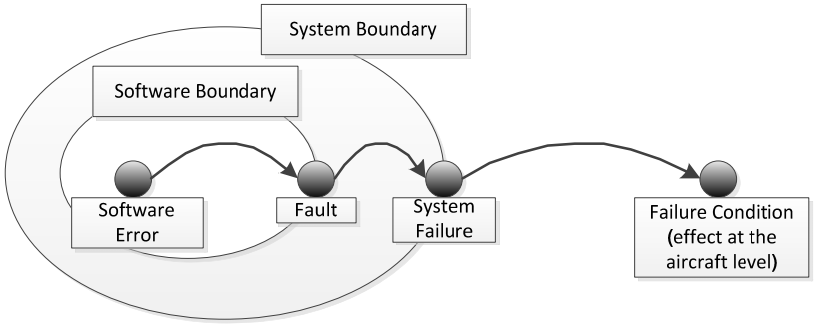

Figure 2: Sequence of Events for a Software Error to lead to a Failure Condition.

The software level is tightly connected to the failure (or hazard) condition categorization. This categorization is defined in five levels, according to the severity of the result of the failure condition occurring, in terms of the effects on the aircraft, the flight crew and the passengers, when applicable.

These levels are described as Hazard Class in the table depicted in Figure 3.

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 3: Hazard Condition Categorization.

From the above failure conditions, five software levels are defined, which can be summarized as:

- Level A – software, which upon partial or complete failure, would cause or contribute to a failure of system function resulting in a catastrophic failure condition of the aircraft.
- Level B - software, which upon partial or complete failure, would cause or contribute to a failure of system function resulting in a hazardous failure condition of the aircraft.
- Level C - software, which upon partial or complete failure, would cause or contribute to a failure of system function resulting in a major failure condition of the aircraft.
- Level D - software, which upon partial or complete failure, would cause or contribute to a failure of system function resulting in a minor failure condition of the aircraft.
- Level E - software, which upon partial or complete failure, would cause or contribute to a failure of system function resulting in a failure condition with negligible effect on the aircraft's operational condition or flight crew workload.

The description of the anomalous behaviour, resulting in the partial or complete failure, of all the above described software, should be defined in accordance with the system safety assessment process. This process determines the software level based on upon the failure condition(s) which result from the anomalous behaviour of the software. This analysis is based upon partial (malfunction) and complete failure of the software. When identifying the categories for failure conditions and determining the software level of the software components, additional considerations may be taken into account for the safety assessment, such as adverse environmental conditions and architectural strategies.

2.3.1.2 Software Life Cycle

This section describes the software life cycle process, the definition of software life cycle and provides some criteria for transition between various life cycle processes. The three software life cycle processes described are the software planning process, the software development process and the quality and configuration processes that manage and control the overall life cycle processes and that ensure the high confidence in the outputs generated by those processes.

The transition criteria between life cycle processes are used to determine if a process may be entered or re-entered. Each life cycle process generates outputs, which can be inputted in other processes or even re-inserted into the life cycle that produced those outputs. This exchange of information depends on determining how the information is recognized, controlled and resolved by the receiving process.

2.3.1.3 Software Planning Process

The software planning process is used to define the means of developing software in order for it to satisfy the requirements and provide the degree of confidence consistent with the software level identified in the safety assessment. Among the objectives of this process is the following: the software development standards are define and are consistent with the safety objectives for the software to be produced.

2.3.1.4 Software Development Processes

The software development processes defined in the standard are Software Requirements process, software design process, software coding process and software integration process.

2.3.1.5 Software Verification Process

This process provides an assessment of the technical outputs of the planning process and the software development processes.

Verification is not simply testing. In general, it cannot be guaranteed the absence of errors through testing alone.

The purpose of the software verification process is to verify that the product is free of errors and in case of detection of such errors to report on them.

2.3.1.6 Software Configuration Management Process

The Software Configuration Management process's purpose is to define control mechanisms to ensure that baselines of all outputs of the previous processes are produced and maintained and to guarantee that monitoring mechanisms are in place for managing the various processes (change management control, error reporting and correction traceability…).

2.3.1.7 Software Quality Assurance Process

The software Quality Assurance process provides confidence that the software life cycle processes are followed in accordance with established standards and guidelines and that the software produced conforms to the requirements defined and is developed to the software level assigned by the software safety assessment process.

2.3.1.8 Certification Liaison Process

This process defines the means, through which communication between the producer of the software and the certification authority is established, also defines what are the necessary steps for ensuring compliance substantiation that the software produced is indeed certifiable to the software level requested.

2.3.1.9 Conclusion

This standard provides a set of guidelines for developing software in accordance with a certain level of safety. It defines five levels of software in accordance with the severity of a system failure to occur and provides guidelines to ensure that, for a given software level assignment, if the indicated life cycle processes are observed and followed, the probability of certifying the software at the requested safety software level is high.

For KARYON, DO-178 provides guidelines for developing the demonstration scenarios in accordance with the software levels or levels of service designed for each scenario. Due to effort concerns, we do not intend to follow the full length of the standard but there those guidelines that ensure that the final demonstration is sufficiently shown to be at that minimum level of service.

2.3.2 RTCA DO-254/ED-80

The RTCA DO-254 document, and its counterpart in Europe EUROCAE ED-80, provides guidelines for design and development of electronic hardware for use in avionic systems. It is a collection of best aviation industry practices for design assurance of airborne electronic hardware to guarantee its safe operation

Historically, the FAA advisory circular AC20-152 recognized the DO-254 as an accepted mean of compliance for qualification of electronic hardware in 2005. After, it becomes an official requirement for suppliers of civil aviation avionics systems.

More specifically, DO-254 is applicable for the design of complex electronic hardware in airborne systems, such as Field Programmable Gate Arrays (FPGAs), Programmable Logic Devices (PLDs), and Application Specific Integrated Circuits (ASICs).

Complex systems, as described on ARP-4754, refers to systems whose safety cannot be shown solely by test and whose logic is difficult to comprehend, without the aid of analytical tools. Typically, these systems are high susceptible to present development errors, as requirements and design errors. Development errors might, in turn, produce undesirable, unintended system effects or failure modes, with potential to result in unsafe aircraft operating conditions.

Since these errors are generally not deterministic and suitable numeric methods are not available to characterize them, qualitative approach, as development assurance methods are used to guarantee that system can satisfy safety objectives.

Development assurance methods establish a structure, the discipline and rigor required for system design and development process, based on the failure condition classifications associated with the aircraft-level functions implemented in the system and item. System development assurance levels (DAL) are defined as:

Failure Condition Classification	System Development Assurance Level
Catastrophic	**A**
Hazardous / Severe Major	**B**
Major	**C**
Minor	**D**
No safety effect	E

Figure 4: System Development Assurance Levels.

Level	Impact of a Failure	Failure Condition	Probability	
			Level	Per Flight Hour
A	Catastrophic	Failure that would prevent continued safe flight and landing.	Extremely Improbable	$<10^{-9}$
B	Hazardous/ Severe-Major	Large reduction in safety margins or functional capabilities, physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.	Extremely Remote	$<10^{-7}$
C	Major	Significant reduction in safety margins or functional capabilities, a significant increase in flight crew workload or in conditions impairing flight crew efficiency, or discomfort to the occupants, possibly including injuries.	Remote	$<10^{-5}$
D	Minor	Slight reduction in safety margins or functional capabilities, a slight increase in flight crew workload, such as routine flight plan changes, or some inconvenience to the occupants.	Probable	$<10^{-3}$
E	No Effect	Failure conditions that do not affect the operational capability of the aircraft or increase the flight crew workload.	–	–

Figure 5: Detailed System Development Assurance Levels.

At a system level, DO-254 rather than specify how to implement the requirements or which test should be completed, it specifies the process of design assurance and certification. According to the document, design assurance is:

All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the hardware satisfies the application certification basis

The standard is defined in the following major sections:

- Introduction
- System Aspects of Hardware Design Assurance
- Hardware Design Life Cycle
- Planning Process
- Hardware Design Processes
- Validation and Verification Process
- Configuration Management Process

- Process Assurance
- Certification Liaison Process
- Hardware Design Life Cycle Data
- Additional Considerations

2.3.2.1 System Aspects of Hardware Design Assurance

The main regulations which must be followed are requirements capturing and tracking throughout the design and verification process. The following items of substantiation are required: Plan for Hardware Aspects of Certification (PHAC), Hardware Verification Plan (HVP), Top-Level Drawing, and Hardware Accomplishment Summary (HAS)

2.3.2.2 Hardware Design Life Cycle

The hardware design and hardware verification need to be done independently. The hardware designer works to ensure the design of the hardware will meet the defined requirements. Meanwhile, the verification engineer will generate a verification plan which will allow for testing the hardware to verify that it meets all of its derived requirements.

2.3.2.3 Hardware Design Processes

- Requirements Capture
- Conceptual Design
- Detailed Design

2.3.2.4 Validation and Verification Process

The validation process provides assurance that the hardware item derived requirements is correct and complete with respect to system requirements allocated to the hardware item.

The verification process provides assurance that the hardware item implementation meets all of the hardware requirements, including derived requirements.

2.3.2.5 Additional Considerations

- Use of Previously Developed Hardware
- Commercial-Off-The Shelf (COTS) Components Usage
- Product Service Experience
- Tool Assessment and Qualification
- Appendix A. Modulation of Hardware Life Cycle Data Based on Hardware Design Assurance Level
- Appendix B. Design Assurance Considerations for Level A and B Functions
- Appendix C. Glossary of Terms
- Appendix D. Acronyms

2.3.2.6 Conclusion

RTCA DO-254 standard has a limited effect on the implementation of KARYON solutions, once it is applicable specifically for logical integrated circuits, as ASIC´s, and depending on the adopted architectural solutions, it might be allocated as a pure software components.

2.3.3 ARINC 653

The avionics domain was dominated for quite some time with a particular operating architecture. This architecture, named federated was based on multiple functions (flight management, communications management, in-flight entertainment, landing gear…) segregated physically. This means that for each avionics function, a dedicated electronics component, named LRU (Line Replaceable Unit) was produced and installed in the avionics bay of the aircraft. Connecting each of these LRUs, a communication protocol was developed, ARINC 429. ARINC 429 was a direct bus connection, based on 32 bit words which linked each LRU to each other it needed to communicate with. Figure 6 provides a simplified example of a typical avionics federated architecture. Each communication channel depicted is a dedicated physical bus connecting the LRUs.

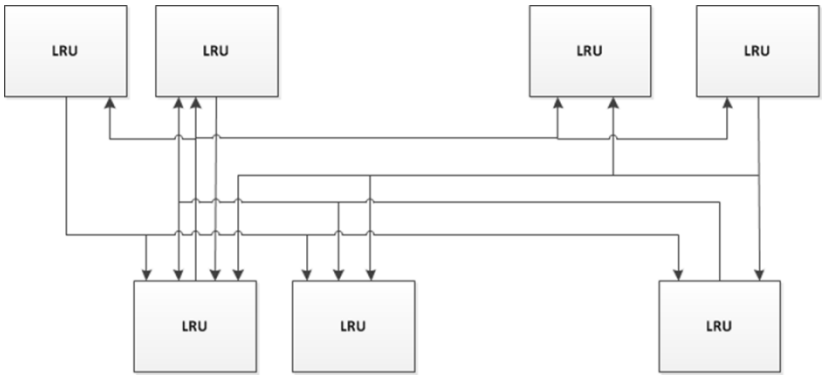

Figure 6: Federated Architecture (example).

This architecture, as can be noticed in Figure 6, had several major roadblocks for new avionics programs. As the number and complexity of the avionics functions evolved, more LRUs and communication physical channels were needed. This made building aircrafts more expensive and led to higher fuel and energy requirements to handle the increased weight and number of equipment's installed.

To alleviate this situation a new architecture paradigm was designed. Named IMA, Integrated Modular Avionics, this led to the replacement of the LRU with a different type of electronic equipment, one with higher computational power and lower energy requirements.

One of these electronics, the Core Processing Module (CPM), was designed to be capable of handling multiple avionics functions simultaneously. However, one of the key aspects of the LRU was that it provided physical segregation in case of failure from other LRUs and therefore allowed for a higher safety level of the whole aircraft.

To assure that the safety level remained identical on the CPM, segregation rules and standards were designed. One of these standards, ARINC 653, defines the API and rules for developing software in an IMA architecture environment.

ARINC 653 defines an APEX (APplication EXecutive) interface between the Operating System and the avionics functions application software. This APEX, defines the behaviour of the IMA system, including scheduling, communication, failure handling...

ARINC 653 is based on a concept of partitioning, both spatially and temporally. The objective is to create virtual LRUs inside the CPM, thus ensuring a similar system than the federated but

with lesser weight, energy requirements and space. Figure 7 depicts the transition from the Federated architecture to an IMA driven architecture, showing a new electronics, LRM (Line Replaceable Module) of type CPIOM. This component is a specialized version of the CPM containing additional functionalities in terms of Input/Output.

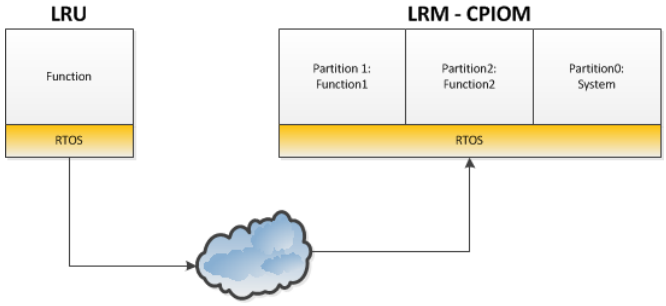

Figure 7: Federated Architecture to IMA.

These partitions follow a strict scheduling scheme, without priority between them, which permit to determine at design time, the most efficient and safe means of operation and also helps to avoid potential starvation of resources in any one partition. Each of the Partitions is expected to emulate one federated LRU and can have multiple processes executing in them. These processes are also subject to scheduling schemes, these with priority associated to them, in order to enforce the correct execution of the needed computational resources. The APEX described by the standard follows strict rules and if used correctly ensures a high level of determinism and provides real time operating systems following the standard with a high degree of safety.

One additional roadblock for the design and production of newer aircrafts was the communication constraints. ARINC 429, based on 32 bit words, had some limitations. Some of these limitations are:

- Low flexibility: each time any new physical equipment is added, additional cabling is necessary to be inserted between all other equipment's communicating with this new one. This led back to an increase in weight and thus in a less efficient final product.
- Low speed: ARINC 429 had two transmission speeds, 12 Kbit/s for low speed transmission and 100 Kbit/s for high transmission speed. This led to the size and frequency of messages exchanged to be constrained due to bandwidth and timing requirements.
- Maximum number of receivers: for a given transmitter the maximum number of supported receivers was 20. This led to an even greater increase of weight due to the necessity of adding additional transmitters for forwarding messages if these messages were required to be delivered to more than 20 receivers.
- Maximum length of cable: the maximum length of cable for ARINC 429 was 100 meters. Granted that this is quite large but it nevertheless imposed a size limitation on the aircraft.

To negate these limitations, a new communication protocol was developed. Some of the requirements for this new protocol were the ability to operate based on COTS protocols, to be capable of higher throughput of messages due to an increased request from the avionics manufacturers for larger transfer of data and the ability to more easily and less costly expand the network if additional equipment's are required.

As such, this new communication protocol, ARINC 664, Part 7 was designed. This new standard, named AFDX (Avionics Full-Duplex Switched Ethernet) was developed in conjunction with ARINC 653. The communication definitions of ARINC 653 inter-Partition services and the services defined by AFDX are quite similar and respect the same naming and functionalities. These services, named Queuing and Sampling Ports, are designed to operate

together, though for the sake of system independency, ARINC 653 port definitions allow for other protocols to be used with them.

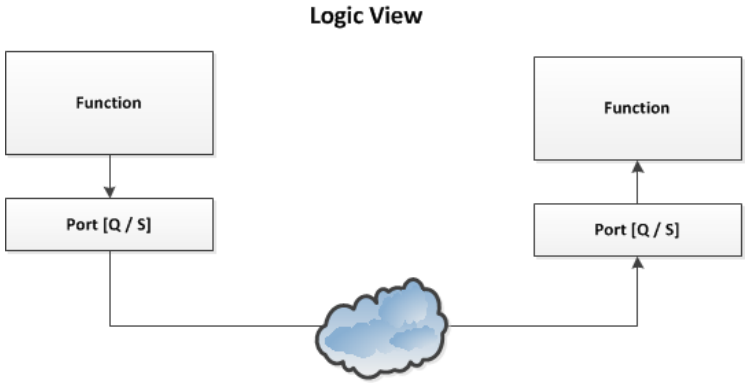

Figure 8: ARINC 653 Ports.

This communication protocol is based on logical communication channels, named VL or Virtual Links that emulate physical links. These VLs are configured at design time to ensure that the communications are deterministic and that any real time requirements can be met if needed. Each VL is configured to have one transmission port, in either queuing or sampling mode or one to various receiving ports in the same mode that the transmission. Queuing ports are used to store data and to ensure that any data sent through them is not lost, while sampling ports only store the last received message. These usually are used for faster communication and or for the transmission of transitory data (data where only the last recorded values are important such as speed or current position) at the expense of the notion of keeping data history.

This communication protocol allows for the reduction of the disadvantages that ARINC 429 suffered from. The maximum speed of transmission possible for a given message varies based on several factors (BAG and MFS primarily).

BAG or Bandwidth Allocation Gap is the minimum guaranteed time interval between message frames, i.e. if one frame is sent at time Tx, the next frame will not be sent before Tx + BAG. This interval is used to ensure that the communication is as deterministic as possible as well as to ensure that collisions in the communication channels do not occur. BAG is always a power of 2 (1, 2, 4, 8, 16…) in the range [1,128] milliseconds.

MFS or Max Frame Size is the maximum size that each message frame is allowed to have in a given communication channel. These vary between 17 and 1471 bytes. At 1471 bytes of MFS and 1 millisecond the real bandwidth for a given VL is 11768 Kbytes/second which when compared with the 100 Kbytes/s and maximum message of 32 bit words of the ARINC 429 protocol provides a good notion of the gains that AFDX provides to the avionics network.

It should be noted that ARINC 653 and indeed the majority of the current avionics standards take into consideration single-core usage and applications. With the increasing attention to multicore applications and with the expected obsolescence of the single-core architecture, more and more efforts are expected to be expended in migrating current solutions to multicore. There are already some programs in Europe [1], studying the possibility of certifying multicore avionics solutions.

2.3.3.1 Conclusion

The segregation between partitions, both spatially and temporally, proves that the concept of safety is possible in the same electronics component and provides a basis for the demonstration of the KARYON concept. Granted that the KARYON concept is more complex than the ARINC 653 partition but some guidelines and rules can be extracted from this standard and applied to KARYON.

Additionally the communication protocol is already proven to be capable of handling high criticality and safety conditions, being used extensively in the avionics domain and thus is also a good basis for the development of communication rules and behaviours for the communication aspects needed to demonstrate the KARYON concept.

2.3.4 Additional Protocols and Guidelines

Additionally to the standards referred above, there is a number of communication protocols and technologies that may be impacted and/or have an impact on the KARYON concept. The main ones are listed below. A more detailed examination is projected during KARYON implementation phase.

ARP4754A, *Guidelines For Development Of Civil Aircraft and* Systems is a guideline from SAE International, dealing with the development processes which support certification of Aircraft Systems.

ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* is a standard (actually a Recommended Practice) from the Society of Automotive Engineers (SAE). In conjunction with SAE ARP4754, ARP4761 is used to demonstrate compliance with 14 CFR 25.1309 in the U.S. Federal Aviation Administration (FAA) airworthiness regulations for transport category aircraft, and also harmonized international airworthiness regulations such as European Aviation Safety Agency (EASA) CS–25.1309.

This Recommended Practice defines a process for using common modeling techniques to assess the safety of a system being put together. The first 30 pages of the document cover that process. The next 140 pages give an overview of the modeling techniques and how they should be applied. The last 160 pages give an example of the process in action.

Some of the methods covered:

- Functional Hazard Assessment (FHA)
- Fault Tree Analysis (FTA)
- Failure Mode and Effects Analysis (FMEA)
- Failure Modes and Effects Summary (FMES)
- Common Cause Analysis (CCA)
- Zonal Safety Analysis (ZSA)
- Particular Risks Analysis (PRA)
- Common Mode Analysis (CMA)

In 2004, SAE began working on Revision A to ARP4761. When released, EUROCAE plans to jointly issue the document as ED–135.

ARP guidelines strive to fully mitigate systems risks at design time of the avionics programs. This leads to extensive and thorough risk analysis and an ever increasing amount of man power as the avionics systems become larger and the avionics platforms become more and more complex. The application of the KARYON concept to some of the analysis through Level of Service analysis and identification can lead to a reduction to that risk analysis effort and therefore to more efficient, cost-wise, future aircraft platforms.

2.3.5 Communication technologies

Fast, accurate, high integrity worldwide data communications the Aeronautical Telecommunications Network (ATN)

A data communication system contains protocols and routings for defined ISO/OSI communication procedures that allowing the end systems (ground and air) to communicate each other's via various kinds of media.

- Transition to the data link communication system; voice as a backup
- Technology improvement on level of accuracy for exchange information and channel capacity
- Remote area : SATCOM, HFDL
- Terminal area : VDL, SSR, and Mode-S
- Required Communication Performance (RCP)
- ATN (Aeronautical Telecommunication Network)
- VHF/HF Voice
- SATCOM
- ACARS / CMU
- CPDLC
- Mode S
- STDMA

2.3.5.1 VDL MODE 2 - Very High Frequency Data Link (VDL) Mode 2

Definition: A Data Link that uses VHF Digital Radio (VDR) to support:

- ACARS Over AVLC communication (AOA) or
- Aeronautical Telecommunications Network (ATN).

2.3.5.2 CPDLC - Control to Pilot Data Link Communication

Definition: Data Link application used by controllers and flight crews as a supplement to voice communications. It allows two way communications between pilot and controller, but using data link instead of voice.

2.3.5.3 ADS-B - Automatic Dependence Surveillance – Broadcast

Definition: ADS-B allows the automatic broadcast transmission of on-board data (e.g. identification, position, time) via a data link. The transmission can be done via transponder (USA, EUROPE, and Australia among others) or radios (Sweden, US – General Aviation).

ADS–B consists of two different services: ADS–B Out and ADS–B In. ADS–B Out periodically broadcast information about each aircraft, such as identification, current position, altitude, and velocity, through an on-board transmitter. ADS–B Out provides air traffic controllers with real-time position information that is, in most cases, more accurate than the information available with current radar-based systems.

ADS-B In is the reception by aircraft of FIS-B and TIS-B data and other ADS-B data such as direct communication from nearby aircraft.

It will replace radar as the primary surveillance method for controlling aircraft worldwide. The ADS-B system can also provide traffic and graphical weather information through TIS-B and FIS-B applications. ADS-B enhances safety by making an aircraft visible, real-time, to ATC

and to other appropriately equipped ADS-B aircraft with position and velocity data transmitted every second.

The system relies on two avionics components — a GPS navigation source and a data-link (ADS-B unit). There are several types of certified ADS-B data links and the most common ones operate at 1090 MHz, essentially a modified Mode S transponder, or at 978 MHz (USA only).

ADS-B system has three main components: 1) Ground Infrastructure, 2) Airborne Component, and 3) Operating Procedures

- A transmitting subsystem that includes message generation and transmission functions at the source; e.g., airplane.
- The transport protocol; e.g., VHF (VDL mode 2 or 4), 1090ES, or 978 MHz UAT.
- A receiving subsystem that includes message reception and report assembly functions at the receiving destination; e.g., other airplanes, vehicle or ground system.

The ADS-B link can be used to provide other broadcast services, such as Traffic Information Service – Broadcast (TIS-B) and Flight Information Service – Broadcast (FIS-B).Another potential aircraft-based broadcast capability is to transmit aircraft measurements of meteorological data.

ADS-B equipment is built to meet one of two sets of US government standards, DO-260B and DO-282B.

Two link solutions are being used as the physical layer for relaying the ADS-B position reports:

- Universal Access Transceiver (UAT)
- 1,090 MHz Mode S Extended Squitter (ES)

Universal Access Transceiver

The term Universal Access Transceiver refers to a data link intended to serve the majority of the general aviation community. It is intended to support not only ADS-B, but also Flight Information Service - Broadcast (FIS-B), Traffic Information Service – Broadcast (TIS-B).

UAT will allow aircraft equipped with "out" broadcast capabilities to be seen by any other aircraft using ADS-B "in" technology as well as by FAA ground stations. Aircraft that are equipped with ADS-B "in" technology will be able to see detailed altitude and vector information from other ADS-B "out" equipped aircraft as well as FIS-B and TIS-B broadcasts

The UAT system is specifically designed for ADS-B operation and is the only ADS-B link standard that is truly bi-directional: UAT users have access to ground-based aeronautical data (FIS-B) and can receive reports from proximate traffic (TIS-B) through a multilink gateway service that provides ADS-B reports for 1090ES equipped aircraft and non-ADS-B equipped Radar traffic.

1090 MHz Mode S Extended Squitter

Europe has not officially chosen a physical layer for ADS-B. A number of technologies are in use. However, the influential EuroControl CASCADE program uses 1090ES exclusively. The Federal Aviation Administration (FAA) accepts 1090 MHz ES and UAT as media for the ADS-B system in the United States, with the 1,090 MHz extended squitter ADS-B link for air carrier and private/commercial operators of high performance aircraft, and Universal Access Transceiver (UAT) ADS-B link for the typical general aviation user.

With 1090ES, the existing Mode S transponder supports a message type known as the extended squitter (ES) message. It is a periodic message that provides position, velocity and time. To enable an aircraft to send an extended squitter message, the transponder is modified and aircraft position and other status information is routed to the transponder. ATC ground stations and aircraft equipped with Traffic Collision Avoidance System (TCAS) already have the necessary

1090 MHz (Mode S) receivers and would only require enhancements to accept and process the additional Extended Squitter information. The technical link standards 1090ES does not support FIS-B service.

2.3.5.4 DO-212 "Minimum Operational Performance Standards for Airborne Automatic Dependent Surveillance (ADS) Equipment":

DO-212 is a performance standard published by RTCA, Incorporated. It contains Minimum Operational Performance Standards (MOPS) for aircraft equipment required for the Automatic Dependent Surveillance (ADS) function (ADSF). The supporting hardware can be a stand-alone ADS unit (ADSU) or alternatively, the ADS function may be installed within other on-board equipment.

2.3.5.5 DO-242A "Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)".

DO-242A is an aviation system standard published by RTCA, Incorporated. It contains Minimum Aviation System Performance Standards (MASPS) for Automatic Dependent Surveillance-Broadcast (ADS-B). These standards specify operational characteristics that should be useful to designers, manufacturers, installers, service providers and users of an ADS-B system intended for operational use on an international basis. DO-242A provides a view of the system-wide operational use of ADS-B, but does not describe a specific technical implementation or design architecture meeting these operational and technical characteristics.

These references are noted in DO-212

- ISO 7498 Information Processing Systems—Open Systems Interconnection—Basic Reference Model
- ISO 8072 Information Processing Systems—Open Systems Interconnection—Transport Service definition
- ISO 8073 Information Processing Systems—Open Systems Interconnection—Connection oriented transport protocol specification
- ISO 8073 Addendum 4 Information Processing Systems—Open Systems Interconnection—Connection oriented transport protocol specification, Protocol enhancements
- ISO 8473 Information Processing Systems—Data Communications—Protocol for providing the connectionless-mode network service
- ISO 8348 Information Processing Systems—Data Communications—Network Services Definition
- ISO 8348 Addendum 1 Information Processing Systems—Data Communications—Network Services Definition, Connectionless-mode transmission
- DO-178 Software Considerations in Airborne Systems and Equipment Certification
- DO-205 Design Guidelines and Recommended Standards To Support Open Systems Interconnection for Aeronautical Mobile Communications. Part 1—Internetworking

2.4 Analysis

One means of communication common to both domains under consideration is the CAN bus. Used in avionics (an example is Airbus A380) and also in automotive it provides a good term of comparison between the usages of common components between the two domains.

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.

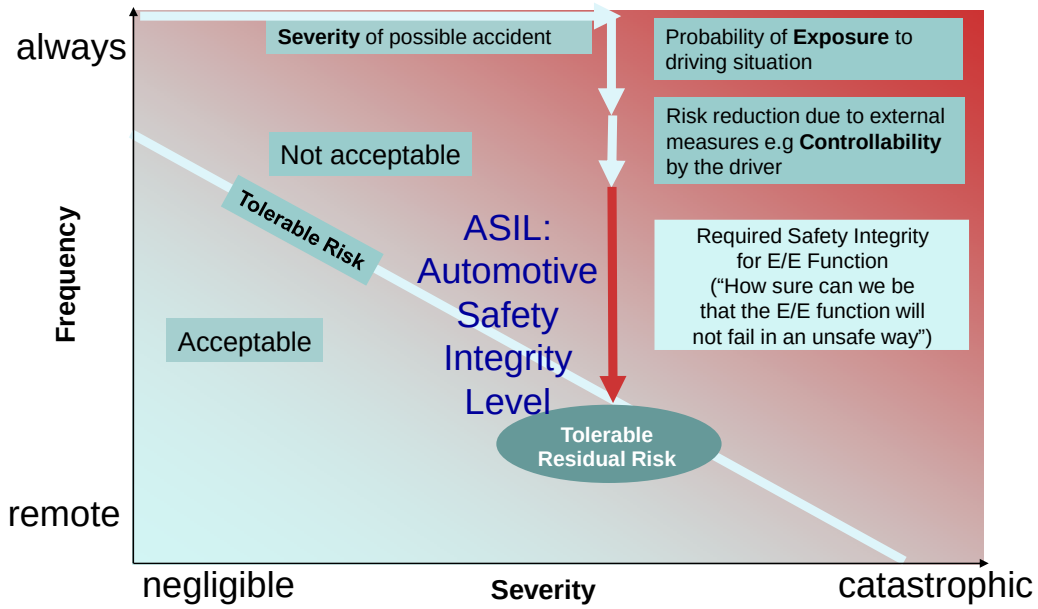

Figure 9: ASIL Risk Decomposition.

Figure 9 depicts the current view on ASIL Risk decomposition in an automotive scenario condition. Note the mention to risk reduction due to the external measures, an item that when discussing autonomous vehicles is severely reduced or eliminated, as no external driver should be considered. When reviewing the Design Assurance Level concept from aviation, a similar decomposition can be found with some minor differences. Indeed if we remove the ASIL and driver mentions from the figure it would be applicable to avionics with minor modifications.

Figure 10 and Figure 11 provides a good description of the similarity between both domains in this respect.

IEC 61508 Risk Matrix			Severity			
			Negligible	*Marginal*	*Critical*	*Catastrophic*
			Minor injuries at worst	Major injuries to one or more persons	Loss of a single life	Multiple loss of life
Frequency	*Frequent*	> 10^{-3}	Undesirable	Unacceptable	Unacceptable	Unacceptable
	Probable	10^{-3} to 10^{-4}	Tolerable	Undesirable	Unacceptable	Unacceptable
	Occasional	10^{-4} to 10^{-5}	Tolerable	Tolerable	Undesirable	Unacceptable
	Remote	10^{-5} to 10^{-6}	Acceptable	Tolerable	Tolerable	Undesirable
	Improbable	10^{-6} to 10^{-7}	Acceptable	Acceptable	Tolerable	Tolerable
	Incredible	≤ 10^{-7}	Acceptable	Acceptable	Acceptable	Acceptable

Figure 10: IEC 61508 Risk Matrix.

A Risk is acceptable when its frequency per flight hour is lower than the one defined for the DAL corresponding to its severity			Severity			
			Minor	*Major*	*Hazardous*	*Catastrophic*
			Failure is noticeable, but has a lesser impact than a Major failure (for example, causing passenger inconvenience or a routine flight plan change)	Failure is significant, but has a lesser impact than a Hazardous failure (for example, leads to passenger discomfort rather than injuries) or significantly increases crew workload	Failure has a large negative impact on safety or performance, or reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers	Failure may cause a crash. Error or loss of critical function required to safely fly and land aircraft
Frequency per flight hour	*Probable*	$10^{-5} < F \leq 10^{-1}$	**DAL D**	Unacceptable	Unacceptable	Unacceptable
	Occasional	$10^{-7} < F \leq 10^{-5}$	Acceptable	**DAL C**	Unacceptable	Unacceptable
	Remote	$10^{-9} < F \leq 10^{-7}$	Negligible	Acceptable	**DAL B**	Unacceptable
	improbable	$F \leq 10^{-9}$	Negligible	Negligible	Acceptable	**DAL A**

Figure 11: ARP4754 Risk Matrix.

As can be noted between the above two figures, the similarities are notorious between the automotive (IEC 61508 applied to various domains apart from the avionics, including the automotive) and the avionics. The probability values considered in one case and the other are different in magnitude (although minor, there is a difference between them) and in the avionics there is no fully acceptable risk for a catastrophic condition, regardless of how improbable the situation is, but apart from that, both domains appear quite equal.

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 analyzed 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 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.

Certifying an electronics component or a real time operating system in avionics has an extremely high cost, in an order of magnitude which would probably make any automotive model, unmarketable if all components inside required certification at that level. This is represented by the costs of each unit, where the average commercial aircraft costs an excess of multiple average automobiles. Indeed from market analysis, the cost of an Airbus® is on average between 100 and 200 Million USD, with the A380 at 390 Million and the A318 at 68 Million in the extremes of the price scale. On average an automobile will cost around 30 thousand USD which means the cost of one A330, currently priced at 210 Million would allow for the purchase of 7000 new automobiles. This can be traced not only to the difference in sizes in terms of the vehicles, after all a commercial aircraft is quite larger than an automobile, but also on the cost linked to the certification/qualification process in both domains.

Redundancy is present in both the automotive and the avionics domains. However, the amount of redundancy in terms of number of duplicated components and the actions to take when an issue is detected appear dissimilar in the two domains. In automotive the number of redundant components is small and only applicable to the highest criticality elements. In terms of avionics, more components are redundant, indeed it is expected that the entire avionics bay to have redundancy with some of the more critical elements to even have triple redundancy. This again, increases the cost of the overall vehicle.

One key difference between the automotive and the avionics domain is the controlling entity responsible in terms of operational safety. The only and ultimate responsible for ensuring safety when operating an automobile is the driver, whilst in the avionics domain, this responsibility is “shared” between the pilot and the ground air traffic manager, with this last one expected to have the final say in terms of deviation from any flight plans. Granted that emergency deviations is in the purview of the pilot but these deviations need to be explained and if time permits it, approved by the ground control. There is no similar “force” in automotive today which would, if implemented, increase road safety. If a driver breaks the speed limit or commits illegal manoeuvres this can only be determined in certain conditions, such as proximity to speed radars or police detection. Addition of road side infrastructures as well as internal communication functionalities would increase the possibility of detection and thus, increase safety in the transit roads. [EC law concerning personal data]

The capabilities provided by the 802.15 standard are somewhat applicable to the avionics domain and indeed ADS-B shares some of the characteristics of 802.15 in terms of communications needs. However, as mentioned, the necessity of certifying the equipments used in avionics precludes currently the use of 802.15 equipments in that domain.

One of the key issues with the avionics architecture, the IMA architecture is the lack of standardization in terms of hardware interfaces. That architecture is dependent on each equipment supplier’s notion of interface and on that supplier’s proprietary solution in terms of operation. Currently this architecture is under study in Europe, the so called IMA second generation, where it is intended to provide interchangeable components, regardless of the supplier. An analysis on AUTOSAR’s modularity and configurability features could provide additional paths of improvement on similar features in the avionics domain. However as mentioned, certification is still an issue in terms of acceptance of these features in such an undertaking. Similarly, the AUTOSAR standardized interfaces facet could be improved with the

incorporation of some of the capabilities of the ARINC 653 APEX interface and scheduling definitions.

An analysis of the scheduling schemes used in avionics and in automotive provides some differences which merit discussion. The avionics scheduling is primarily aimed at ARINC 653 scheduling schemes where you have fixed, non-priority partition schedule followed by preemptive priority based schedule for the processes inside each partition. Automotive schedule options are, according to AUTOSAR, OSEK and actual industrial application, based on two separate types of schedule:

- Rate-Monotonic.
- Priority assignment criticality based.

Both approaches have advantages and disadvantages. The Rate-Monotonic is the most used as it is also considered the most efficient in an error free environment. It is when errors occur that this type of schedule may fail and produce undesirable and unsafe behaviours. This may lead to priority inversion problem (vide the MARS PATHFINDER priority inversion problem) and thus lead to potential collision probabilities in case of failure. The priority assignment priority based is similar in a fashion with the ARINC 653 process scheduler approach and in similar fashion suffers from the same disadvantage: it is not very efficient resource-wise. It prevents, however, the priority inversion problem which plagues the RMS and has started being used in high criticality systems in the automotive domain.

One analysis of these issues was already performed [2] in another European project, RECOMP project (ARTEMIS JU) and the conclusion taken from that study is that the most appropriate solution appears to be a hybrid scheduling approach (AUTOSAR Timing Protection). Application of this approach to avionics is not possible outside the partition, due to the strict time partitioning rules currently enforced in avionics but it may be possible to improve performance inside the partition scheduling schemes. In addition one of the issues under study recently is the usage of multicore in avionics, a situation which, although deemed the future of the architectures still raises considerable challenges due to the aforementioned rules. Leveraging the multicore studies in Europe with “new” scheduling schemes, one of the contention problems identified: single partition, multiple processes in several cores vs several partitions in multicores, processes in single-core vs several partitions in several cores and multiple cores also in several cores will require careful scheduling rules.

2.5 Other Domains

The two domains where the KARYON can be more easily adapted are the Railways and the maritime transport ones. Both involve mobility of vehicles; both can operate in an open environment, with the maritime more open than the railways. Although the railways are forced to operate on the rail tracks, the possibility of a disruption in the rails, both in terms of obstacles and in terms of damage to the tracks leads to the necessity of developing means of detection for those issues in order to ensure the safety of the vehicles.

In maritime transport, the situation is similar to the avionics, with the increased need of taking into account the water drag effect. A large ship does not stop fast nor does it stop in a short distance if at medium to high, relatively speaking, speed. This means that detection of obstacles and coordination of ships is essential for a safe operation, particularly in large commercial harbours.

Road side infrastructures or air traffic management communication and sensor capabilities, when applied to a commercial harbour or a large railway depot can lead to an increase of the safety of the operations as well as to a potential increase on the efficiency of said operations.

The standards considered in these two domains are based on ERA's and on the IMO's safety standards in use today. ERA (European Railway Agency) and IMO (International Maritime Organization) provide the basic standards needed to ensure the safety parameters when operating vehicles in the open world.

Concerning the maritime safety aspects, three main guides can be considered:

- International Convention for the Safety of Life at Sea, 1974 (SOLAS)
- Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREG)
- International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978 (STCW)

From these three standards the main one under consideration would be COLREG, as the other are more focused on crewmembers, both in terms of safety and human controlled operation than on actual ship coordination aspects. It does not mean that they do not cover some of the aspects that the KARYON concept strives to prove, but these concepts are in more evidence in COLREG. This standard specifies guidelines for the steering of naval vessels, their crossing and overtaking, as well as guidelines for restricted detectability and the means through which to overcome it, both visually and audibly.

These rules are similar in scope and form to the automotive driving rules, with the added concern of the water drag effect as previously mentioned.

3. Roadmap for KARYON

3.1 Objective

The purpose of this section is to provide a roadmap for standardization of the new concepts which form the basis of the KARYON hybrid safety architecture. In that aspect we will take into account the results coming from the architecture analysis performed in other WP as well as the requirements needs expressed in Deliverable D1.1 of the project.

As mentioned in the requirements document a full use of the standards analyzed in this document is not possible in KARYON, due to effort and time limitations. However it is possible to extrapolate a convergence path between the avionics and the automotive standards and to attempt to extract the maximum of benefits from both domains while at the same time to minimize the discrepancies.

One key divergence between the automotive and avionics is the certification/qualification processes. It is not considered possible to eliminate the certification process in aviation, but with the proper usage of the hybrid architecture concept it may be possible to ease the certification needs and costs and therefore to provide to the avionics domain a more cost effective means of developing avionics components. Similarly it may be possible to leverage this cost effective means to attempt to increase the qualification degree in automotive in order to approach the certification level of avionics. This would allow an increase in the safety of automobiles today and it would also provide an excellent stepping stone in the process of reaching fully autonomous vehicles in the roads of Europe.

The application of ARINC 653 rules to the implementation and operation of automotive run-time routines would permit a gain in safety and determinism which would then allow for an easier qualification/certification of those routines. ARINC 653 is already being considered in other domains than the avionics, namely space applications such as on-board satellite applications and the effort to use it in automotive would not be excessive. Indeed without proper real time deterministic command and control mechanisms it is not considered possible to provide safe autonomous vehicles in real world conditions.

Communication mechanisms in the automotive and the avionics share similar necessities and constraints. The greater focus on safety that the avionics domain requires, forces in some ways the path of convergence from the automotive to the avionics, with some caveats in it. The rules specified in part 2 of IEEE 802.15 already define the necessary steps to be taken to permit the coexistence of other wireless networks in proximity to the one under study. Applying these rules to the avionics domain, permits an increased sharing of the airwaves with some limitations, due to the licensed versus unlicensed frequency bands.

3.2 Requirements

The identified requirements in D1.1 which are applicable to the KARYON concept based on the standard analysis are:

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.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. 4.2.170

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

Following the analysis of the standards in this document, the above referred requirements are deemed sufficient to cover the KARYON concept.

4. Conclusions

From the analysis of the avionics and automotive domains, some similarities were identified as well as some divergences. The similarities provide a good basis for the harmonization of the safety architecture to be devised in KARYON, while the divergences means that true adaptation of automotive standards to avionics and vice versa requires quite a large amount of effort, if indeed it is possible.

One of the key issues, the certification versus qualification is deemed a quite complicated item, as the costs of certification are usually in an order of magnitude larger than the costs of qualification. Certifying a real time operating system or electronics component for avionics at the highest criticality can be on the order of the millions of Euros, a value which in the automotive is believed unbearable to the manufacturers. One of the advantages of the KARYON concept is the ability to eventually allow for a reduction of the criticality of some of the systems under study and therefore to a reduction of the cost of certification in terms of the avionics domain. This would permit to lower the cost of the avionics programs in Europe and thus the time to market of such vehicles.

References

[1] MULCORS - The Use of MULticore proCessORs in airborne Systems [EASA].

[2] Christoph Ficek, Nico Feiertag, Dr. Kai Richter, “Applying the AUTOSAR timing protection to build safe and efficient ISO 26262 mixed-criticality systems”, ERTS 2012

[3] Antoine Rauzy, “Safety Integrity Levels”, Séminaire de Sûreté de Fonctionnement de l’X, 2012-11-23.

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

[5] ETSI EN 302 665, Intelligent Transport Systems (ITS): Communications Architecture

[6] ETSI TR 102 638 Intelligent Transport Systems (ITS): Vehicular Communications; Basic Set of Applications Definitions

[7] ETSI TS 102 637-2 Intelligent Transport Systems (ITS): Vehicular Communications; Basic Set of Applications Part 2: Specification of Cooperative Awareness Basic Service

[8] ETSI TS 102 868-1 Intelligent Transport Systems (ITS): Testing; Conformance test specification for Co-operative Awareness Messages (CAM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma

[9] ETSI TR 102 863 Intelligent Transport Systems (ITS): Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization

[10] ETSI TR 102 893 Intelligent Transport Systems (ITS): Security; Threat, Vulnerability and Risk Analysis (TVRA)

[11] ETSI TR 102 862 V1.1.1 (2011-12) Intelligent Transport Systems (ITS): Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part

[12] FAR 25 Regulations – sec. 25.1309

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

[14] RTCA DO-254, Design Assurance Guidance For Airborne Electronic Hardware

[15] DO-212, Minimum Operational Performance Standards for Airborne Automatic Dependent Surveillance (ADS) Equipment

[16] ARP4754A, Guidelines For Development Of Civil Aircraft and Systems

[17] ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

[18] ARINC 653, Avionics Application Standard Software Interface.

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

