SAFEPOWER

D2.6 Final Safety-Concept. Public.

v1.0

Document information

Contract number	687902
Project website	Safepower-project.eu
Contractual deadline	30/06/2017
Dissemination Level	PU
Nature	R
Author	IKL
Contributors	-
Reviewer	USI and IAB
Keywords	Certification, Safety Concept, Railway, Avionic, Plan

Notice:

This project and the research leading to these results has received funding from the European Community's H2020 program [H2020-ICT-2015] under grant agreement 687902

Change log

VERSION	DESCRIPTION OF CHANGE
v0.1	Draft version based on D2.4.
v0.2	Integration of Appendix A, Appendix B and comments of D2.4 considered
v0.3	To be reviewed by TÜV Rheinland
v0.4	TÜV Rheinland feedback is considered
v0.5	Ready for internal Review
v0.6	USI and IAB members’ feedback considered
v1.0	Submitted version

Table of contents

1. EXECUTIVE SUMMARY

This D2.5 Final Safety Concept deliverable is mapped into task T2.3 Safety Concept within WP2. The main objective of WP2 is to develop a cross-domain reference architecture for low-power mixed-criticality systems comprised of networked multi-core chips that takes into consideration relevant safety standards (e.g., IEC 61508). The purpose of task T2.3 is to define and positively asses a safety concept considering safety implications of low-power techniques in the view of future industrialization. The outcomes of this task will be later explained in Section 0 of this document.

In order to achieve mentioned objectives, other WPs have also considered safety implications on their tasks. In Task T1.1 deliverable D1.1 [1] was developed, which contains most relevant cross-domain industrial requirements. These requirements considered, among others, safety/security standard requirements. Deliverable D1.2 [2] carried out on Task T1.2, offers an analysis and selection of low-power and CRTES technology, all candidate technologies and their combination were investigated from a safety standard perspective.

The results and conclusions of task T2.3 “Safety Concept” will be incorporated in tasks T2.1 “Definition of Reference Architecture” and T2.2 “Definition of Low-Power Techniques”. In particular, deliverable D2.2 “Initial Low Power Techniques” has its focus mainly on particular low-power technologies and their compliance with safety standards. The aim of this document is to offer a global overview of all the activity that has been carried out within the T2.3 “Safety Concept” task of WP2. In fact, this task has several phases including the review and feedback on a certification authority (e.g., TÜV Rheinland) which has required a living document that has been evolving across time.

Overall, the goals of the T2.3 Safety Concept task for certification analysis are:

- **GOAL1:** to assess the technical compliance of SAFEPOWER technology w.r.t. certification standards by achieving the positive assessment of an independent certification authority.
- **GOAL2:** to achieve this assessment and feedback early in the research project (M12-M15) to steer the technical choices in the proper direction.

To this end, the remainder of this document is structured within three separate chunks: Section 0 provides a detailed description of task T2.3 “Safety Concept” planning, explaining the deadlines and several interactions with the different actors (EC, Certification Authority and other tasks within SAFEPOWER); section 3 defines the Safety Concept structure for the railway signalling case-study application within the project based on the SAFEPOWER approach. And, section 4, defines the Safety Concept structure for the avionics use case.

Two dossiers on certification have been generated within task T2.3: a first dossier for the railway signalling case-study application, which has been reviewed by a certification authority during Q1-2017, and, additionally, a second dossier on avionics that has taken as argumentation the SAFEPOWER architecture and the safety-concept document on the railway domain to analysis the certification conformity on the avionics sector considering

EASA’s CAST-32A position paper. Both dossiers have been classified as confidential and are part of deliverable D2.5 “Final Safety-concept”.

2. PLANNING

This section describes Task 2.3 "Safety Concept" planning (Table 1), which lasts from M6 to M18. The safety concept has been delivered and assessed on two stages, from M6 to M9 the initial safety concept (Task 2.3.1) has been developed, as an early version of the safety-concept and its feedback has been reported in deliverable D2.4 that has been released to the EC. The final safety concept (Task T2.3.2) has been carried out from M10 to M18; this task comprises the preparation of the TÜV assessment and the final version of the safety concept. To this end, the safety concept has been first updated with the feedback from the EC and then all necessary documents and presentations for the certification authority (e.g., TÜV Rheinland) assessment have been prepared. According to the feedback received from the certification authority and the extended features, the safety concept has been updated once again. Finally, this consolidated final safety concept version has been released to the EC together with deliverable D2.5.

Table 1: Task T2.3 Safety Concept planning

	year 1							year 2						
	6	7	8	9	10	11	12	13	14	15	16	17	18	19
WP2 Task 2.3	■	■	■	■	■	■	■	■	■	■	■	■	■	
TASK 2.3.1 INITIAL SAFETY CONCEPT	■	■	■	■										
D2.4 EC Review					■									
TASK 2.3.2 FINAL SAFETY CONCEPT					■	■	■	■	■	■	■	■	■	
Task 2.3.2.1 Certification Authority assessment preparation					■	■	■							
Review meetings planning					▨									
Update Safety Concept with feedback from EC						▨								
Document and presentations preparation							▨							
Task 2.3.2.2 Safety Concept final version preparation										■	■	■		
Update Safety Concept with feedback from Certification Authority										▨				
Integration of the extended features in the Safety Concept										▨	▨	▨		
Task 2.3.2.3 Safety Concept 2nd version													■	
Review prior to release													▨	
Safety Concept 2nd version release for EC (D.2.5)													▨	
D2.5 Review														■

Figure 1 shows the content evolution from deliverables D2.4 (M9) to deliverable D2.5 (M18). The former is an initial version of the safety concept, which contains an introduction and planning of the safety concept task and an initial version of the railway use case safety concept as an annex. On the transition from one to another, there is an intermediate interaction with the certification authority that will include EC feedback, as well as IAB concerns and insights of the SAFEPOWER technology (the catalogue of low-power techniques) developed for the primary phase of the project. This interaction has been developed on Task 2.3.2.2 and has been completed by M15. The later, is the final version of the safety concept, which contains the introduction and conclusions related to the safety concept and the final version of the railway use case safety concept. In the avionics domain there is not any formal external authority (such as, TÜV Rheinland) to assess the technical compliance of the SAFEPOWER approach, therefore, this report includes generic cross-domain conclusions derived from the certification authority review and which can be extrapolated to the avionics use-case. An initial analysis of the CAST-32A position paper of the EASA has been elaborated to check its compliance of the SAFEPOWER architecture.

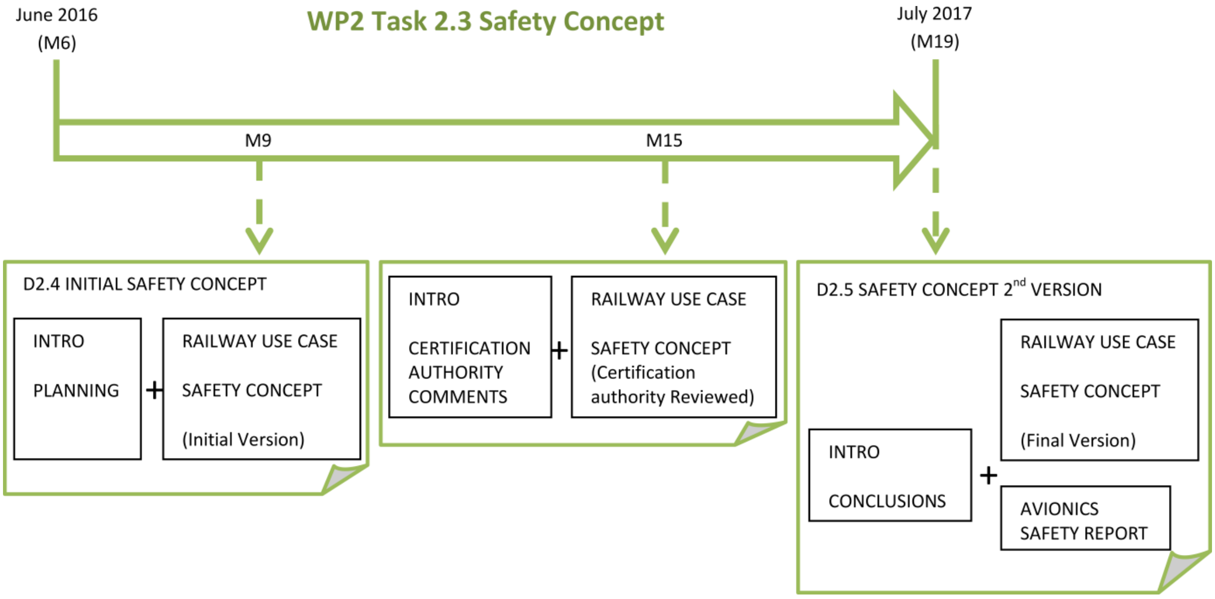

Figure 1: Task T2.3 deliverable evolution

3. SAFETY CONCEPT STRUCTURE (RAILWAY)

A safety concept serves to demonstrate the technical compliance of specific technologies w.r.t. to a specific certification standard for a given application. It is developed by defining the safety goals and safety architecture of the system to achieve an acceptable level of safety. Within the SAFEPOWER safety-concept, security aspects are also considered on a separate annex. As it is reviewed by an independent certification agency, the safety concept is a self-contained and self-explanatory document with the following parts:

1. **Introductory part:** The SAFEPOWER project is introduced and the key technologies described (i.e., application domain, mixed-criticality, Zynq technology, low power, etc.). The intention of this section is to provide context to the certification authority and it is not formally reviewed.

2. **Safety Requirements:** The safety requirements and the scope of the industrial application are shown. This section is reviewed by the certification authority. In this respect, only safety (and security) relevant project requirements are tracked down to the concept and specific new requirements are defined to illustrate the safety case of the application under assessment. The implementation of those requirements within the scope of the research project ends up with its evaluation w.r.t. the certification standard. If a requirement is marked as mandatory within the safety-concept, it will be mandatory during the industrialization and certification on a follow up to the research project.

3. **Safety Concept:** The definition of the safety concept starts with the description of a federated approach that is 'common practice in industry'. This section is reviewed by the certification authority. The federated safety concept is then transformed into an integrated mixed-criticality solution described in a top-down approach. In the case of SAFEPOWER the transformation is carried out through the following steps:

    a. *System-level safety Concept*: A federated architecture composed of three replicated safety related nodes in a triple module redundant (TMR) architecture and several non-safety-related nodes is described on a high abstraction fashion.

    b. *Detailed node-level safety concept*: all the details of the SAFEPOWER node safety argumentation are provided (fault hypothesis, FMEA, safety techniques and measures and system reaction to errors) to justify the validity of the SAFEPOWER multicore partitioned approach. To show the safe management of low power techniques in the SAFEPOWER architecture, the use of degraded modes is also explained in this section.

Appendix A: Security Analysis: additionally to the more classical safety-concept, the SAFEPOWER approach will also consider the way a security analysis is performed and this will be illustrated within this annex. This annex is reviewed by the certification authority.

Appendix B: Low Power Techniques: the SAFEPOWER techniques and services are included within the application together with their safety implications.

As commented in the planning on Section-2, the initial Safety-Concept version was completed with EC, IAB and project technology feedback and was consolidated in D2.5 (M18) after the review of the certification authority.

4. SAFETY CONCEPT STRUCTURE (AVIONICS)

CAST-32A position paper [3] studies the certification of multicore processors on avionics context and the objective of the Avionics Safety Concept is the analysis of the CAST-32A paper highlighting its main guidelines and considering the SAFEPOWER architecture. The avionics dossier is divided in the next sections:

1. **Executive summary**

2. **Introduction and scope**: The avionics context is introduced with related to multicore processors, because the current avionics standards only cover single-core systems. This section is completed with an overview of the SAFEPOWER approach and the specification of the provided services.

3. **CAST-32A summary:** The objective of the position paper is to identify the aspects that could impact on safety performance and this section summarizes its main topics. Additionally, two key concepts are highlighted: the Robust Partitioning and the Safety Net, which support the argumentation for a certification process.

4. **Analysis:** SAFEPOWER on the scope of CAST-32A: This section mentions three aspects of SAFEPOWER architecture which are compatible with the position paper:

    4.1 Partitioning SAFEPOWER local scope software partitioning with an embedded hypervisor and global scope hardware partitioning with a statically configured NoC.

    4.2 Planning: as safety certification standards do not recommend the use of dynamic configuration, SAFEPOWER considers pre-computed static schedules.

    4.3 Planning: Monitoring: SAFEPOWER presents partition level fault hypothesis and Failure Mode and Effect Analysis

5. **Conclusion:** The main conclusions are obtained in terms of analyzed partitioning, planning and monitoring issues. This certification dossier will be updated in Task 5.4 “Validation of the safety concept and compliance with standard”.

5. SUMMARY

This deliverable describes the goals of Task 2.3 for certification analysis through safety-concept argumentation and the planning to achieve does goals. To this end, the safety concept approach is described and it is illustrated with a railway case study safety concept.

The main contributions of the safety concept are listed below:

1. Degraded modes: to deal with power management in safety critical applications, the low-power approach is focused on the use of degraded modes. This technique, called also *Graceful degradation* (IEC 61508-3) [4] is used to allow a lower power consumption by dropping the less critical functions. Each of the operational modes includes a predefined and predictable configuration.

2. The analysis of how the application of low-power techniques impacts on safety. For this analysis, FMEA analysis is used in order to propose failure detection methods when a specific low power technique is implemented. To complete the study, safety arguments related with each function are also determined. These safety arguments are presented in the DREAMS project [5] to demonstrate that safety properties are satisfied for a given application in a given environment.

3. The security analysis: a first approach of security analysis is carried out proposing the use of different security requirements regarding the specific power mode. The objective is to make a first attempt for a system that is not mature and bearing in mind that safety is the main purpose. It is also an approach to assess the implication of power management features in security.

After the elaboration of the safety concept and the review process with the certification authority, the related significant conclusions are obtained.

- Regarding certification process, the importance of the predictability must be highlighted. The use of state machines, which consider all possible scenarios, contributes to the compliance with safety standards.
- In order to obtain cross-domain conclusions, a systematic comparison of different domain standards will be helpful. In case of avionics, comparing the DO-178B[6]/DO-254 [7] with the generic standard IEC61508 [8] and the railway specific EN 5012x will help extrapolating safety concept guidelines to the avionics application.
- The safety analysis of each low-power technique is largely dependent on its specific implementation and the specific device. Safety arguments help providing a more generic perspective.

Regarding avionics domain, the initial certification analysis reflects the coherence of the SAFEPOWER architecture with main CAST-32A position paper guidelines:

- SAFEPOWER supports the required robust partitioning in both software level (with hypervisor) and hardware level (with the NoC).
- SAFEPOWER requires also a planning in terms of software, timing and resource allocation.
- Partition level monitoring of SAFEPOWER is compatible with CAST-32A terminology with respect to failure mode analysis

The updated version of the avionics safety report will include guidance about the use of low-power techniques in the scope of certification analysing their safety impact. Equally, it will provide a clarification in terms of feasible dynamic features, because although they are mentioned in CAST-32A, their application is not clear.

6. REFERENCES

[1] CAF, "Deliverable D1.1 - Cross-domain industrial requirements - Version 1.a," SAFEPOWER2016, Available: http://safepower-project.eu/.

[2] OFFIS, "Deliverable D1.2 - Analysis and selection of low power techniques, services and patterns - Version 1.0," SAFEPOWER2016, Available: http://safepower-project.eu/.

[3] F. A. Administration, "Certification Authorities Software Team (CAST) - Position Paper CAST-32A: Multi-core Processors," ed, 2016.

[4] IEC 61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements, IEC 61508, 2010.

[5] "DREAMS - D5.1.2. Modular Safety Case for COTS processors," 2015.

[6] RTCA/DO-178B, Software Considerations in Airbone Systems and Equipment Certification, 2012.

[7] RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, 2000.

[8] IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements, IEC 61508, 2010.