SAFEPOWER

D6.5 Communication and Dissemination reports

V1.0

Document information

Contract number	687902
Project website	safepower-project.eu
Contractual deadline	01/07/2016
Dissemination Level	PU
Nature	Report
Author	UNIVERSITAET SIEGEN (USI)
Contributors	All
Reviewer	IK4-IKERLAN (IKL)
Keywords	Dissemination

Notices:

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	First draft USI (Babak Sorkhpour)
V0.2	Second draft USI (Roman Obermaisser)
V0.3	3rd Draft USI (Babak Sorkhpour)
V0.4	4th Draft USI (Babak Sorkhpour)
V0.5	Reviewed by IKL (Laura Ezkurra, Cristina Zubia)
V1	Submitted version

Table of contents

1. EXECUTIVE SUMMARY 5

2. INTRODUCTION 6

2.1. ESTABLISHMENT PROCESS OF THE DELIVERABLE 6
2.2. CONTENTS OF THE DELIVERABLE 7

3. DISSEMINATION POLICY, GOALS AND PLAN 8

3.1. BROADCAST OF THE RESEARCH RESULTS TO SCIENTIFIC COMMUNITY 8
3.2. DISSEMINATION TO INTERESTED INDUSTRY SECTORS 8
3.3. COMMUNICATION TO SAFETY-CERTIFICATION ORGANIZATIONS 9
3.4. INFORMATION EXCHANGE WITH OTHER RELATED FP7, CIP AND H2020 PROJECTS 9
3.5. PUBLIC AWARENESS 9

4. TIMELINE 11

5. TARGET GROUPS 12

5.1. INDUSTRIAL DOMAINS 12
5.1.1. Avionics 12
5.1.2. Railway 13
5.1.3. Further Domains 13
5.2. STAKEHOLDERS ALONG SUPPLY CHAINS 13
5.2.1. System Integrators 13
5.2.1.1. Tool Developers 14
5.2.1.2. Hardware platform developers 14
5.2.1.3. Tool developers 14
5.2.2. Public 15

6. DISSEMINATION 16

6.1. SCIENTIFIC DISSEMINATION 16
6.1.1. Architectures 16
6.1.2. Real-Time Systems and Scheduling 16
6.1.3. Fault Tolerance 17
6.1.4. Certification and Safety 17
6.1.5. On-chip Networks 17
6.1.6. Virtual platforms 18
6.1.7. Low power systems 18
6.1.8. Operating Systems and Hypervisors 19
6.1.9. Application Domains (Scientific) 19
6.2. INDUSTRIAL DISSEMINATION 20
6.2.1. Avionics 20
6.2.2. Railway 20
6.2.3. Targeted "Position" in Supply Chains – Hardware 21
6.2.4. Targeted "Position" in Supply Chains – Software developers 21
6.2.5. Targeted "Position" in Supply Chains – Tool developers 21

7. DISSEMINATION CHANNELS 22

7.1. SCIENTIFIC AND ACADEMIC CHANNELS 22

7.2. CHANNELS FOR INDUSTRIAL DISSEMINATION........ 23
7.3. COMMUNITY CHANNELS 23

8. REPORT OF DISSEMINATION ACTIVITIES........24

8.1. PAST ACTIVITIES........ 24
8.2. UPCOMING ACTIVITIES 25

9. PROCEDURE FOR THE DISSEMINATION OF THE ACTIVITIES AND PUBLICATIONS 26

1.EXECUTIVE SUMMARY

This deliverable provides the first report on the communication and dissemination plan of the SAFEPOWER project.

The goals of the SAFEPOWER dissemination strategy comprise the broadcasting of the research results in order to achieve the widest possible awareness and external communication of results and technologies from SAFEPOWER.

The dissemination activities are aligned with the SAFEPOWER timeline and the appropriate results in the different phases of the project.

Main dissemination target groups of SAFEPOWER comprise stakeholders in the SAFEPOWER application domains (avionics, railway) as well as stakeholders along supply chains (e.g. system integrators, tool developers), safety-certification organizations, other research projects, relevant scientific communities and the public at large.

Scientific dissemination addresses different communities, such as real-time systems and scheduling, multi-core chips, model-based development. Industrial dissemination takes place in the SAFEPOWER application domains as well as along the supply chains. Furthermore, different dissemination channels are introduced for the scientific and industrial communities.

The reporting of past and upcoming dissemination activities gives an overview of the different publications, presentations and events that have already been carried out or that are planned for the future.

2.INTRODUCTION

This deliverable is the first report on the dissemination strategy, goals, target groups and dissemination channels. The SAFEPOWER dissemination plan provides a regular flow of information rather than occasional ad-hoc announcements since this will contribute to the establishment of recognition and increase the opportunities for publicity.

Dissemination comprises the following activities:

- Creation of a project web site for marketing purposes and its maintenance during the lifetime of the project.
- Preparation of communication and dissemination materials (logo, visual identity, communication templates flyer roll-up banner, poster, standard presentation with key messages, one page project description).
- Preparation of project dissemination plans.
- Preparation and presentation of scientific publications at conferences and their publication in academic journals.
- Participation in meetings of certification agencies.
- Newsletters.
- Social Media presence.

2.1. Establishment Process of the Deliverable

The initial steps in the establishment process of this deliverable comprised a clear definition of the target groups for the SAFEPOWER dissemination and exploitation. It was followed by a thorough analysis of stakeholders within the target groups also including supply chains.

Project-internal experts of the respective SAFEPOWER application domains (see Table 1) contributed to this analysis and identified the key industrial dissemination interests in SAFEPOWER as well as the targeted "positions" in the supply chains (e.g., software developers, system integrators).

Table 1: SAFEPOWER main industrial domains and experts

Industrial Domain	Partner	Lead Expert
Avionics	SAA	Gustav Johansson
Railway	CAF	Manuel Villalba
Further domains	IKL	Peio Onaindia (vertical transportation) and Jon Perez (industrial control machinery, wind-turbines)

In parallel, the scientific domains represented in SAFEPOWER were identified and dedicated experts were selected to take care of the scientific community needs (see Table 2).

Table 2: SAFEPOWER scientific domains and experts

Scientific Domain	Partner	Lead Expert
Architectures	USI	Roman Obermaisser
Real-Time Systems and Scheduling	FENTISS	Alfons Crespo
Fault Tolerance	USI	Roman Obermaisser
Certification and safety	IKL	Mikel Azkarate-askasua
On-chip networks	KTH	Johnny Öberg
Virtual platforms	IMPERAS	Duncan Graham
Low power systems	OFF	Kim Grüttner
Operating Systems and Hypervisors	FENTISS	Alfons Crespo

2.2. Contents of the deliverable

This document is organized as follows. In section 3, the dissemination policy and goals are given and a detailed analysis of the dissemination pillars is presented. Section 4 is about the dissemination timeline of the overall dissemination events and tasks within the overall timeline of the project. In section 5 the targeted dissemination groups are analysed for the major groups of application domains, stakeholders of the supply chain and public. Section 6 introduces dissemination strategies at the different levels of SAFEPOWER from a scientific and commercial point of view. Scientific, commercial and community channels of dissemination are illustrated in section 7. A report of past dissemination activities and planned activities is presented in section 8. Finally, in section 9 the procedure for the dissemination of the activities and publications is described.

3.DISSEMINATION POLICY, GOALS AND PLAN

SAFEPOWER has set up a complete range of activities leading to the optimal visibility of the project and its results, increasing the likelihood of market uptake of the knowledge it produces and ensuring a smooth handling of the individual and collective intellectual property rights of the involved partners in view of paving the way to knowledge transfer.

The dissemination strategy of the SAFEPOWER project consists of the following five pillars: First, broadcast of the research results to scientific community through publications and newsletters. Second, the dissemination to interested industry sectors at industrial conferences, workshops and using the advisory board. Third, the communication to safety-certification organizations. Fourth, information exchange with other related FP7, CIP and H2020 projects. And fifth, public awareness. In the following, a detailed analysis of the pillars is presented.

3.1. Broadcast of the research results to scientific community

The broadcast of the research results will be achieved by presentation of the results in leading international conferences and in leading scientific journals. The academic and industrial partners will spread the know-how of the SAFEPOWER project by the following means:

- Publication in high-ranked international journals, e.g. Journal of Computer Systems Science & Engineering, Computing & Control Engineering Journal, IEEE Transactions on Dependable and Secure Computing, IEEE Embedded Systems Letters, etc. as well as presentation at leading European and international conferences, e.g., IFAC World Congress, IEEE International Conference on Emerging Technologies and Factory Automation, IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Design Automation and Test, Design Automation Conference, the Network-on-Chip Symposium, IEEE RTSS, ECRTS, the Embedded Systems Week conferences, Embedded Real Time Software and Systems Congress, etc.
- Publications and conference presentations involving several project partners will illustrate the joint research effort and dissemination approach. This is achieved by means of collaborating with project partners in the elaboration of research papers for journals, conferences and workshops.

3.2. Dissemination to interested industry sectors

The SAFEPOWER results will be presented at various exhibitions, fairs and conferences. At selected events (e.g. bi-annual ICT Event, ARTEMIS Technology Conference, HIPEAC) project presence will be ensured to highlight project achievements and to connect to stakeholders and decision makers. Posters and handouts will be used to describe the SAFEPOWER project and expected results. Demonstrators will be used for visualization purposes. Furthermore, press releases shall be distributed in advance to the subject fair/exhibition via email in order to raise the attention. Partners exhibiting will represent the SAFEPOWER consortium and will also distribute SAFEPOWER brochures and other materials and will display SAFEPOWER posters at their exhibition and booths.

3.3. Communication to safety-certification organizations

The SAFEPOWER project has a direct communication with TÜV Rheinland certification organization as an Industrial Advisory Board member. Besides, the technical compliance of the technology developed in SAFEPOWER w.r.t. safety-certification standards will be assessed by a safety-certification organization (e.g., TÜV Rheinland or equivalent) through a use-case (e.g., railway) safety concept and direct discussions and feedback are planned. Additionally, the bi-annual TÜV Rheinland Symposium targeting industry and safety-certification community is identified to publish a SAFEPOWER position paper or a summary of the previously mentioned safety-concept.

3.4. Information exchange with other related FP7, CIP and H2020 projects

The SAFEPOWER project is firmly based on other European and national projects in different industrial domains and technological areas. In case of on-going projects, continuous information exchange between the projects is planned.

The SAFEPOWER project is part of the mixed-criticality cluster, which also includes the FP7 projects DREAMS, CONTREX and PROXIMA. The mixed-criticality cluster organizes joint events (e.g., joint booths, workshops and special sessions on mixed-criticality at conferences) and provides a platform for the exchange of technical results and strategic information (e.g., upcoming events). The mixed-criticality cluster also organizes regular telephone conferences with the coordinators and dissemination leaders of the projects.

In addition, SAFEPOWER has joined the mixed-criticality forum[1], which provides news on mixed-criticality activities, a catalogue of projects' results and a code repository. This forum increases the visibility of mixed-criticality projects and provides a basis for joint dissemination and exploitation.

3.5. Public Awareness

The measures described above are also targeted to have impact on non-SAFEPOWER stakeholders. To further raise the public awareness for innovative steps the following communication tools will be used to spread the achievements of the SAFEPOWER project:

- **Project homepage** covering the project's goals, objectives, accomplishments, background information and partner's role and contribution. It runs in parallel with the project's evolution in order to provide timely and appropriate information, thereby being constantly updated and maintained.
- **Press releases** (that are mutually released by agreement of all project partners) will be issued on a regular basis.

[1] http://www.mixedcriticalityforum.org

- **Social Networks:** The SAFEPOWER project is active in the social networks LinkedIn and twitter.

The visibility of the SAFEPOWER project is strengthened through a project logo, project design for Power-Point slides, reports and poster templates. In addition, several partners include information about SAFEPOWER on the webpages of their organizations. Partners show the SAFEPOWER logo on their websites and add a description of the project, its goals, and results.

4.TIMELINE

Dissemination of results within SAFEPOWER is closely coupled to the timing of the project and the respective phases. The dissemination work package starts in project month one and concludes together with the overall project in month 36.

The three main phases of SAFEPOWER and their temporal order are as follows:

- **PHASE I: Technical development phase:** During this phase the preparatory work (e.g., analysis of requirements) and the key technical developments of the project will be carried out. The outputs of this phase will be theoretical as a basis for the implementation during the next phases.

  The disseminated results of this phase will include the new architectural model and design, the methods and techniques for low-power consumption in mixed-criticality systems and the safety concept of the resulting architecture.

- **PHASE II: Implementation phase**: During this phase, the different outputs will be physically implemented into the prototypes. The disseminated results of this phase will include the SAFEPOWER architecture, techniques, methods, tools and platform technologies for low-power and safety (e.g., adaptable and safe NoC, novel simulation techniques, and hypervisor extensions).
- **PHASE III: Demonstration phase**: After the first prototypes are ready, the demonstration phase will occur. In parallel, the implementation of the SAFEPOWER platform will be finalized. The disseminated results will include information about the demonstrators, evaluations of the SAFEPOWER technology and information about the final virtual and physical platforms.

5.TARGET GROUPS

The aim of the dissemination activities is to widely spread the project results to the relevant communities and to increase public awareness of its benefits. The purpose of this chapter is to identify the main dissemination target groups and describe their interests and specify methods to address these interests.

5.1. Industrial Domains

The following subsections provide information on the stakeholder groups of the different application domains addressed by SAFEPOWER.

5.1.1.Avionics

The group of stakeholders in the avionics domain reaches from global airplane manufacturers down to SMEs representing external suppliers or third-party service providers.

The concept of Integrated Modular Avionics (IMA), which is applied in modern aircrafts, allows the parallel use of the same hardware for different applications. The number of applications using the computational resources of the system is steadily growing. Hence, the avionics domain is currently facing the growing need for an increase of processing power without increasing the power supply or equipment weight. Single core processors have reached their limits due to physical bounds of the maximum core frequency, which leads to the introduction of parallel computing into critical systems deployed in the avionics domain.

The first generation of multi-core solutions available to the avionics industry is limited for use in safety-critical applications because of shared resources. Since hardware is shared in an IMA system it is essential that more than one safety-critical application can be independently executed on the same hardware without interfering with each other. This will also open the possibility to have mixed-criticality applications on the same hardware.

The solutions of predictable multi-core platforms, networked multi-core chips for mixed-criticality applications and fault-recovery mechanisms as proposed by SAFEPOWER, are very relevant in this domain together with the architectural style, models, development tools and methods.

In view of recently published guidelines on certification objectives from authorities in the avionics domain it is important to develop new possibilities for parallel computing, where the SAFEPOWER platform is a candidate to meet these objectives.

5.1.2. Railway

The railways domain is a promising candidate since the dependability of critical systems plays an important role in this domain. The functional safety standard IEC-61508 is of central importance when it comes to validation and certification of railway systems.

In the railway domain, low power requirements are present both in the infrastructure side and on-board the trains. Energy savings are always welcome, but in some cases the available energy is limited. Typical cases are remote places along the railway infrastructure, and freight wagons. Removing the need for power cables is also advisable to avoid their theft and the subsequent interruption of the railway service.

5.1.3. Further Domains

Further application domains beside the ones covered by SAFEPOWER demonstrators are also relevant for dissemination of the achieved results.

For example, an interesting field of application for the SAFEPOWER results is the automotive domain. Modern cars have more than 50 electronic control units, which run applications with different criticality levels (e.g. brake control, multimedia). The SAFEPOWER results in regard to virtualization and segregation of subsystems could help to significantly reduce this number by providing the possibility to combine several electronic control units virtually on one platform.

Another interesting field is vertical transportation. Modern lifts include strong safety requirements (e.g., door closing/opening) and a set of increasing energy requirements related to the back-up energy storage systems that are jointly installed e.g., to safety move the lift in case of blackouts. Similar safety and energy requirements could be found on wind-turbine and other industrial machinery control applications that often have to reach a safe state also with a limited energy budget.

5.2. Stakeholders along Supply Chains

In the following different stakeholders along supply chains are described ranging from system integrators to suppliers.

5.2.1. System Integrators

The key role of system integrators is the integration of software and hardware components for complex systems, such as airplanes, trains or factory automation systems. System integrators often provide reference platforms to suppliers and architectures to be used for their own developments.

System integrators are a key part of the supply chain stakeholders, because SAFEPOWER covers a platform combing safety and power-efficiency with the seamless integration of independently developed mixed-criticality subsystems with real-time support and reliability.

5.2.1.1. Tool Developers

Tool developers are responsible for the provision of adequate tooling for different purposes during the development of the system. Their products reach from simple programming tools and compilers up to complex integrated development environments as well as model transformation, design exploration and optimization tools and platform component configurators as part of model-driven development methodologies.

The main objective of the development tools is to increase efficiency and productivity of the customers that apply the tools within their companies. This goes along with a reduction of complexity by only focusing on the relevant parts. A model-driven engineering suite for mixed-criticality systems will enable the customer to concentrate on the models rather than having to deal with the implementation details directly. Other important groups of tool developers comprise providers of simulation environments and tool providers for system validation, verification and certification support.

5.2.1.2. Hardware platform developers

Hardware platform developers (e.g., semiconductor companies) need to be convinced of the benefits that are provided by the SAFEPOWER architecture and the ensuing added value for their customers. They require that SAFEPOWER addresses the technological challenges requested by the future application requirements in HealthCare, Avionic, Automotive, etc. to consider SAFEPOWER results in their services and products.

5.2.1.3. Tool developers

In analogy to hardware platform developers, software developers need to be made aware of the SAFEPOWER results with the ensuing economic benefits (e.g., productivity, time-to-market) and the technical characteristics (e.g., real-time, security). Software developers will be interested in the SAFEPOWER virtual platform.

Software developers will be able to use the SAFEPOWER virtual platform for application development and test, for the various vertical markets such as Automotive, Avionics, and Medical Electronics that SAFEPOWER addresses. Software tool developers will be able to build new tools to integrate with the SAFEPOWER virtual platform to extend the SAFEPOWER efforts in areas such as timing and power analysis, fault injection, and software quality and reliability.

5.2.2. Public

Achievements and results of the project will be made known to a wide public through effective dissemination material and activities. Examples are press releases and high-level overviews (in addition to detailed technical information) on the project web page. The participation in public events related to application domains to address their own customers will also play an important role to increase public awareness and interest in innovative mixed-criticality solutions. Additionally, newsletters, articles and many of the project deliverables will be available to the public through the project’s webpage.

6. DISSEMINATION

SAFEPOWER dissemination takes place in the scientific as well as in the industrial area. More detailed information on the covered domains and fields of research is provided in the following subsections.

6.1. Scientific dissemination

6.1.1. Architectures

One of the primary scientific fields covered by SAFEPOWER is the area of computer architectures. Distributed system architectures provide the scientific and engineering foundation for the construction of embedded systems. The goals are to discover design principles and to develop architectural services that enable a component-based development of embedded systems in such a way that the ensuing systems can be built cost-effectively and exhibit key non-functional properties (e.g. composability, robustness, maintainability).

Especially the area of real-time architectures is of special interest. It covers architectures, models and techniques related to real-time processing of data as well as the associated communication between the architectural components.

The domain is currently facing significant challenges as for example the shift from single core processor architectures towards multi/many-cores. Beside the shift from single to multi/many-core architectures, the semiconductors suffer reduced reliability w.r.t. transients due to manufacturing processes with ever-smaller structure widths. In addition, the inter-chip, inter-device and inter-machine communication plays an increasingly important role for the architecture of a system. Another key issue is energy efficiency since many architectures are targeting mobile devices with an ever-presence of power constraints.

Examples of communities of interest for disseminating the SAFEPOWER results are the Real-Time and Embedded Technology and Applications Symposium (RTAS) and conferences and workshops such as Annual International Computer, Software & Applications Conference (COMPSAC), Architecture of Computing Systems (ARCS), International Conference on Cyber-Physical Systems (ICCPS), Real-Time Service-Oriented Architecture and Applications (RTSOAA).

6.1.2. Real-Time Systems and Scheduling

The dissemination of SAFEPOWER scientific innovations in the field of real-time systems is one of the key scientific channels. Significant contributions of SAFEPOWER include mixed-criticality aspects (e.g., real-time scheduling of resources for subsystems with different criticalities), end-to-end real-time guarantees across networked multi-core chips, real-time support upon the integration of different models of computation, integrated resource management and the consideration of temporal guarantees in design space exploration together with further extra-functional requirements such as reliability and energy efficiency. The scientific dissemination in the field of real-time and scheduling can be done through publications in numerous conferences such as the IEEE *real-time system symposium* (RTSS), the international flagship conference, Euromicro conference on real-time systems (ECRTS), the top quality European venue, *real-time and embedded technology and applications symposium* (RTAS), the major application and systems oriented symposium, a number of focused workshops, such as the Workshop on Mixed Criticality Systems (WMC), *workshop on applications for multi-core architectures* (WAMCA), *workshop on scheduling for parallel computing* (SPC) and *real-time systems* (journal). The relevance to these conferences and journals is mainly related to the scientific work in WP2 “Reference SAFEPOWER architecture” andWP3 “Platform implementation”.

6.1.3. Fault Tolerance

Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components. There is a large number of conferences and journals that are focusing on the dependability aspects of the systems that can be targeted during the dissemination of the SAFEPOWER project, such as the *international conference on dependable systems and networks* (DSN), *European conference on computer systems* (EuroSys), ACM *dependable and adaptive distributed systems* and *the IEEE transactions on dependable and secure computing*. The scientific research solutions related to this topic are the outcomes of the work done in WP2-3.

6.1.4. Certification and Safety

Safety is one of the key points in regard to critical systems deployed in domains such as avionics or railways. In this context, safety and especially safety engineering is always closely coupled to certification.

As SAFEPOWER is focusing on mixed-criticality systems safety is a key aspect of the SAFEPOWER architecture defined in WP2. Certification is dealt with in WP2 providing a safety concept on the scope of one of the use-cases. It is important to mention that the SAFEPOWER architecture will not be certified itself since this is out of the scope of the project, but the technical compliance of the SAFEPOWER technology w.r.t. safety-certification standards will be assessed.

6.1.5. On-chip Networks

Networks-on-chip have a huge potential as platform for low-power mixed-criticality multiprocessor systems. In particular, network-on-chips can provide a scalable and predictable communication structure for multiprocessor systems, which even can cope with faulty communication links. The scientific research related to this topic is conducted in WP2 and WP3.

SAFEPOWER aims to disseminate the scientific results in relevant premium and specialized conferences, like Design Automation and Test in Europe (DATE), Design Automation Conference (DAC), International Symposium on Networks-on-Chip (NOCS), and Hardware/Software Codesign and System Synthesis (CODES+ISSS), and leading international journals, like IEEE Transactions on Very Large Scale Integration (VLSI) Systems (TVLSI) and ACM Design Automation of Electronic Systems (TODAES).

6.1.6. Virtual platforms

Virtual platforms are state-of-the-art for functional software testing. Compared to software testing on a hardware prototyping board, virtual platforms offer the advantage of full non-intrusive observability. This enables better testability of complex software systems. Furthermore, virtual platform can be easily integrated into regular software regression tests and make embedded software development in large teams more efficient. The advantages of virtual platforms come at the cost of reduced timing accuracy and support for extra-functional properties (such as power consumption and temperature). Within SAFEPOWER, the following virtual platform extensions are interesting for dissemination to a scientific and technical audience:

- Time triggered execution scheme for instruction accurate virtual platforms
- Quasi cycle accurate timing extensions for dynamic translation based virtual platforms with multiple processors and shared resources
- Power and temperature models and measurement based model construction/calibration for virtual platforms
- Virtual power and temperature sensors for providing software access to the power and temperature model (support for testing of software power and temperature management)

These contributions could be disseminated through the following scientific channels: Design Automation Conference (DAC), Design, Automation and Test in Europe (DATE) conference, Euromicro Conference on Digital System Design (DSD), International Workshop on Software and Compilers for Embedded Systems (SCOPES), International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS), HiPEAC conference, ACM TODAES Journal, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.

The following industrial conferences and exhibitions are also suitable dissemination channels: EmbeddedWorld Conference & Exhibition, ARM TechCon.

6.1.7. Low power systems

The main goal of SAFEPOWER is the usage of low power techniques in Critical Real-Time Embedded Systems. The focus of the project is on the application of well-known techniques (such as clock gating, voltage gating and dynamic frequency & voltage scaling (DVFS)). For this reason, the project will not advance the state-of-the-art in low power system design, but come up with architectural principles and solutions to safely integrate power management into hard real-time systems. Targeted conferences include the traditional EDA oriented conferences: Design Automation Conference (DAC), Design, Automation and Test in Europe (DATE) conference, Euromicro Conference on Digital System Design (DSD), International Workshop on Software and Compilers for Embedded Systems (SCOPES), International Conference on Embedded Computer Systems: Architectures and Modelling and Simulation (SAMOS). As well as the main real-time system conferences: IEEE real-time system symposium (RTSS), Euromicro conference on real-time systems (ECRTS) and real-time and embedded technology and applications symposium (RTAS).

6.1.8. Operating Systems and Hypervisors

Operating systems abstract from the underlying hardware by providing the user with a set of services and interfaces. Hypervisors are used to virtualize computational resources such as embedded platforms. Virtualization of the hardware makes it accessible to different software components at the same time.

Hypervisors are a key element of the SAFEPOWER architecture to provide virtualization on different levels. SAFEPOWER has a main focus on virtualization of multicore processors with strict temporal and spatial segregation.

Important conferences for operating systems and hypervisors include the ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments as well as International Virtualization Conference.

6.1.9. Application Domains (Scientific)

The SAFEPOWER project targets several application domains starting with the two project’s demonstrators (i.e. rail and avionics). The SAFEPOWER project plans to provide solutions and scientific methods to cover and convince the application domains to adapt the mixed-criticality approach of networked multicore systems based on the SAFEPOWER project. All scientific areas mentioned earlier are also important research topics for the application domains. In the following a list of candidate conferences and workshops is given that enable domain-specific dissemination of the SAFEPOWER scientific results.

- **Avionics:** Digital Avionics Systems Conference (DASC), International Symposium on Rapid System Prototyping (RSP)
- **Rail**: Railway use-case related publications could be addressed to the different industrial tracks mentioned below.
- **Industrial:** international conference on industrial informatics (INDIN), IEEE International Symposium on Industrial Embedded Systems (SIES), IEEE International Conference on Industrial Technology (ICIT)

- **Factory automation:** IEEE Conference on Emerging Technologies & Factory Automation (ETFA), IEEE International Workshop on Factory Communication System (WFCS)
- **Automotive:** Automotive Embedded Multi-Core Systems summit, Automotive meets Electronics (AME), SAE World Congress

6.2. Industrial dissemination

6.2.1. Avionics

Two different channels will be used for the commercial dissemination of the SAFEPOWER solutions for the avionics domain: internal and external.

For internal communication SAAB will present tools, methods, software & hardware solutions and certification approaches enabling the development of power-efficient mixed-critical solutions using internal dissemination events.

External dissemination of project results targeting the avionics domain can be done through the organization of sessions and/or booths at different events like http://paris-space-week.com.

To further spread the knowledge learned from the SAFEPOWER project the demonstrator will be used as an example and information basis when discussing projects with partners to the industry. These partners can be suppliers in the avionics industry, authorities, research projects or other domains that could benefit from the results, such as the automotive industry.

6.2.2. Railway

In order to promote the commercial use of the SAFEPOWER findings, CAF will deploy a number of actions:

- Internal dissemination of SAFEPOWER technical findings:
  - Information to the management of the company, including managers involved in R&D, Safety, Operations, Project engineering, Commercial and Marketing. This action will be started with a presentation to the Board of Directors. A first feedback will be requested, including the identification of follow-up actions.
  - Technical Seminar addressed to engineers involved in R&D tasks.
  - Technical workshop with members of the Safety Department
- Participation in specific external dissemination actions together with the SAFEPOWER Consortium. The specific actions to participate will be selected taking into account the interest of the potential audience in the railway business

- Workshop with one selected Independent Safety Assessor in order to identify the issues related to Safety Acceptance of products to be built using the SAFEPOWER technology.
- Brainstorming session with R&D, marketing and commercial managers in order to identify possible products that can benefit from the technology developed under SAFEPOWER project. This action could be followed by a business case analysis of the opportunities identified.

CAF is not interested in performing wide dissemination of technology results to their customers, because they show little interest in pure technological findings, and their main concern is in products and solutions that can benefit their business.

6.2.3.Targeted “Position” in Supply Chains – Hardware

The hardware implementations carried out in the SAFEPOWER project include the design and fabrication of a highly instrumented Printed Circuit Board (PCB) including a Xilinx Zynq chip. A possible industrial dissemination action could be done to open and publish the PCB schematics as a reference design in Sundance/Xilinx websites.

6.2.4.Targeted “Position” in Supply Chains – Software developers

Software developers shall be targeted as they are responsible for the extensions of SAFEPOWER architecture. Moreover, the software developers will be addressed to obtain very good understanding of this architecture in order to be able to provide tools, extensions of services (e.g. optional services) and software components based on SAFEPOWER. Software developers and their companies will be convinced by the SAFEPOWER benefits, i.e. improvement of the reuse of components and reduction of development costs due to the integration of mixed criticality. SAFEPOWER will provide training events and tutorials for software developers, which will open channels of communication with companies working in our field and the related industry as a whole.

6.2.5.Targeted “Position” in Supply Chains – Tool developers

IMP will promote and distribute the SAFEPOWER virtual platform through a variety of channels. These include an initial public announcement of the availability of the SAFEPOWER virtual platform in Q3 2016, posting information on the ARM Connected Community website, making the SAFEPOWER virtual platform available through the Open Virtual Platforms website (www.OVPworld.org), and promotion at various trade shows that Imperas participates in as an exhibitor. The SAFEPOWER virtual platform dissemination could also be targeted to industrial conferences such as ARM Techcon, DATE and Embedded World. While the dissemination materials for SAFEPOWER virtual platform will discuss both the technical and economic benefits and features of the virtual platform, the SAFEPOWER virtual platform will be delivered to users with SAFEPOWER software stack running on it, such as hypervisor and operating system, and so users will be able to demonstrate for themselves the technical characteristics and benefits of the virtual platform approach to software development.

7.DISSEMINATION CHANNELS

7.1. Scientific and Academic Channels

SAFEPOWER will participate in scientific dissemination by writing conference papers, journal articles, by preparing posters and giving presentations with SAFEPOWER project results. Target conferences and workshops will be those with scientific audience interested in embedded platform solutions, architecture, software and hardware components, certification, simulation as mentioned in the previous sections. Organizing conferences and special sessions is also very important for the dissemination strategy in SAFEPOWER. Examples of already co-organized events are:

- 4rd International HiPEAC workshop on the "Integration of mixed-criticality subsystems on multi-core and manycore processors, January 2016.
- Special session on mixed-criticality systems at 11th IEEE International Symposium on Industrial Embedded Systems (SIES'2016), May 2016.

Furthermore, concepts and solution ideas from the project results were disseminated at the Date Conference Workshop on Power Analysis in April 2016. Also, a position paper was submitted to the Euromicro Conference on Digital System Design. The position paper gives an overview of the state-of-the-art, the research challenges towards power-efficient mixed-criticality systems and the SAFEPOWER project.

In order to widen the recognition of SAFEPOWER and to ensure the scientific relevance of the project results, publications in journals are one of the key factors in disseminating scientific results of research projects. Partners of the SAFEPOWER consortium will consequently submit relevant results to important journals related to the mixed-criticality community.

Tutorials are part of the overall dissemination strategy of SAFEPOWER. At the one hand, they are planned to train the stakeholders or to demonstrate the results to them, and at the other hand, they can also be used to gather feedback about the project results.

The SAFEPOWER consortium features various research and academic entities that offer post-graduate programs to young researchers. The SAFEPOWER project proposes new aspects on research that are explored in the scope of PhD projects. Also, university partners will use selected project results in lectures as well as in bachelor and master theses, which will further disseminate the project results and raise awareness of mixed-criticality in the student communities.

7.2. Channels for Industrial Dissemination

A very important means for disseminating the results of the SAFEPOWER project will be through commercial dissemination channels. SAFEPOWER will participate in exhibitions and fairs of major conferences, as well as in specialized exhibitions. In these exhibitions, SAFEPOWER will demonstrate the solutions and services developed by the project through direct presentation to the relevant associations and organizations.

A preliminary list of industrial exhibitions is as follows:

- ICES
- Embedded world

SAFEPOWER, as an Innovation Action project will directly interact with the Industrial Community. Thus, two workshops will be organized by FEN and IMP with the support of the RTD partners of the consortium (IKL, OFF, USI, KTH).

7.3. Community channels

A dedicated project website was established early in the project lifecycle (M3) to provide wide dissemination of SAFEPOWER methodology, use-case activities, results and validation methods, papers, and general information about the project. USI, as Dissemination responsible, hosts the project website, providing uninterruptedly maintenance and refinement during the project lifecycle.

SAFEPOWER produces a newsletter every year, in electronic format and in English. News is also disseminated using social media. SAFEPOWER has set up a Twitter account and a LinkedIn profile. The LinkedIn profile has requested its membership in all H2020 specific related groups.

Clustering activities are performed including the mixed-criticality cluster and the mixed-criticality forum (cf. Section 3.4) in order to exchange information with co-existing projects (e.g., DREAMS, CONTREX, PROXIMA) to seek synergies to explore mutual benefits coming from a joint activity (e.g. booths in an event by sharing the space). Contacts with other relevant projects like DREAMS, PROXIMA, CONTREX and alliances from the industry will be established to communicate challenges and scientific findings. We are contacting these projects through several dissemination channels in order to:

- Introduce SAFEPOWER to the above mentioned projects and industry alliances.
- Invite them to workshop and conferences.
- Invite them to seminars as participants and speakers.

8.REPORT OF DISSEMINATION ACTIVITIES

The following two subsections provide an overview on the dissemination activities of SAFEPOWER. Section 8.1 lists the dissemination activities from the start of the SAFEPOWER project in January 2016 until the compilation of the final version of this deliverable in June 2016.

Upcoming activities for the next time period are listed in the table of Section 8.2. This section also contains currently pending publications.

8.1. Past Activities

Table 3: Past Dissemination Activities

Partners	Title of talk/paper	Conference/Venue/Exhibition	Date
IKL, OFF, USI	Introduction to SAFEPOWER (Secure and safe cyber-physical- systems with low power requirements)	4rd International workshop on the “Integration of mixed-criticality subsystems on multi-core and manycore processors	January, 2016
IKL, OFF, USI	Towards platform and ecosystems	COLLABORATION WORKSHOP: Advanced Computing and Cyber-Physical Systems, Brussels	June, 2016
OFF	Analysis of Power - Measurement, Simulation, and Composability	Date Conference Workshop IMPAC, Getting more for less: Innovative MPSoC Architecture Paradigms for Analysability and Composability of Timing and Power, Dresden	April, 2016
USI	<LinkedIn>	LinkedIn Group where all news and events will be posted	Continuous
USI	<Twitter>	SAFEPOWER_H2020 is the account under which all news and events will be posted	Continuous
IKL	SAFEPOWER Project	Radio interview in Basque radio show "Ekosfera"	March, 2016
IKL	SAFEPOWER project: Safe and secure mixed-criticality systems with low power requirements	HiPEAC newsletter	April, 2016
IKL	SAFEPOWER project: Safe and secure mixed-criticality systems with low power requirements	PREFIERES newsletter on energy efficiency	March, 2016

Partners	Title of talk/paper	Conference/Venue/Exhibition	Date
USI	Event-Triggered and Time-Triggered Communication in Mixed Criticality Systems."	Keynote at Second International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP)	June, 2016

8.2. Upcoming Activities

Table 4: Past Dissemination Activities

Partners	Title of talk/paper	Conference/Venue/Exhibition	Date
All SAFEPOWER Partners	SAFEPOWER project: Architecture for Safe and Power-Efficient Mixed-Criticality Systems	Euromicro Conference on Digital System Design (DSD 2016)	September, 2016
OFF	MCSDIA (Mixed Criticality System Design, Implementation and Analysis) special session	Euromicro Conference on Digital System Design (DSD 2016)	September, 2016
OFF	Integrating Power Models into Instruction Accurate Virtual Platforms for ARM-based MPSoCs	ARM TechCon 2016	October, 2016

9.PROCEDURE FOR THE DISSEMINATION OF THE ACTIVITIES AND PUBLICATIONS

The process describes how a request for publication is made, how the owners of information can respond, and the criteria that can be used in deciding for or against publication. It also defines the timing and deadlines for the process. The period of 21 days is binding also for abstracts if the publication cannot be withdrawn after submission.

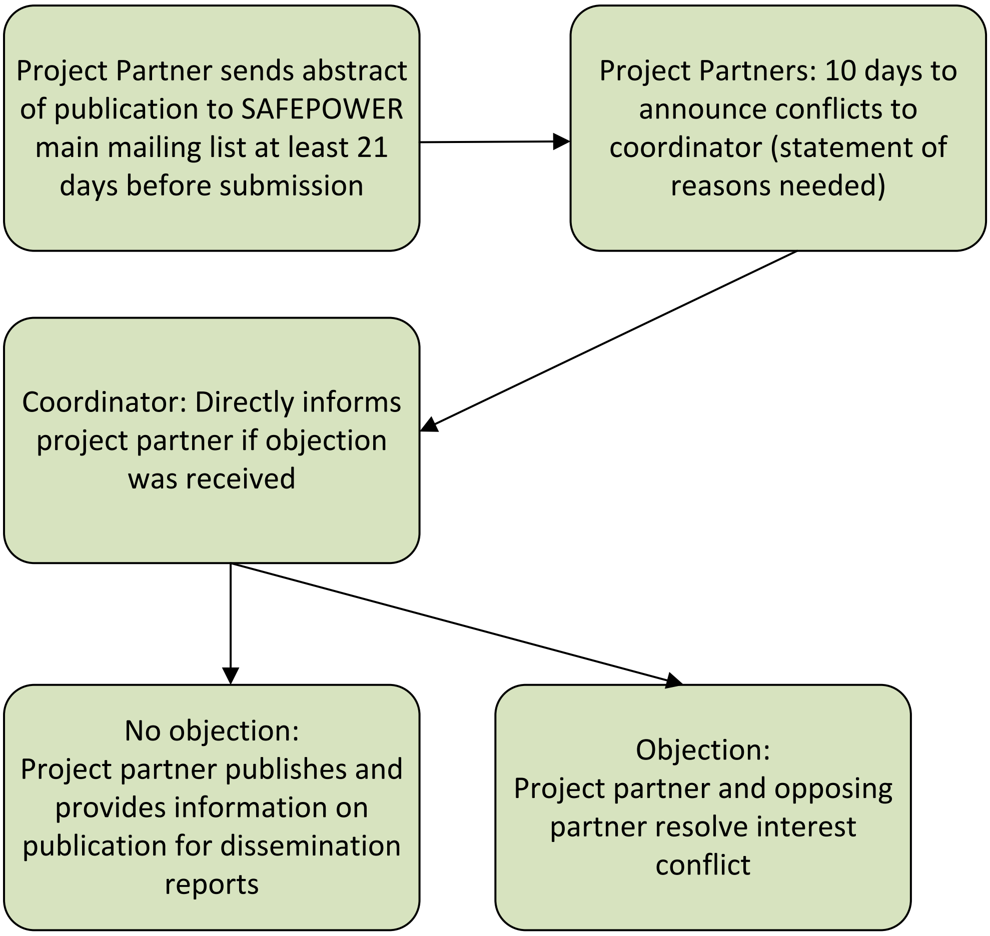
Project Partner sends abstract of publication to SAFEPOWER main mailing list at least 21 days before submission
Project Partners: 10 days to announce conflicts to coordinator (statement of reasons needed)
Coordinator: Directly informs project partner if objection was received
No objection: Project partner publishes and provides information on publication for dissemination reports
Objection: Project partner and opposing partner resolve interest conflict

Figure 1: The "Request for publication" process

All publications shall include the following statement to indicate that the foreground was generated with the assistance of financial support from the European Union:

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