SAFURE

D1.2
Requirements Specification

Project number:	644080
Project acronym:	**SAFURE**
Project title:	SAFety and security by design for interconnected mixed-critical cyber-physical systems
Project Start Date:	1st February, 2015
Duration:	36 months
Programme:	H2020-ICT-2014-1
Deliverable Type:	Report
Reference Number:	ICT-644080-D1.2
Work Package:	WP 1
Due Date:	21st November, 2016
Actual Submission Date:	21st November, 2016
Responsible Organisation:	ESCR
Editor:	Cheng Lu
Dissemination Level:	PU
Revision:	1.0
Abstract:	This SAFURE requirements specification provides a list of functional and non-functional requirements corresponding to different use cases defined in D1.1
Keywords:	requirements, automotive, telecommunication, multi-core, functional, non-functional

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080.

This work is supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

Editor

Cheng Lu(ESCR)

Contributors

Christina Petschnigg, Martin Deutschmann (TEC)
Stefania Botta, Luigi Santamato (MAG)
Carolina Reyes (TTT)
Mikalai Krasikau (SYSG)
Jonas Diemer (SYM)
Sylvain Girbal (TRT)
Daniel Thiele, Robin Hofmann (TUBS)
Jaume Abella (BSC)
Marco Di Natale (SSSA)
Philipp Miedl, Rehan Ahmed (ETHZ)
Dominique Ragot (TCS)

Executive Summary

This document provides the requirements for the SAFURE project corresponding to different use cases which are defined in Task T1.1. The common requirements are listed in Chapter 2. The requirements of the telecom scenario are described in Chapter 3. The requirements of the automotive multi-core scenario are described in Chapter 4. Finally, the requirements of the automotive network scenario are described in Chapter 5.
All the requirements are categorized into functional and non-functional requirements. The non-functional requirements include subclasses such as security, safety, time, temperature, mixed-critical, hardware platform, etc. In addition, the requirements, which have already been integrated into SAFURE project at the time of this delivery, are listed separately at the beginning of each related chapter. The integrated requirements means that these requirements are already been fulfilled at the time of this delivery. As a result of Task T1.2, the D1.2 requirements specification will be used as reference in the other SAFURE work packages to implement and analyze platforms and demonstrators.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Objectives of D1.2

The main objective of deliverable D1.2 is to derive a list of requirements from the use cases of deliverable D1.1. All the requirements will be categorized and grouped in order to guide development in the other SAFURE work packages.

1.2 Use of the D1.2 Outcomes

The requirements specified in deliverable D1.2 are an important basis for other deliveries and work packages of the SAFURE project. These requirements have been specified by the project partners based on the use cases presented in D1.1. The work packages WP2, WP3, WP4, and WP5 aim at refining these requirements as well as implementing and analysing platforms that realize the defined use cases fulfilling the stated requirements. Finally, the implementations are going to be evaluated against the use case definitions in work package WP6. The dependencies between the different work packages are illustrated in Figure 1.1.

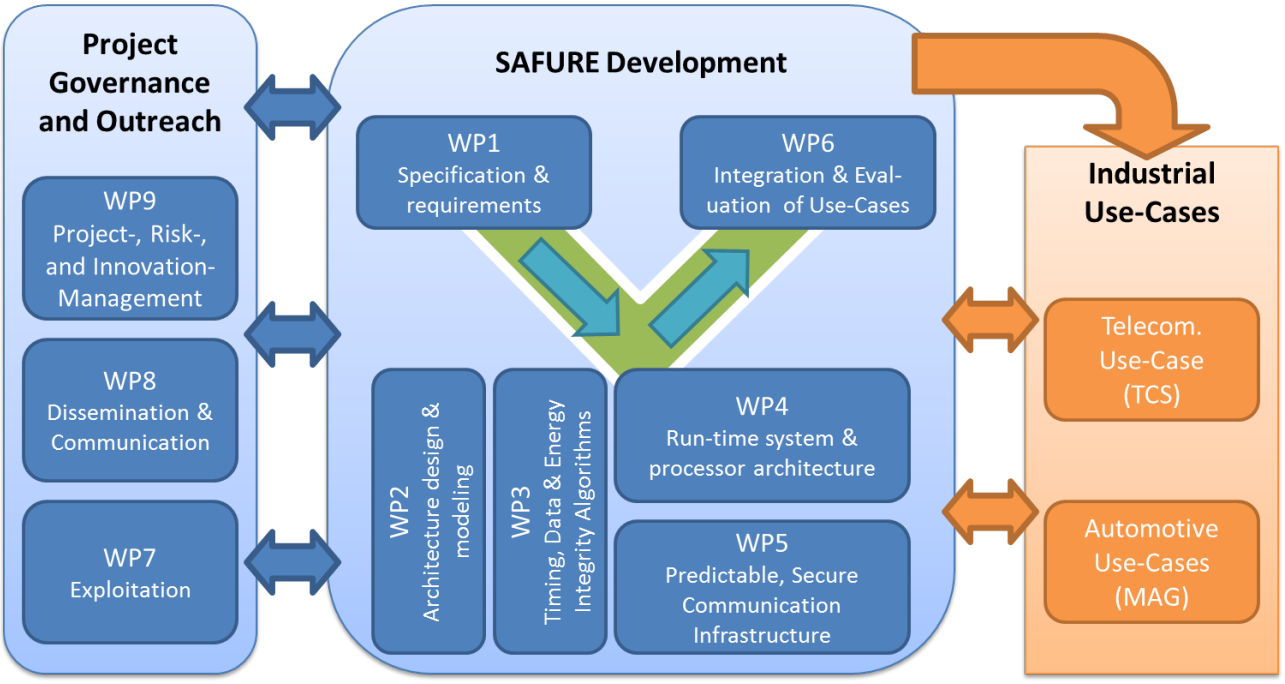

Figure 1.1: Workplan for SAFURE Project

1.3 Methodology of definition of requirements

The document aims to provide a complete set of requirements for the SAFURE platform. To provide a solid basis for extracting the requirements, several relevant use cases have been identified and specified in D1.1. Each partner has been requested to identify functional and non-functional requirements depending on the use cases. To this end, each partner has been provided an input sheet to provide these requirements. Following the requirement collection phase the consolidation phase started. The goal of the consolidation phase is to eliminate repeated requirements, assure similar wording, and identify possible conflicts between the requirements. The outcome of the consolidation phase is one list of functional and non functional requirements which can be found in this document. The link between the consolidated requirements and the initial requirements of the partners has been kept to enable backtracking in case of unclear issues. Furthermore, assessment is also introduced for each requirement and will be filled in by each partner in order to track the status of the requirements during the project. To distinguish those requirements, which have been already fulfilled or integrated into SAFURE project at the time of this delivery, a list of integrated requirements will be stated separately at the beginning of each corresponding chapter.

There are two different types of tables for listing the functional and non-functional requirements. Both types of tables include column "ID", which is used for tracking the each requirement, column "Description", which states the details of the requirement, and column "Comments", which gives short remarks for the requirement. The non-functional requirements table has an additional column "Type" for distinguishing different types of the non-functional requirements.

Chapter 2

Common Requirements for All Scenarios

This chapter presents the functional and non-functional requirements in a general view which should be applied into all three use cases. The non-functional requirements are further divided into real-time operating system, timing, temperature, security, safety, mixed criticality and hardware platform requirements. The common requirements which have been already integrated into SAFURE at the time of this delivery, have been extracted and listed in Section 2.1.

2.1 Integrated Requirements

The table 2.1 lists the common requirements which have been already integrated into SAFURE project at the time of this delivery.

Type	ID	Description of Requirements	Comments
Real-Time Operating System	CR-NF-001	The hypervisor shall provide real-time guarantees when scheduling virtual machines/partitions	
	CR-NF-003	The real-time operating system should provide ways to access the hardware monitoring features of the hardware platform. Virtualization needs to have a minimal impact on the availability and accuracy of the monitoring features.	For monitoring features required by WP3 and WP4
Time analyses	CR-NF-032	An upper bound must be computed on the delay of communication over Ethernet for safety-critical traffic.	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-033	An upper bound must be computed on the delay of communication over Ethernet for safety-critical traffic also in the presence of unknown/unexpected traffic.	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-034	An upper bound must be computed on the hardware utilization of communication over Ethernet (bandwidth, buffer) for safety-critical traffic.	Applies to all use cases for which timing analysis shall be performed.

Temperature	CR-NF-013	The hypervisor should provide support to treat energy/temperature information on scheduling level or propagate it to the dedicated user applications.	In hardware-virtualization mode, Peripheral Management Access Unit (PMAU) and scheduling /synchronization API can be used by application
Security	CR-NF-014	The hypervisor shall provide means to confine HW-based covert/side channels.	In hardware-virtualization mode, PMAU and scheduling /synchronization API can be used by application as appropriate setup of time and partition isolation
	CR-NF-017	The hpervisor should provide support for Public Key Infrastructure (PKI).	e.g. file provider API
	CR-NF-020	The cryptographic services shall provide a common interface to Hardware Security Models and Software libraries.	Interfaces are provided so that other software applications do not need to know the implementation of all cryptographic services
Mixed-Critical	CR-NF-023	The hypervisor shall provide temporal and spacial separation of applications.	Generic from the DoA. Integrated for Safety.
	CR-NF-025	Multiple safety/security criticality levels have to be considered for software/hardware components, not only a 'naive' separation between the critical and the non-critical ones (best-effort). These different levels of criticality have to be taken into account at tool, especially at the analysis level of the tool composing the tool-flow	
Hardware platform	CR-NF-029	The proposed hardware platforms to be evaluated in WP4 for final selection should encompass some shared hardware resources shared by several cores (>4) such as shared memory (such as distributed memories or caches, preferably distributed SRAM memories), but also the SoC interconnect, and I/O devices. The real-time analysis should not only take the shared memory into account, but also the other resources.	WP4 requirements. Covered by the chosen hardware platform.
	CR-NF-030	According to the system predictability criteria defined by the PREDATOR project, there is a strong need for large local memories on the multi-core platform.The size of the local memories should be enough for the storage (instructions & data) of any single application task.	To control interferences. Covered by the chosen hardware platform.

	CR-NF-031	The selected hardware platform should encompass multi-core technology with at least 4/8 cores such as the 4-core iMx6q, the 8-core P4080 or the 12-core T4240. To make sure that all the techniques proposed in the SAFURE project are scalable, dual-core architectures should be avoided as they usually encompass specific non-scalable hardware features.	From the DoA, targeting multi-cores. Covered by the chosen hardware platform.

Table 2.1: Integrated Common Non-Functional Requirements for All Scenarios

2.2 Functional Requirements

ID	Description of Requirements	Comments
CR-F-001	Mixed-critical safety requirements and time-critical requirements need to be coupled in at least one of the use-case supporting PikeOS, including the possibility to run concurrently different tasks with different safety levels, or the ability to support a degraded mode for lowest critical tasks.	Requirement for the research performed in WP4. Else WP4 will use a dedicated prototype. Integrated in the WP4 prototype.
CR-F-002	The use-cases should quantify their usage and requirements in term of accesses to the different shared hardware resources of the target platforms for the adaptive solution to guarantee the associated requirements based on observed behavior.	Requirements for QoS algorithm developed in WP3.

Table 2.2: Common Functional Requirements for All Scenarios

2.3 Non-Functional Requirements

Type	ID	Description of Requirements	Comments
Real-Time Operating System	CR-NF-002	All the use cases should use tools and SW that are an expression of an acknowledged standard or have a reliable open source implementation	
Time analyses	CR-NF-005	System description (topology, etc.) must be available in an accessible format.	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-006	System configuration (communication, tasks, etc.) and timing properties (execution times, frame sizes, etc.) must be available in an accessible format.	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-007	System constraints (deadlines, max. load, etc.) should be available in an accessible format	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-008	Timing behavior must be known/specified for all arbitration points (CPU scheduler, network arbitration, shared resource access, etc.)	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-009	For unknown time consumers (attackers), constraints should be specified (e.g. what resources are affected).	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-010	Standard arbitration protocols should be used for OS and networks (e.g. AUTOSAR, OSEK, Ethernet).	There will likely be no support from SYM for non-standard / custom protocols for timing analysis.

	CR-NF-011	Timing properties should be derived via tracing, static analysis or budgeting.	Applies to all use cases for which timing analysis shall be performed.
	CR-NF-012	WCET analysis techniques and dedicated isolation techniques should provide Time Composability in target multi-core systems by providing features allowing us to compute or bound the co-running interference overhead.	
Security	CR-NF-015	The hypervisor shall support secure boot of the whole system and each partition separately.	
	CR-NF-016	The hypervisor shall provide secure update of a partition.	
	CR-NF-018	The SAFURE platform must provide services for cryptographic mechanisms and handle cryptographic objects (i.e. keys, certificates). The services must include the following features: a) Managing cryptographic keys. (Generating, deleting and storing keys) b) Calculation of cryptographic functions: - Signature generation and verification - Message Authentication Codes (MACs) - Encryption and decryption c) Management of cryptographic certificates. (Storing and updating certificates)	This requirement needs to be fulfilled if a system wants to provide security like confidentiality, integrity, and authenticity.

	CR-NF-019	The cryptographic services must provide a configuration mechanism to define the access methods and rights to the cryptographic objects. a) The configuration shall only be done by authorized entities. b) The access rights shall be enforced by the security architecture. c) Access rights must be definable for - Roles and Users - Services - Domains d) Access rights shall define: - Overall access - Access to individual functions using the cryptographic objects.(i.e. generating or deleting keys) e) Usage rights of cryptographic objects should be defined: - Keys for encrypting, decrypting, signing, verifying. - If keys can be deleted, exported, derived or not.	This requirement needs be fulfilled if a system wants to provide access control.
Safety	CR-NF-021	A software component should not be allowed to alter, contaminate or delay another software component's code, I/O, scheduling, or data storage areas in uncontrollable ways, especially from the less critical components to the most critical ones. Time isolation and Spatial isolation have to be ensured. New isolation mechanisms can be introduced to ensure software independence in multi-core systems, enabling the safe execution of software components with different criticality levels.	Generic from safety definition
	CR-NF-022	Failure on hardware unique to a software component should not cause adverse effects on any other software component.	Generic from safety definition
Mixed-Critical	CR-NF-024	Mixed-criticality must be supported in hardware.	Mixed-criticality should be sufficiently isolated.

	CR-NF-026	Incremental changes should be supported in the design and verification. The tools should exploit the isolation to keep the effects of incremental changes as small as possible for the higher levels of criticality. This feature is required for incremental certification.	Generic from mixed-critical definition
Hardware platform	CR-NF-027	The hypervisor shall support the platform selected in the telecom use-case.	
	CR-NF-028	The selected hardware platform has to provide monitoring features such as Performance Monitoring Counter (PMC) or hardware counters, allowing to monitor the timing behavior, the runtime workload on the different hardware resources, and power consumption or energy related features.	For monitoring features required by WP3 and WP4

Table 2.3: Common Non-Functional Requirements for All Scenarios

Chapter 3

Functional and Non-functional Requirements for Scenario 1: Telecom Scenario

This chapter presents the functional and non-functional requirements for the telecom use case. The non-functional requirements are further divided into real-time operating system, timing, temperature, security, mixed criticality and hardware platform requirements. The requirements which have been already integrated into SAFURE at the time of this delivery, have been extracted and listed in Section 3.1.

3.1 Integrated Requirements for Telecom Scenario

The table 3.1 lists the functional requirements which have been already integrated into SAFURE project at the time of this delivery.

ID	Description of Requirements	Comments
S1-F-001	Linux/GNU based OS for the COTS.	Needed for integration of thermal protection mechanisms
S1-F-010	The hypervisor shall be able to execute Linux and other runtime environments	

Table 3.1: Integrated Functional Requirements for Telecom Scenario

The table 3.2 lists the non-functional requirements which have been already integrated into SAFURE project at the time of this delivery.

Type	ID	Description of Requirements	Comments
Time analyses	S1-NF-003	One of the HW platforms must include a COTS multi-core with at least 4 cores (e.g. Freescale iMX6q, Freescale P4080)	This requirement should be compatible with TRT ones on this case study The HW platform chosen provides this feature, so this requirement is covered
	S1-NF-004	The COTS multi-core in the previous requirement must include some on-chip shared resources across cores: at least (1) a shared interconnection network between the cores and a shared cache or shared memory, and (2) a shared memory controller. It is also valuable if such multi-core includes a cache memory shared across cores.	This requirement should be compatible with TRT ones on this case study The HW platform chosen provides this feature, so this requirement is covered
Security	S1-NF-010	The device shall protect communications with the IMDs (Implantable Medical Devices) and with the medical cloud server in accordance with the SFPP security requirements.	Communication with IMD devices : to ensure a compatibility with existing devices, security mechanism implemented in the Bluetooth protocol are used.
Hardware platform	S1-NF-019	The hardware platform shall offer multiple cores.	All platforms selected by SAFURE are multicore.
	S1-NF-021	The hardware platform shall offer an USB interface.	All platforms selected by SAFURE have an USB interface
	S1-NF-030	Multi Core Processor (MPSoC)	Fundamental use-case requirement. Covered by the chosen hardware platform
	S1-NF-031	One Temperature Sensor per Core	Required for integrating thermal protection mechanisms. Covered by the chosen hardware platform
	S1-NF-032	The resolution of the Temperature Sensors needs to be equal/smaller than 1 K	Required for integrating thermal protection mechanisms. Covered by the chosen hardware platform
	S1-NF-033	The system has to have power or thermal management build in.	Required for providing thermal protection Covered by the chosen hardware platform

Table 3.2: Integrated Non-Functional Requirements for Telecom Scenario

3.2 Functional Requirements for Telecom Scenario

ID	Description of Requirements	Comments
S1-F-002	The functional architecture of the telecommunications use case(s) should be defined (at least in part) by means of a formal (possibly standard and commercial) modeling language.	
S1-F-003	The device shall provide applications to control and monitor the IMD. These applications shall be configurable by authenticated user only.	An application will be developed to monitor/control a medical device or a simulated device. It will depend on the availability of a device using open communication protocols and providing an API/SDK to access the sensor streams.
S1-F-004	The device shall be able to forward data recorded or processed in the critical environment to a cloud server. This requirement implies the existence of inter-partition communication means.	An application will be developed to transmit the data from the critical partition to a cloud server.
S1-F-005	The device shall allow the update of medical applications over the air. For example the update could be stored on a cloud server.	An android market(not the Google Play market) will be used to store the application. An OSS such as Fdroid could be used to create our own repository containing the application.
S1-F-006	The device shall provide the Android operating system with all basic applications (browser, mail client, multimedia player, phone client etc).	It will depend on the features offered by the hypervisor and specifically the screen sharing between two Android partitions. In this case, the non-critical partition will contain basic applications.
S1-F-007	The device shall provide a mechanism to separate the domain specific applications (e.g. IMD applications) from the general purpose applications or prohibit the installation of those general purpose applications by users.	The separation between the IMD applications is made by design. In fact, PikeOS is used to separate the critical applications (IMD apps) and general purpose applications.
S1-F-008	A mechanism shall enforce authenticity and integrity of the software stack in accordance with the SFPP security requirements.	
S1-F-009	Remote control of the platform shall be available to legitimate users in accordance with the SFPP security requirements.	Control orders of IMD devices are transmitted from the medical server over the specific VPN used to transmit medical data. After that, these data are sent to the IMD having actuators.

Table 3.3: Functional Requirements for Telecom Scenario

3.3 Non-functional Requirements for Telecom Scenario

Type	ID	Description of Requirements	Comments
Real-Time Operating System	S1-NF-001	The critical environment containing medical applications shall implement a real-time operating system enforcing the security policy regarding real-time communication needs.	An Android partition is used as a critical environment. Security policy is ensured by design by using an hypervisor(separation kernel) and by using Android permissions.
	S1-NF-002	The operating systems running on the PikeOS hypervisor should be kept as minimalistic as possible, allowing direct access of the hardware close to bare bone style. Complex unpredictable scheduler politics such as the one included in Linux systems should be avoided for safety critical systems, especially those with time-critical requirements.	Requirements for controlling interferences on time critical systems.
Time analyses	S1-NF-005	Performance monitoring counters (PMCs) must be abundant and allow tracking activities occurring in the on-chip shared resources such as the number (and preferably also the type) of accesses to the on-chip interconnection network and the memory controller indicated in the previous requirement.	This requirement should be compatible with TRT ones on this case study.
Temperature	S1-NF-006	The device temperature shall remain under 45°. In particular, this shall be the case when the Android environment is being intensively used.	
	S1-NF-007	Different application modes of the devices should be required for low, medium and high computational effort	To enable sophisticated thermal protection mechanisms
	S1-NF-008	Different applications should have different thermal characteristics for each core	To enable sophisticated thermal protection mechanisms
	S1-NF-009	The applications have to be periodic.	Required for providing thermal protection
Security	S1-NF-011	The device shall protect in confidentiality and authenticity critical data in accordance with the SFPP security requirements. In particular application data shall be protected in confidentiality, integrity, authenticity and availability.	These properties are ensured by using security mechanisms provided by Android(Cipher class) or CycurLIB with PikeOS.

	S1-NF-012	Access to the device, and especially access to the critical environment shall be granted only after a correct authentication of the user in accordance with the SFPP security requirements.	Android authentication mechanism(local or authenticating server) will be used
	S1-NF-013	The device shall implement a separation kernel with at least one partition for non-critical applications and one partition for critical applications in accordance with the SFPP security requirements.	An hypervisor compatible with the hardware platform is to separate the 2 environments: Ensured by Design(Hypervisor and architecture supporting the device)
	S1-NF-014	The telecommunications use case should provide one example of communication or interaction with security concerns/issues that can be expressed in a quantitative and formal way.	
	S1-NF-036	The device shall protect the anonymity and the confidentiality of the medical data transmitted to the medical staff	A specific VPN will be used to transmit only the medical data between the terminal device to a medical server.
	S1-NF-037	The device shall protect the privacy, the anonymity and the confidentiality of the data transmitted to the support product staff(manufacturer, seller of the product, etc.)	A specific VPN will be used to transmit only the data concerning IMD devices. The VPN will be used between the terminal device and a server used by the support product staff. These data will be used by the support team to ensure the correct functioning of the IMD devices.
	S1-NF-038	Anonymity: A subset of the medical data shall be provided to authorized users, without any information that may reveal the identity of the IMD holder	
	S1-NF-039	Privacy: The device shall be able to ensure that a subset of the data is accessible only to the terminal holder and to other users to whom the terminal holder has granted access	
Mixed-Critical	S1-NF-015	Critical applications (e.g. medical applications) and non-Critical applications (mail/social network/game/...) should run at the same time on the same system.	Fundamental use case requirement

Hardware platform	S1-NF-016	The hardware platform shall be able to run Android above PikeOS. Preferably the latest version of Android : Android 5.0 a.k.a Lollipop	This will be ensured by using the work made by SYSGO. The Android OS will be used as a partition in PikeOS. The Android personality will be provided by a partner
	S1-NF-017	The hardware platform shall be able to run the separation kernel PikeOS.	The platform selected by TCS for the telecommunication use case will be supported by PikeOS. SYSGO will provide an installation with a PS Provided by a partner
	S1-NF-018	The hardware platform shall be able to run Linux OS above PikeOS.	SYSGO will provide a Linux running PikeOS for the telecommunication platform
	S1-NF-020	The hardware platform shall offer a Graphics Processor Unit (GPU) addressed by at least one partition.	Either PikeOS provide a direct access to the GPU of the platform or provides a specific driver to have an access from multiple partitions to the GPU(indirectly).
	S1-NF-022	The hardware platform may offer an Secure Digital High Capacity (SDHC) interface.	
	S1-NF-023	The hardware shall offer a 3G/4G interface.	All smart phones and some tablets have a 3G/4G interface
	S1-NF-024	The hardware shall offer a Wi-Fi interface in order to communicate with the cloud server.	The chosen platform provides a WIFI interface
	S1-NF-025	Documentation about the hardware platform shall be available and detailed enough to design a Binary Space Partitioning (BSP).	
	S1-NF-026	The hardware platform shall allow to configure the boot loader.	Some manufacturers such as SONY allow us to configure the boot loader
	S1-NF-027	The hardware platform shall be preferably a smart phone, a tablet, or a development tablet (in this order).	
	S1-NF-028	The underlying hardware shall provide an hardware virtualization mechanisms set.	
	S1-NF-029	The underlying hardware may provide an NFC interface.	
	S1-NF-034	Minimum one power sensor for the MPSoC.	This requirement would enable the study of power covert channels.

Other	S1-NF-035	The number of applications has to be limited	Required for providing thermal protection

Table 3.4: Non-functional Requirements for Telecom Scenario

Chapter 4

Functional and Non-functional Requirements for Scenario 2: Automotive Multi-Core Use Case

This chapter presents the functional and non-functional requirements for the automotive multi-core use case. The non-functional requirements are further divided into architectural design, safety, security, timing, mixed criticality and hardware platform requirements. The requirements which have been already integrated into SAFURE at the time of this delivery, have been extracted and listed in Section 4.1.

4.1 Integrated Requirements for Automotive Multi-Core Scenario

The table 4.1 lists the functional requirements which have been already integrated into SAFURE project at the time of this delivery.

ID	Description of Requirements	Comments
S2-F-002	A mechanism provided by OS shall enforce authenticity and integrity of the software stack in order to satisfy safety goals.	ERIKA OS provides these mechanisms that are crucial for ISO26262 compliance

Table 4.1: Integrated Functional Requirements for Automotive Multi-Core Scenario

4.2 Functional Requirements for Automotive Multi-Core Scenario

ID	Description of Requirements	Comments
S2-F-001	The functional architecture of the automotive use cases should be defined (at least in part) by means of a formal (possibly standard and commercial) modeling language	
S2-F-003	The Electronic Control Unit (ECU) must be able to manage a four cylinders engine and simulate the control of automatic transmission gearbox.	

Table 4.2: Functional Requirements for Automotive Multi-Core Scenario

4.3 Non-functional Requirements for Automotive Multi-Core Scenario

Type	ID	Description of Requirements	Comments
Architectural Design	S2-NF-001	Modeling all the components should be required to simulate the entire system and allow a predictable time analysis and task/runnable allocation.	Architectural Design Requirement. The simulation is mandatory for ISO26262. The time analysis is a new requirement.
Safety	S2-NF-002	The automotive use case should provide at least one example of communication or interaction with safety concerns/issues that can be expressed in a quantitative and formal way.	
Security	S2-NF-003	Controller Area Network (CAN) bus communication should be protected from external attacks.	
	S2-NF-004	The Data stored on multi-core ECU must be protected against adversaries.	
	S2-NF-005	The automotive use case should provide at least one example of communication or interaction with security concerns/issues that can be expressed in a quantitative and formal way.	
	S2-NF-006	There should be a mechanism to prevent/limit unknown/unexpected task activations (e.g. Interrupt Request (IRQ) limiting)	
	S2-NF-007	A security mechanism for authentication during flashing phase must be provided.	Currently There is not a dedicated UC for this requirement, but it is important for security aspects.

	S2-NF-008	Internal memory access from not authorized devices must be blocked and refused.	
	S2-NF-009	All types of memory access from different cores must be arbitrated to provide freedom of interference.	
Time analyses	S2-NF-010	Security SW Components should not exceed 10% CPU load globally.	
	S2-NF-011	Total system should not exceed 80% CPU load for each core.	this requirement is mandatory to guarantee the correct scheduling to avoid the loss of task activation.
	S2-NF-012	The automotive use case should provide at least one example of timing constraints that need verification.	
	S2-NF-013	Temporal overheads for accessing shared resources must be known (cache, on-chip memory, IO, etc.)	
Mixed-Critical	S2-NF-014	A mechanism for spatial and temporal isolation of the two cores must be guaranteed in order to protect from external attacks and meet safety goals.	
	S2-NF-015	Engine Control Unit must be allocated on core 0, and a simulation of automatic transmission ECU must be allocated on core 1.	
Hardware platform	S2-NF-016	The automatic transmission ECU output commands must be simulated on CAN message and showed on external terminal.	

Table 4.3: Non-functional Requirements for Automotive Multi-Core Scenario

Chapter 5

Functional and Non-functional Requirements for Scenario 3: Automotive Network Use Case

This chapter presents the functional and non-functional requirements for the automotive network use case. The non-functional requirements are further divided into security, timing, mixed criticality and safety requirements. The requirements which have been already integrated into SAFURE at the time of this delivery, have been extracted and listed in Section 5.1.
In WP6, the implementation and evaluation of the automotive network use case is split into two demonstrators: (a) a virtual prototype by TUBS, which will be mainly used to show the research results regarding advanced Ethernet features for safe mixed-critical communication (cf. Task T5.1), and (b) an actual Ethernet demonstrator by TTT showing the security features and anti-counterfeiting measures from Tasks T5.2 and T5.3. This separation is because, in the proposal phase, the involved partners have anticipated that the purpose of some of the advanced research topics in Task T5.1 is mainly to serve as guidelines for Ethernet setups and (potentially) future Ethernet standards. These advanced ideas, most likely cannot be implemented in actual hardware during this project. However, partners TUBS and TTT will try to evaluate as much of the results from Task T5.1 on the actual demonstrator as possible.

5.1 Integrated Requirements for Automotive Network Scenario

The table 5.1 lists the functional requirements which have been already integrated into SAFURE project at the time of this delivery.

ID	Description of Requirements	Comments
S3-F-001	The Software Defined Networking (SDN) mechanism used to configure the (virtual) network must have access to all relevant switch configuration options, which will be identified in WP5.	

Table 5.1: Integrated Functional Requirements for Automotive Network Scenario

The table 5.2 lists the non-functional requirements which have been already integrated into SAFURE project at the time of this delivery.

Type	**ID**	**Description of Requirements**	**Comments**
Time analyses	S3-NF-014	Admission control must complete in bounded time.	
Mixed-Critical	S3-NF-019	The switches and/or end points shall use Time and Space Partitioning to separate traffic streams.	Covered by SOTA - There are switches and End Systems already supporting TSN. Also, TTEthernet technology used within SAFURE (physical network demonstrator) covers the time and space partitioning requirement.

Table 5.2: Integrated Non-functional Requirements for Automotive Network Scenario

5.2 Functional Requirements for Automotive Network Scenario

ID	Description of Requirements	Comments
S3-F-002	The protocol for securely updating software makes use of the PUF feature to secure a hardware fingerprint	PUF topic was discussed with the consortium and it was concluded that the PUF technology is in a too early stage for standardised application in the SAFURE relevant UCs. Further, the selected platform does not provide a PUF

Table 5.3: Functional Requirements for Automotive Network Scenario

5.3 Non-functional Requirements for Automotive Network Scenario

Type	ID	Description of Requirements	Comments
Security	S3-NF-001	The cryptographic services, such as the management of cryptographic keys and certificates, shall be applied to meet the needs of secure communication in Ethernet-based real-time networks.	It is required for secure communication for ethernet-based real-time network.
	S3-NF-002	The network admission controller must have an authorization mechanism which allows only the authorized entities to send requests.	Authenticity is required.
	S3-NF-003	There should be a mechanism to prevent/limit unknown/unexpected traffic (e.g. admission control, shaping)	
	S3-NF-004	The support for trust anchors and secure storage of keys should be provided for secure authentication and communication	Generic from security definition
	S3-NF-005	Information collected within a vehicle should be authentic with respect to origin and time if the vehicle performs actions based on that information.	Generic from security definition
	S3-NF-006	The mechanism is required to ensure integrity for information collected within a vehicle. Especially the pieces of information the vehicle performs actions on.	Generic from security definition
	S3-NF-007	The mechanism is required to ensure availability of ECUs for safety critical applications (robustness to denial of service attacks).	Generic from security definition

	S3-NF-008	Implementation of security algorithms must not violate timing constraints.	Generic from security definition
	S3-NF-009	Communication in Ethernet-based real-time network shall be secured with regards to confidentiality, authenticity and integrity whilst respecting real-time constraints (i.e. predictable latency and low jitter).	This requirement is required if SAFURE aims to support secure real-time system applications.
	S3-NF-010	For the initial demonstrator, a simple level of verification and validation of the security measures should be ensured.	This is an implementation requirement. The verification and validation of the security measures will be provided by the SAFURE platform in the sense of a man-in-the-middle attack, timing analysis and worst case performance analysis.
	S3-NF-011	Network-related security applications should allow for global network flow control, increase network dynamics and permit on-the-fly reconfiguration for all types of traffic classes.	In SAFURE, the inclusion of the newly developed security mechanisms should not have a negative impact on the network behavior.
Time analyses	S3-NF-012	Time and safety critical traffic must state their special requirements (e.g. deadlines, redundancy, weakly hard constraints for typical case analysis) in a way which can serve as in input description to our analysis tools.	
	S3-NF-013	If a traffic stream uses Typical Case Analysis (TCA), its description must provide enough information for a TCA analysis. TCA gives "m-out-of-k" guarantees (e.g. m out of k frames will meet their deadline). Hence, the parameters m and k must be provided along with a deadline.	
	S3-NF-015	Network re-configuration must be performed in a bounded time.	
	S3-NF-016	Each traffic stream must specify whether it requires special fault/failure tolerance, e.g. Automatic Repeat Request (ARQ), TCA, redundant paths.	
	S3-NF-017	If a traffic stream uses ARQ, its description must provide enough information for the selected ARQ scheme, i.e. the ARQ scheme, the retransmission timeout, and the number of expected retransmissions (e.g. errors).	

	S3-NF-018	Redundant paths must be specified at design time.	
Mixed-Critical	S3-NF-020	Each traffic stream must be categorized into critical (e.g. time- and/or safety-critical) or non-critical traffic (e.g. best effort).	
	S3-NF-021	The arbitration scheme in the switches must support mechanisms to distinguish critical (e.g. timing, safety) from non-critical traffic streams to guarantee freedom from interference/sufficient independence for critical traffic streams.	
Safety	S3-NF-022	There must be some kind of admission control in the (virtual) network to ensure robustness to denial of service attacks.	
	S3-NF-023	Switches and/or end stations (in the virtual network) must support the detection of hardware failures, e.g. broken links or switches.	
	S3-NF-024	Switches and/or end stations (in the virtual network) must support monitoring schemes capable of timely detecting attacks and misbehaving traffic. The monitoring scheme must be configurable, e.g. via SDN, and their parameters should be provided, e.g. number of replenishment tokens and replenishment interval for leaky bucket shapers or l-repetitive arrival functions for advanced monitoring.	
	S3-NF-025	Switches and/or end stations (in the virtual network) must support mechanisms to shape/block attacking/misbehaving traffic in a timely and appropriate way. These mechanisms must be configurable, e.g. via SDN.	
Hardware Platform	S3-NF-026	The SDN mechanisms together with the (virtual) network equipment (e.g. switches) must support the reconfiguration of the network.	

	S3-NF-027	SAFURE platform should provide Non-Volatile Memory (NVM) and a Physical Unclonable Function (PUF) feature.	PUF topic was discussed with the consortium and it was concluded that the PUF technology is in a too early stage for standardized application in the SAFURE relevant UCs. Further, the selected platform does not provide a PUF

Table 5.4: Non-functional Requirements for Automotive Network Scenario

Chapter 6

Summary

6.1 Summary of the Requirements

The requirements described are corresponding to three different use cases. In particular:

- The **Telecom Scenario**, cf. Chapter 3, focuses on the requirements to provide secure communication between general-purpose smartphones and medical devices. In addition, timing, temperature, mixed-critical requirements are also considered to make smartphones and medical devices separate the processing of business operation from other processes in order to guarantee a high assurance safety for health applications.
- The **Automotive Multi-Core Scenario**, cf. Chapter 4, focuses on the requirements to provide secure and safety multi-core automotive use case. In particular, their aim is to guarantee memory protection between different cores and prevent malicious attacks through CAN protocol. In addition, timing, mixed-critical, architectural and hardware requirements are also considered to develop Automotive Multi-Core scenario.
- The **Automotive Network Scenario**, cf. Chapter 5, focuses on the requirement specification for safe and secure mixed-critical communication. The requirements cover multiple aspects such as predictable timing, network reconfiguration and isolation, and secure communication regarding confidentiality, authenticity, and integrity.

6.2 Use of the Requirements

All the requirements are derived to ensure safety and security in the design of cyber-physical systems. For several embedded stakeholders, like: assurance market, medical sector, automotive OEMs, telecommunication market, and end users, these requirements should be taken into account and evaluated. The project SAFURE will implemented the demonstrators which realize all the described requirements to provide safety and security for the mixed-critical cyber-physical systems.