SAFE COOPERATING CYBER-PHYSICAL SYSTEMS USING WIRELESS COMMUNICATION

D4.1

SAFECOP PLATFORM ARCHITECTURE, METHODS AND RUNTIME MECHANISMS

Report type	Deliverable
Report name	SafeCOP platform architecture, methods and runtime mechanisms
Dissemination level	PU
Report status:	Final
Version number:	3.2
Date of preparation:	30.09.2018

Authors

All WP4 partners

Revision chart and history log

Version	Date	Reason
1.0	2017/01/11	First draft and table of contents
1.1	2017/01/30	Revised table of content and initial description of contributions
1.2	2017/03/09	Contributions from ROT, FMI, AIT
1.3	2017/03/13	Contributions from IBTS
1.4	2017/03/15	Contributions from CNR
1.5	2017/03/27	Contributions from UNIVAQ
1.6	2017/03/30	Integration of contributions and revision from VODA
1.7	2017/04/09	IBTS platform description
1.8	2017/07/03	Major revision from DTU and UNIVAQ
1.9	2017/07/31	Minor revision from UNIVAQ, POLIMI and VODA
2.0	2017/08/08	Added UC5 content RSU-C by Aitek
2.1	2017/10/02	Contributions from UNIVAQ
3.0	2017/10/07	Document split into “root” and “leafs”
3.1	2018/07/02	Updated content and structure
3.2	2018/09/17	Candidate final version for internal revision

Contents

Acronyms and abbreviations

Abbreviation	Description
ASIL	Automotive Safety Integrity Level
RSU	Road-Side Unit
OBU	On-Board Unit
RTMA	Run-Time Manager
RTME	Run-Time Mechanisms
RTMO	Run-Time Monitor

1 INTRODUCTION

The purpose of this deliverable is to summarize the technical work of Work Package 4. The goal of WP4 is to define a reference platform architecture for Cyber-Physical Systems (CPS) which guarantees the integrity of safety-critical cooperative functions, and which is able to restrict the runtime functionality within the pre-determined design-time boundaries. To this purpose the work of WP4 relies on the basis built in WP2 and WP3. In particular WP2 defines a methodological approach to enforce safety for distributed and cooperating functions, while WP3 discusses and presents the mechanisms, the techniques and tools to support secure and safe communication mechanisms. The main points addressed by the deliverable are the following:

- To collect and discuss the proposals for cooperative platforms in the CPS (CPS-CP/CO-CPS) domain from existing project and from the literature.
- To identify and propose runtime mechanisms that can support the safety assurance process of safety-critical cooperative functions.
- To propose extensions to platforms used in the UCs (e.g. AUTOSAR, ROS) to include the SafeCOP mechanisms for safety assurance support of safety-critical cooperative functions.

In addition to these activities, simulation and validation methodologies and tools are also considered. Since the technical content of this deliverable is rather varied and touches several different aspects of the projects's goals, for the sake of clarity is has been split into several self-contained sub-documents.

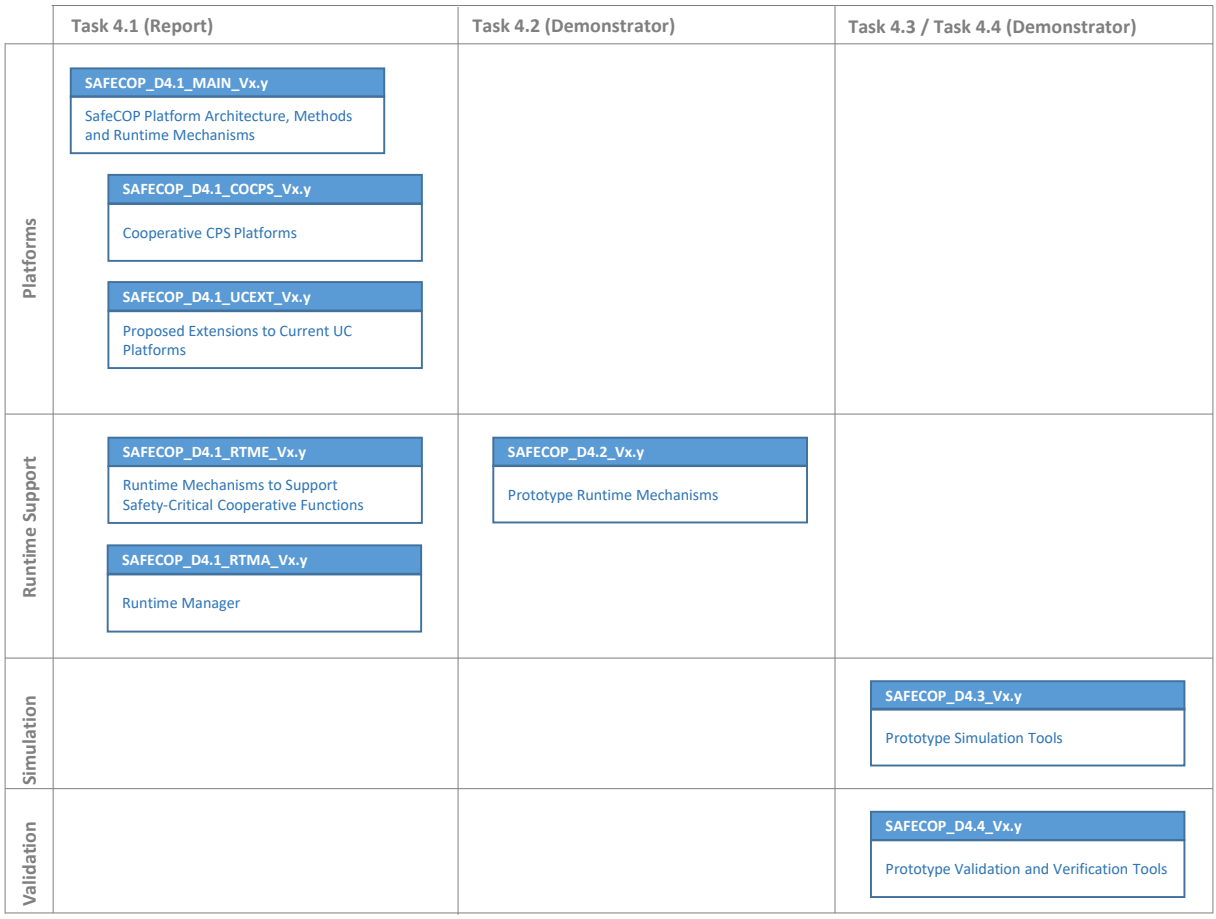

Figure 1. Document map

Furthermore, since D4.2, D4.3 and D4.4 are classified as “Demonstrators”, they will simply be a collection of short description of the methodologies and tools for runtime management, simulation and validation, while the technical content and all theoretical aspects are dealt with in this document. The overall organization of the document is depicted in the document map of Figure 1.

2 OUTLINE

This section shortly summarizes the contents of the different portions of the present document.

2.1 COOPERATIVE CPS PLATFORMS

Cooperation is defined as “an act or instance of working or acting together for a common purpose or benefit; joint action.” As people do, different technologies too can cooperate to complete a common bigger objective. So, this Section proposes a survey of the most relevant *Cooperative Platforms* in the *Cyber-Physical Systems* domain (*CO-CPS Platform*). In such a context, a platform is indented as “something” that can be exploited to avoid building a new system from scratch. So, the platform can be represented by means of a high-level architectural view (i.e. a structure of components with the description of their functionality) or by means of an implementation-oriented view (i.e. composed of a *HW Architecture*, an *Operating System*, and possibly of a *Middleware*). In a broader sense, it is possible to include in the platform also concepts about processes, methods and tools already available to support system development. The main goal is to identify CO-CPS Platforms suitable to be exploited to support safety-critical cooperative functions. For this, the survey will focus on the literature (with particular focus on existing projects) with the aim to analyze existing CO-CPS Platforms with respect to (functional) safety issues and SafeCOP goals. Then, it will be defined a generic *SafeCOP Reference Platform* (SRP). Each *SafeCOP Use Case* (SUC) will instantiate a specific instance of SRP. In particular the following platforms have been analyzed:

- KAYRON
- EUROMILS
- COMPANION
- XCYCLE
- Agilla2

The second part of the section is devoted to the description of a new reference platform defined by the project consortium, along with two possible alternative architectures that have also been proposed. The contents of this section can be found in the document “SAFECOP_D41_COCPS_Vxx.doc”

2.2 RUN-TIME MECHANISMS TO SUPPORT SAFETY-CRITICAL COOPERATIVE FUNCTIONS

The goal of this section is to analyze a general set of *Run-Time Mechanisms* (RTME) that can be exploited to support safety-critical cooperative functions and the safety assurance process in CPS-CP. It is worth noting that such mechanisms can be properly composed in the different *SafeCOP Use Case* (SUC) to provide *Run-Time Monitoring* (RTMO) services and to support the development of the *Run-Time Manager* (RTMA).

The document begins with a classification of the run-time mechanisms that have been considered and the provides an in-depth description of both the founding principles , along with a discussion of the technical details of (some) possible implementations.

The run-time mechanisms that have been identified are described in detail in the document “SAFECOP_D41_RTME_Vxx.doc”

2.3 PROPOSED EXTENSIONS TO CURRENT UC PLATFORMS

This section focuses on the SafeCOP Use Cases (UCs) baseline platforms and the main goal is to perform a preliminary analysis with respect to the extensions needed to support safety-critical cooperative functions. Such extensions will be based on the mechanisms described in Section 2.2 and they will finally give rise to UC specific instantiations of the SRP. The extended platforms will be able to provide *Run-Time Monitoring* services and to support the *Run-Time Manager* as will be described in T4.2/D4.2.

The document "SAFECOP_D41_UCEXT_Vxx.doc" describes, per each use-case, the structure of the overall system architecture, current status and functionality of the subsystems, and, referring to the run-time mechanisms identified in in Section 2.2, highlights the required extensions needed to the cooperative safety function at run-time.

2.4 RUN-TIME MANAGER

The document "SAFECOP_D41_RTMA_Vxx.doc" describes the general architecture of the run-time manager.